



Guide du développeur

AWS Backup



AWS Backup: Guide du développeur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que c'est AWS Backup ?	1
Présentation des fonctionnalités	1
Gestion de sauvegarde centralisée	1
Sauvegarde basée sur une politique	1
Politiques de sauvegarde basées sur les balises	2
Politiques de gestion du cycle de vie	2
Sauvegarde entre régions	2
Gestion et sauvegarde entre comptes	3
Audit et création de rapports avec AWS Backup Audit Manager	3
Sauvegardes incrémentielles	4
AWS Backup Gestion complète	4
Surveillance des activités de sauvegarde	5
Sécurisation de vos données dans des coffres-forts de sauvegarde	5
Prise en main	6
AWS Ressources et applications prises en charge	6
Tarification	8
AWS Backup disponibilité des fonctionnalités	8
Fonctionnalités disponibles pour toutes les ressources prises en charge	8
Disponibilité des fonctionnalités par ressource	9
Disponibilité des fonctionnalités par Région AWS	14
Services pris en charge par Région AWS	22
Comment ça marche	29
Travailler avec les AWS services pris en charge	29
Utilisation avec les données Amazon S3	30
Utilisation de machines VMware virtuelles	31
Utilisation d'Amazon DynamoDB	31
Utilisation des systèmes de FSx fichiers Amazon	32
Travailler avec Amazon EC2	33
Utilisation avec Amazon EFS	34
Utilisation avec Amazon EBS	35
Utilisation avec Amazon RDS et Aurora	35
Utilisation d'Aurora DSQL	36
Travailler avec AWS BackInt	37
Travailler avec AWS Storage Gateway	37

Utilisation avec Amazon DocumentDB	37
Utilisation avec Amazon Neptune	37
Travailler avec Amazon Redshift et Amazon Redshift Serverless	38
Utilisation avec Amazon Timestream	38
Travailler avec AWS Organizations	38
Travailler avec CloudFormation	38
Travailler avec AWS BackInt, AWS Systems Manager pour SAP et SAP HANA	39
Travailler avec Amazon EKS	39
Travailler avec Amazon GuardDuty	39
Comment AWS les services sauvegardent leurs propres ressources	40
Mesure, coûts et facturation	40
AWS Backup tarification	8
AWS Backup facturation	41
Balises d'allocation des coûts	41
AWS Backup Tarification d'Audit Manager	42
Tarification d'Amazon Aurora	42
Blogs, vidéos, didacticiels et autres ressources	42
Premiers pas	46
Prérequis	46
Inscription au service	47
Plans de sauvegarde	49
Création d'un plan de sauvegarde	49
Création de plans de sauvegarde à l'aide de la AWS Backup console	50
Créez des plans de sauvegarde à l'aide du AWS CLI	52
Options et configuration d'un plan de sauvegarde	53
CloudFormation modèles de plans de sauvegarde	63
Supprimer un plan de sauvegarde	66
Mettre à jour un plan de sauvegarde	67
Comprendre le résumé du plan de sauvegarde	68
Composants récapitulatifs	68
Aperçu des exécutions de sauvegarde planifiées	68
Validation de compatibilité des fonctionnalités	69
Accès aux résumés des plans de sauvegarde	70
Inscrivez-vous et attribuez des ressources	71
Inscrivez-vous aux services, puis attribuez des ressources	71
Activation du service	71

Attribution des ressources	72
Attribuer des ressources via la console	72
Attribuez des ressources avec AWS CLI	75
Attribuez des ressources avec CloudFormation	83
Quotas d'affectation des ressources	86
Coffres-forts de sauvegarde	87
Création et suppression d'un coffre-fort de sauvegarde	87
Autorisations requises	87
Création d'un coffre-fort de sauvegarde (console)	89
Création d'un coffre-fort de sauvegarde (par programmation)	90
Nom du coffre-fort de sauvegarde	90
AWS KMS clé de chiffrement	90
Balises du coffre-fort de sauvegarde	91
Suppression d'un coffre	91
Coffre-fort à isolation logique	92
Vue d'ensemble des coffres-forts à espacement logique	92
Cas d'utilisation pour les coffres-forts à espacement logique	93
Comparaison et contraste avec un coffre-fort de sauvegarde standard	94
Créez un coffre hermétique de manière logique	97
Afficher les détails des coffres-forts ventilés de manière logique	100
Création de sauvegardes dans un coffre-fort isolé de manière logique	101
Partagez un coffre-fort isolé de manière logique	104
Restaurez une sauvegarde à partir d'un coffre-fort isolé de manière logique	107
Supprimer un coffre-fort isolé de manière logique	108
Options programmatiques supplémentaires pour les coffres-forts à espacement logique	108
Comprendre les types de clés de chiffrement pour les coffres-forts séparés de manière logique	109
Résoudre un problème lié à un coffre hermétique	116
Sauvegardes principales vers des coffres-forts à isolation logique	118
Approbation multipartite pour les coffres-forts à espacement logique	136
Stratégies d'accès aux coffres	153
Rejet de l'accès à un type de ressource dans un coffre-fort de sauvegarde	154
Rejet de l'accès à un coffre-fort de sauvegarde	154
Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde	154
Verrouillage du coffre-fort	156

Modes de verrouillage du coffre-fort	156
Avantages de Vault Lock	157
Verrouillage d'un coffre-fort de sauvegarde à l'aide de la console	157
Verrouillage d'un coffre-fort de sauvegarde par programmation	158
Vérifiez la configuration Vault Lock d'un AWS Backup coffre-fort de sauvegarde	160
Suppression du verrouillage de coffre-fort pendant le délai de grâce (mode Conformité)	162
Compte AWS fermeture avec coffre verrouillé	162
Considérations supplémentaires en matière de sécurité	163
Création, maintenance et restauration de sauvegardes	165
Sauvegardes à la demande	166
Sauvegardes continues et PITR	168
Considérations relatives à la sauvegarde continue et au PITR	169
Services pris en charge	171
Résultat d'une sauvegarde continue	175
Restauration d'une sauvegarde continue	175
Arrêt ou suppression des sauvegardes continues	176
Copie des sauvegardes continues	177
Modification de votre période de rétention	177
Suppression de la seule règle de sauvegarde continue d'un plan de sauvegarde	178
Backup créé par type de ressource	178
Création de sauvegardes automatiques	178
Création de sauvegardes à la demande	178
Statuts des tâches de sauvegarde	179
Sauvegardes incrémentielles	179
Accès aux ressources source	180
CloudFormation empiler des sauvegardes	181
Sauvegardes SQL Amazon Aurora	188
Sauvegarde DynamoDB avancée	189
Sauvegardes Amazon EBS	195
Sauvegardes Amazon RDS	196
Sauvegardes Amazon Redshift	198
Sauvegardes sans serveur Amazon Redshift	201
Amazon EKS	204
Sauvegarde SAP HANA sur Amazon EC2	213
Sauvegardes Amazon S3	224
Sauvegardes Amazon Timestream	237

Sauvegardes de machines virtuelles	240
Création de sauvegardes Windows VSS	283
Sauvegarde et copie de balises	285
Réessayer de copier la tâche	286
Sauvegarde entre régions	287
Sauvegarde entre comptes	291
Copier les balises sur les sauvegardes	304
Suppression d'une sauvegarde	305
Suppression manuelle de sauvegardes	306
Résolution des problèmes liés aux suppressions manuelles	307
Backup et modification des balises	308
Recherche de sauvegardes	309
Aperçu	309
Cas d'utilisation pour les index de sauvegarde et la recherche	309
Accès	310
Flux de processus	311
Index des sauvegardes	311
Recherches	314
Résultats de la recherche	318
Exporter les résultats de recherche vers un compartiment S3	319
Considérations relatives aux coûts et meilleures pratiques	320
Restaurer à partir de la recherche	321
Hiérarchisation des sauvegardes	321
Aperçu	321
Configurations de hiérarchisation	322
Création de configurations de hiérarchisation	323
Gestion des configurations de hiérarchisation	325
Comment s'appliquent les configurations de hiérarchisation des sauvegardes S3	327
Structure des coûts et surveillance	327
Exemples de configuration	328
Fonctions prises en charge et limitations	330
Résolution des problèmes	331
Restaurer par type de ressource	331
Comment restaurer	331
Restaurations non destructives	332
Tests de restauration	332

Copie de balises lors d'une restauration	333
Statuts de la tâche de restauration	337
Restauration d'Aurora	338
Restauration d'Aurora DSQL	341
CloudFormation restaurer	349
Restauration de DocumentDB	350
Restauration DynamoDB	353
Restauration EBS	356
EC2 restaurer	361
Restauration EFS	367
Restauration EKS	372
FSx restaurer	380
Restauration de Neptune	390
Restauration RDS	393
Restauration Redshift	394
Restauration sans serveur Redshift	399
Restauration de SAP HANA	403
Restauration S3	413
Restauration de Storage Gateway	420
Restauration du flux temporel	422
Restauration de machines virtuelles	425
Tests de restauration	431
Aperçu	432
Comparaison avec les restaurations	432
Gestion des plans	434
Création d'un plan de test	435
Mise à jour d'un plan de test	440
Affichage des plans de test	442
Affichage des tâches de test	442
Suppression d'un plan	443
Tests Audit	445
Quotas et paramètres	445
Résolution des problèmes	445
Métadonnées déduites	447
Restaurer la validation des tests	456
Arrêter une tâche de sauvegarde	458

Afficher les sauvegardes existantes	459
Liste des sauvegardes par ressource protégée dans la console	459
Liste des sauvegardes par coffre-fort de sauvegarde dans la console	460
Liste des sauvegardes par programmation	460
AWS Backup Audit Manager	461
Utilisation de frameworks d'audit	462
Choix de vos contrôles	463
Activation du suivi des ressources	466
Création de frameworks à l'aide de la AWS Backup console	473
Création de frameworks à l'aide de l' AWS Backup API	474
Affichage du statut de conformité du cadre	489
Recherche de ressources non conformes	491
Mise à jour de frameworks d'audit	491
Suppression de frameworks d'audit	491
Utilisation des rapports d'audit	492
Contexte de rapport de travail amélioré	493
Choix de votre modèle de rapport	494
Création de plans de rapport	505
Création de plans de rapports à l'aide de l' AWS Backup API	508
Création de rapports à la demande	511
Affichage des rapports d'audit	512
Mise à jour des plans de rapport	513
Suppression de plans de rapport	513
Utilisation CloudFormation pour déployer les ressources AWS Backup d'Audit Manager	513
Activation du suivi des ressources	473
Déploiement des contrôles par défaut	519
Exonération des rôles IAM de l'évaluation des contrôles	520
Création d'un plan de rapport	521
Utilisation AWS Backup d'Audit Manager avec AWS Audit Manager	522
Contrôles et mesures correctives	522
Les ressources de sauvegarde sont incluses dans au moins un plan de sauvegarde	523
Fréquence minimale du plan de sauvegarde et conservation minimale	524
Les coffres-forts empêchent la suppression manuelle des points de récupération	525
Les points de récupération sont chiffrés	525
Rétention minimale établie pour le point de récupération	526
Une copie de sauvegarde entre régions est planifiée	526

Une copie de sauvegarde entre comptes est planifiée	527
Les ressources sont incluses dans un plan de sauvegarde avec un AWS Backup Vault	
Lock	528
Le dernier point de récupération a été créé	528
Temps de restauration des ressources pour atteindre l'objectif	529
Des ressources dans un coffre hermétique	530
Gérez plusieurs comptes avec AWS Organizations	532
Vue d'ensemble de la gestion entre comptes	532
Création d'un compte de gestion dans Organizations	534
Activation de la gestion entre comptes	534
Politiques de sauvegarde	535
Administrateur délégué	535
Conditions préalables	536
Enregistrement d'un compte membre en tant que compte administrateur délégué	538
Annuler l'enregistrement d'un compte membre	539
Déléguez AWS Backup les politiques via AWS Organizations	540
Surveillance des activités dans plusieurs Comptes AWS	540
Règles d'activation des ressources	541
Définition des politiques, syntaxe des politiques et héritage de politique	541
AWS Backup et CloudFormation	542
En général	542
Déploiement d'un coffre-fort de sauvegarde, d'un plan de sauvegarde et d'attribution de ressources avec CloudFormation	542
Déploiement de plans de sauvegarde avec CloudFormation	542
Déploiement AWS Backup des frameworks Audit Manager et des plans de rapports avec CloudFormation	543
Utilisation CloudFormation avec AWS Organizations	543
En savoir plus	543
Réseau	544
Points de terminaison	544
AWS PrivateLink	544
Considérations relatives aux points de terminaison d'un VPC Amazon	545
Création d'un point de AWS Backup terminaison VPC	545
Utiliser un point de terminaison VPC	546
Création d'une stratégie de point de terminaison de VPC	546
Sécurité	549

Validation de conformité	550
Protection des données	550
Chiffrement pour les sauvegardes dans AWS Backup	551
Chiffrement des informations d'identification de l'hyperviseur de machine virtuelle	563
Gestion des identités et des accès	565
Authentification	566
Contrôle d'accès	567
Fonctions du service IAM	577
Politiques gérées	580
Utilisation des rôles liés à un service	666
Prévention du cas de figure de l'adjoint désorienté entre services	675
Sécurité de l'infrastructure	676
Intégrité	676
AWS Backup objectif d'intégrité des données	676
AWS Backup implémentation de l'intégrité des données	676
Confirmation objective et audit de l'intégrité des données AWS Backup	677
Conservations légales	677
Vue d'ensemble de la conservation légale	677
Maintenances légales multiples	678
Création d'une conservation légale	679
Affichage des conservations légales	680
Libération d'une conservation légale	683
Protection contre les logiciels malveillants	684
Intégration avec Amazon GuardDuty	685
Accès instantané	685
Comment utiliser l'analyse des logiciels malveillants	686
Accès	686
Analyses incrémentielles ou complètes	687
Surveillance de vos analyses de malwares	688
Comprendre les résultats du scan	689
Résolution des problèmes de numérisation	690
Mesure	691
Quotas	691
Étapes d'utilisation de la console et de la CLI pour les types d'analyse des programmes malveillants	692
Résilience	696

Quotas	698
Sauvegarde	698
Index de sauvegarde et quotas de recherche	700
Quotas de politiques	701
Quotas d'analyse des logiciels	702
Quotas de ressources Amazon Timestream	703
AWS Backup Quotas d'Audit Manager	703
Rétablir les quotas du plan de test	704
AWS Backup gateway quotas	706
Quotas Amazon EKS	706
Quotas de coffre répartis de manière logique	707
Quotas associés	707
Surveillance AWS Backup	709
Tableaux de bord de la console	709
Aperçu	710
Tableau de bord des emplois	710
Motifs problématiques	712
Données du tableau de bord avec AWS CLI	716
Surveillance des événements à l'aide de EventBridge	718
Événements Backup Job	719
Événements du Backup Plan	724
Événements Backup Vault	726
Événements Copy Job	728
Événements de Recovery Point	731
Événements relatifs aux paramètres régionaux	732
Événements Restore Job	733
Événements d'indexation des points de restauration	736
Malware Scan Job Events	739
AWS Backup statistiques avec Amazon CloudWatch	746
CloudWatch Tableau de bord	746
Métriques avec CloudWatch	748
Journalisation des appels d' AWS Backup API avec CloudTrail	752
AWS Backup événements à CloudTrail	754
Comprendre les entrées du fichier AWS Backup journal	755
Journalisation des événements de gestion entre comptes	759
Options de notification avec AWS Backup	763

Notifications des utilisateurs et AWS Backup	763
Amazon SNS et événements AWS Backup	764
Résolution des problèmes AWS Backup	771
Dépannage de problèmes généraux	771
Résolution des problèmes liés à la création de ressources	772
Résolution des problèmes liés à la suppression de ressources	773
Résolution des problèmes liés à la restauration de ressources	773
Résolution des erreurs de formatage	774
AWS Backup API	775
Actions	775
AWS Backup	780
AWS Backup gateway	1267
AWS Backup	1362
Types de données	1424
AWS Backup	1427
AWS Backup gateway	1609
AWS Backup	1634
Paramètres communs	1667
Erreurs courantes	1669
Historique de la documentation	1671
.....	mdccxlviii

Qu'est-ce que c'est AWS Backup ?

AWS Backup est un service entièrement géré qui facilite la centralisation et l'automatisation de la protection des données dans l'ensemble AWS des services, dans le cloud et sur site. Ce service vous permet de configurer des politiques de sauvegarde et de surveiller l'activité de vos AWS ressources en un seul endroit. Il vous permet d'automatiser et de consolider les tâches de sauvegarde précédemment effectuées service-by-service, et élimine le besoin de créer des scripts personnalisés et des processus manuels. En quelques clics dans la console AWS Backup, vous pouvez automatiser vos politiques et planifications de protection des données.

AWS Backup ne régit pas les sauvegardes que vous effectuez dans votre AWS environnement en dehors de celles-ci AWS Backup. Par conséquent, si vous recherchez une end-to-end solution centralisée répondant aux exigences commerciales et réglementaires, commencez à l'utiliser AWS Backup dès aujourd'hui.

Présentation des fonctionnalités

AWS Backup fournit de nombreuses fonctionnalités et capacités, notamment les suivantes.

Gestion de sauvegarde centralisée

AWS Backup fournit une console de sauvegarde centralisée, un ensemble de sauvegardes APIs et le AWS Command Line Interface (AWS CLI) pour gérer les sauvegardes sur l'ensemble AWS des services utilisés par vos applications. Vous pouvez AWS Backup ainsi gérer de manière centralisée les politiques de sauvegarde qui répondent à vos exigences en matière de sauvegarde. Vous pouvez ensuite les appliquer à vos AWS ressources dans l'ensemble AWS des services, ce qui vous permet de sauvegarder les données de vos applications de manière cohérente et conforme. La console de sauvegarde AWS Backup centralisée offre une vue consolidée de vos sauvegardes et des journaux d'activité des sauvegardes, ce qui facilite l'audit de vos sauvegardes et garantit leur conformité.

Sauvegarde basée sur une politique

Avec AWS Backup, vous pouvez créer des politiques de sauvegarde appelées plans de sauvegarde. Utilisez ces plans de sauvegarde pour définir vos exigences en matière de sauvegarde, puis appliquez-les aux AWS ressources que vous souhaitez protéger dans l'ensemble AWS des services que vous utilisez. Vous pouvez créer différents plans de sauvegarde afin de répondre à des

exigences de conformité réglementaires et commerciales spécifiques. Cela permet de garantir que chaque AWS ressource est sauvegardée conformément à vos besoins. Les plans de sauvegarde facilitent l'application de votre stratégie de sauvegarde dans l'ensemble de votre organisation et de vos applications de manière scalable.

Pour connaître toutes les options de configuration des plans de sauvegarde, consultez [Options et configuration d'un plan de sauvegarde](#).

Politiques de sauvegarde basées sur les balises

Vous pouvez AWS Backup appliquer des plans de sauvegarde à vos AWS ressources de différentes manières, notamment en les étiquetant. Le balisage facilite la mise en œuvre de votre stratégie de sauvegarde dans toutes vos applications et garantit que toutes vos AWS ressources sont sauvegardées et protégées. AWS les balises constituent un excellent moyen d'organiser et de classer vos AWS ressources. L'intégration avec les AWS balises vous permet d'appliquer rapidement un plan de sauvegarde à un groupe de AWS ressources, afin qu'elles soient sauvegardées de manière cohérente et conforme.

Pour connaître toutes les manières dont vous pouvez attribuer vos ressources aux plans de sauvegarde, consultez [Sélectionnez AWS les services à sauvegarder](#).

Politiques de gestion du cycle de vie

AWS Backup vous permet de répondre aux exigences de conformité tout en minimisant les coûts de stockage des sauvegardes en stockant les sauvegardes dans un niveau de stockage à froid à faible coût. Vous pouvez configurer des stratégies de cycle de vie qui transfèrent automatiquement les sauvegardes du stockage chaud au stockage froid en fonction de la planification que vous aurez définie.

Pour une liste des ressources qui peuvent être transférées vers le stockage à froid, consultez [Disponibilité des fonctionnalités par ressource](#). Pour savoir comment activer le stockage à froid dans votre plan de sauvegarde, consultez la section [Cycle de vie et niveaux de stockage](#).

Sauvegarde entre régions

Vous pouvez ainsi copier des sauvegardes Régions AWS sur plusieurs sites différents à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. AWS Backup La sauvegarde entre régions est particulièrement utile en cas d'exigences de continuité d'activité ou de conformité

pour stocker les sauvegardes à une distance minimale de vos données de production. Pour plus d'informations, consultez [Création de copies de sauvegardes entre Régions AWS](#).

Gestion et sauvegarde entre comptes

Vous pouvez l'utiliser AWS Backup pour gérer vos sauvegardes dans Comptes AWS l'ensemble de votre [AWS Organizations](#) structure. Avec la gestion entre comptes, vous pouvez utiliser automatiquement des politiques de sauvegarde pour appliquer des plans de sauvegarde sur l'ensemble des Comptes AWS au sein de votre organisation. Ceci garantit une conformité et une protection des données efficaces à grande échelle et réduit les frais d'exploitation. Cela permet également d'éliminer la duplication manuelle des plans de sauvegarde sur les comptes individuels. Pour plus d'informations, consultez [Gestion des ressources AWS Backup sur plusieurs Comptes AWS](#).

Vous pouvez également copier des sauvegardes sur plusieurs sites différents au Comptes AWS sein de votre structure AWS Organizations de gestion. Ainsi, vous pouvez « ventiler » les sauvegardes vers un seul compte de référentiel, puis « ventiler » les sauvegardes pour une meilleure résilience. [Création de copies de sauvegarde entre Comptes AWS](#).

Avant de pouvoir utiliser les fonctionnalités de gestion et de sauvegarde entre comptes, vous devez disposer d'une structure d'organisation existante configurée dans AWS Organizations. Une unité organisationnelle (UO) est un groupe de comptes qui peut être géré comme une seule entité. AWS Organizations est une liste de comptes qui peuvent être regroupés en unités organisationnelles et gérés comme une seule entité.

Audit et création de rapports avec AWS Backup Audit Manager

AWS Backup Audit Manager vous aide à simplifier la gouvernance des données et la gestion de la conformité de l'ensemble de vos sauvegardes AWS. AWS Backup Audit Manager fournit des contrôles intégrés et personnalisables que vous pouvez adapter aux exigences de votre organisation. Vous pouvez également utiliser ces contrôles pour suivre automatiquement vos activités et ressources de sauvegarde.

AWS Backup Audit Manager peut vous aider à localiser des activités et des ressources spécifiques qui ne sont pas encore conformes aux contrôles que vous avez définis. Il génère également des rapports quotidiens que vous pouvez utiliser pour prouver la conformité de vos contrôles au fil du temps.

Pour intégrer la conformité de vos sauvegardes à votre posture de conformité globale, vous pouvez importer automatiquement les résultats AWS Backup d'Audit Manager dans AWS Audit Manager.

Sauvegardes incrémentielles

AWS Backup stocke efficacement vos sauvegardes périodiques de manière incrémentielle. La première sauvegarde d'une ressource AWS sauvegarde une copie complète de vos données. Pour chaque sauvegarde incrémentielle successive, seules les modifications apportées à vos AWS ressources sont sauvegardées. Les sauvegardes incrémentielles vous permettent de bénéficier de la protection des données grâce aux sauvegardes fréquentes tout en minimisant les coûts de stockage.

Pour une liste des ressources qui prennent en charge les sauvegardes incrémentielles, consultez [Disponibilité des fonctionnalités par ressource](#).

Pour plus d'informations sur les comportements dans les coffres-forts, consultez [Sauvegardes incrémentielles](#).

AWS Backup Gestion complète

Certains types de ressources prennent en charge AWS Backup la gestion complète. Les avantages de la AWS Backup gestion complète incluent :

- Chiffrement indépendant. AWS Backup chiffre automatiquement vos sauvegardes avec la clé KMS de votre AWS Backup coffre-fort, au lieu d'utiliser la même clé de chiffrement que votre ressource source. Cela augmente vos niveaux de défense. Pour plus d'informations, consultez [Chiffrement pour les sauvegardes dans AWS Backup](#).
- **awsbackup**Noms des ressources Amazon (ARNs). Backup ARNs commence par `arn:aws:backup` au lieu de `arn:aws:source-resource`. Cela vous permet de créer des stratégies d'accès qui s'appliquent spécifiquement aux sauvegardes et non aux ressources sources. Pour plus d'informations, consultez [Contrôle d'accès](#).
- Facturation de la sauvegarde centralisée et balises de répartition des coûts Cost Explorer. Les frais AWS Backup (y compris le stockage, les transferts de données, les restaurations et la suppression anticipée) apparaissent sous la rubrique « Sauvegarde » de votre Amazon Web Services facture, au lieu d'apparaître sous chaque ressource prise en charge. Vous pouvez également utiliser les balises de répartition des coûts de Cost Explorer pour suivre et optimiser vos coûts de sauvegarde. Pour plus d'informations, consultez [Comptage, coûts et facturation pour AWS Backup](#).

Pour savoir quels types de ressources sont éligibles à AWS Backup la gestion complète, consultez [Disponibilité des fonctionnalités par ressource](#).

Surveillance des activités de sauvegarde

AWS Backup fournit un tableau de bord qui facilite l'audit des activités de sauvegarde et de restauration dans l'ensemble AWS des services. En quelques clics sur la AWS Backup console, vous pouvez consulter l'état des dernières tâches de sauvegarde. Vous pouvez également restaurer des emplois dans l'ensemble AWS des services afin de garantir que vos AWS ressources sont correctement protégées.

AWS Backup s'intègre à Amazon CloudWatch et Amazon EventBridge. CloudWatch vous permet de suivre les métriques et de créer des alarmes. EventBridge vous permet de visualiser et de surveiller les AWS Backup événements. Pour plus d'informations, consultez les sections [Surveillance AWS Backup des événements à l'aide EventBridge](#) et [Surveillance AWS Backup des métriques avec CloudWatch](#).

AWS Backup s'intègre à AWS CloudTrail. CloudTrail vous offre une vue consolidée des journaux d'activité de sauvegarde qui permet d'auditer rapidement et facilement la manière dont vos ressources sont sauvegardées. AWS Backup s'intègre également à Amazon Simple Notification Service (Amazon SNS), vous fournissant des notifications d'activité de sauvegarde, par exemple en cas de réussite d'une sauvegarde ou de lancement d'une restauration. Pour plus d'informations, consultez [Journalisation des appels d' AWS Backup API avec CloudTrail Amazon SNS et AWS Backup événements](#).

Sécurisation de vos données dans des coffres-forts de sauvegarde

Le contenu de chaque AWS Backup sauvegarde est immuable, ce qui signifie que personne ne peut le modifier. AWS Backup sécurise davantage vos sauvegardes dans des coffres-forts de sauvegarde, ce qui les sépare en toute sécurité de leurs instances sources. Par exemple, votre coffre-fort conservera vos sauvegardes Amazon EC2 et Amazon EBS conformément à la politique de cycle de vie que vous aurez choisie, même si vous supprimez l' EC2instance Amazon source et les volumes Amazon EBS.

Les coffres-forts de sauvegarde proposent le chiffrement et des stratégies d'accès basées sur les ressources afin de définir qui a accès à vos sauvegardes. Vous pouvez définir des stratégies d'accès pour un coffre-fort de sauvegarde. Elles définissent les personnes autorisées à accéder aux sauvegardes de ce coffre-fort et les actions qu'elles peuvent effectuer. Il s'agit d'un moyen simple et sécurisé de contrôler l'accès à vos sauvegardes sur l'ensemble AWS des services. Pour consulter AWS les politiques gérées par le client pour AWS Backup, consultez la section [Politiques gérées pour AWS Backup](#).

Vous pouvez utiliser AWS Backup Vault Lock pour empêcher quiconque (y compris vous) de supprimer des sauvegardes ou de modifier leur période de conservation. AWS Backup Vault Lock vous aide à appliquer un modèle write-once-read-many(WORM) et à ajouter une couche de défense supplémentaire à votre défense en profondeur. Pour commencer, consultez [AWS Backup Vault Lock](#).

Prise en main

Pour en savoir plus AWS Backup, nous vous recommandons de commencer par [Commencer avec AWS Backup](#).

AWS Ressources et applications prises en charge

Vous trouverez ci-dessous des AWS ressources et des applications tierces que vous pouvez sauvegarder et restaurer à l'aide de ces ressources AWS Backup. Pour de plus amples informations, veuillez consulter [the section called “AWS Backup disponibilité des fonctionnalités”](#).

Service	Types de ressources pris en charge
Amazon Elastic Compute Cloud (Amazon EC2)	EC2 Instances Amazon soutenues par des volumes Amazon EBS
Amazon Simple Storage Service (Amazon S3)	Données Amazon S3
Amazon Elastic Block Store (Amazon EBS)	Volumes Amazon EBS
Amazon DynamoDB	Tables Amazon DynamoDB
Amazon Relational Database Service (Amazon RDS)	Instances de base de données Amazon RDS (y compris tous les moteurs de base de données) ; clusters à plusieurs zones de disponibilité
Amazon Aurora DSQL	Clusters monorégionaux et clusters multirégionaux
Amazon Aurora	Clusters Aurora
Amazon Elastic File System (Amazon EFS)	Système de fichiers Amazon EFS

Service	Types de ressources pris en charge
FSx pour Lustre	FSx pour les systèmes de fichiers Lustre
FSx pour le serveur de fichiers Windows	FSx pour les systèmes de fichiers Windows File Server
Amazon FSx pour NetApp ONTAP	FSx pour les systèmes de fichiers ONTAP
Amazon FSx pour OpenZFS	FSx pour les systèmes de fichiers OpenZFS
AWS Storage Gateway (Passerelle de volumes)	AWS Storage Gateway volumes
Amazon DocumentDB	Clusters basés sur des instances Amazon DocumentDB
Amazon Neptune	Clusters Amazon Neptune
Amazon Redshift	Cluster Amazon Redshift
Amazon Timestream	Tableaux Amazon Timestream
VMware Cloud™ activé AWS	VMware Machines virtuelles Cloud™ sur AWS
VMware Cloud™ activé AWS Outposts	VMware Machines virtuelles Cloud™ sur AWS Outposts
CloudFormation	CloudFormation piles
Bases de données SAP HANA	Bases de données SAP HANA sur les instances Amazon EC2
Amazon Elastic Kubernetes Service (Amazon EKS)	Clusters Amazon EKS et sauvegardes de stockage persistantes

Tarification

Avec AWS Backup, vous payez pour le stockage des sauvegardes, la restauration des données, les tests de restauration, le transfert de données entre régions et AWS Backup Audit Manager. Pour plus d'informations, consultez [Tarification d'AWS Backup](#).

AWS Backup disponibilité des fonctionnalités

AWS Backup les fonctionnalités sont proposées en fonction des ressources et Région AWS. Les sections et tableaux suivants peuvent vous aider à déterminer la disponibilité des fonctionnalités.

Table des matières

- [Fonctionnalités disponibles pour toutes les ressources prises en charge](#)
- [Disponibilité des fonctionnalités par ressource](#)
- [Disponibilité des fonctionnalités par Région AWS](#)
- [Services pris en charge par Région AWS](#)

Fonctionnalités disponibles pour toutes les ressources prises en charge

AWS Backup propose les fonctionnalités suivantes pour ses AWS services pris en charge, ainsi que pour les applications tierces prises en charge. La prise en charge d'une fonctionnalité ou d'un service ne doit pas être supposée, sauf mention explicite.

- [Planifications de sauvegarde automatiques et gestion de la rétention](#)
- [Surveillance centralisée des sauvegardes](#)
- [Sauvegardes cryptées](#)
- [Sauvegardes incrémentielles](#)
- [Gestion multi-comptes avec AWS Organizations](#)
- [Audits et rapports de sauvegarde automatisés avec AWS Backup Audit Manager](#)
- [Écriture unique, lecture multiple \(WORM\) avec Vault Lock AWS Backup](#)

Disponibilité des fonctionnalités par ressource

Pour être utilisé AWS Backup avec un AWS service pris en charge dans une région donnée, le service doit être disponible dans la région. Pour déterminer la disponibilité du service dans une région, consultez les [points de terminaison du service](#) dans le Références générales AWS.

Pour plus d'informations sur les régions optionnelles et sur les ressources et fonctionnalités prises en charge dans ces régions, consultez [Disponibilité des fonctionnalités par Région AWS](#).

AWS Backu soutie	Sauve e entre région	Sauve e entre compt	AWS Backu Audit Mana	Sauve e incrén ielle	Sauve e et point- in- time restau ion contin	Gestic compl	Cycle de vie jusqu' stocké à froid	Restaur ion au niveau de l'élémer 1	Tests de resta ion	Coffre fo rt à isolati logiqu	Reche de sauve es	Hiéran sation des sauve es	Protectio n contre les logiciels malveillan ts
Amaz EC2	✓	✓	✓	✓					✓	✓			✓
Amaz	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Amaz EBS	✓	✓	✓	✓			✓	✓	✓	✓	✓		✓
Instan unique Amaz RDS	✓ ³	✓ ³	✓ ⁴	✓	✓				✓				
Cluste Amaz RDS	✓ ³	✓ ³	✓ ⁴	✓					✓				
Amaz	✓ ³	✓ ³	✓	✓ ⁶	✓				✓	✓			

AWS Backup soutie	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continue	Gestion compl	Cycle de vie jusqu'à stocker à froid	Restauration au niveau de l'élément ¹	Tests de restauration	Coffret à isolation logique	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Amazon Aurora DSQL	✓	✓				✓	✓			✓			
Amazon FSx	✓	✓	✓	✓		✓	✓	✓	✓	✓			
FSx pour Lustre	✓	✓	✓	✓					✓	✓			
FSx pour le serveur de fichier Windows	✓	✓	✓	✓					✓ ⁸	✓			
FSx pour ONTAP			✓ ²	✓					✓				
FSx pour OpenFS	✓	✓					✓	✓					
AWS Backup	✓	✓	✓	✓						✓			

AWS Backup soutie	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continue	Gestion compl	Cycle de vie jusqu'à stocker à froid	Restauration au niveau de l'élément ¹	Tests de restauration	Coffret à isolation logique	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Amazon DocumentDB	✓ ³	✓ ³							✓	✓			
Amazon Neptune	✓ ³	✓ ³							✓	✓ ⁹			
Amazon Redshift sans serveur								✓					
Amazon TimeStream	✓	✓		✓		✓	✓			✓			
Windows VSS	✓	✓	✓	✓						✓			
Machines virtuelles	✓	✓	✓	✓		✓	✓	✓		✓			
AWS CloudFormation	✓ ⁵		✓	✓ ⁵			✓						
Amazon DynamoDB			✓						✓				

AWS Backup soutie	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continue	Gestion compl	Cycle de vie jusqu'à stocker à froid	Restauration au niveau de l'élément 1	Tests de restauration	Coffret à isolation logique	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Dynamique avec les fonctionnalités avancées AWS Backup	✓	✓	✓			✓	✓		✓	✓			
Bases de données SAP HANA sur les instances Amazon EC2	✓	✓		✓ ⁶	✓	✓	✓						
Amazon EKS 10	✓	✓				✓		✓					

Certains types de ressources disposent à la fois d'une fonctionnalité de sauvegarde continue et d'une copie entre régions et entre comptes. Lorsqu'une copie entre régions ou entre comptes d'une sauvegarde continue est réalisée, le point de récupération copié (sauvegarde) devient une

sauvegarde instantanée (périodique). PITR (Point-in-Time Restore) n'est pas disponible pour ces copies.

- Amazon RDS et Amazon S3 prennent en charge la copie entre comptes et entre régions à partir de sauvegardes incrémentielles. Amazon RDS prend également en charge la copie simultanée d'instantanés entre régions et entre comptes en une seule action.
- Les EC2 instances Amazon Aurora et SAP HANA sur Amazon prennent en charge la copie entre comptes et entre régions à partir de sauvegardes complètes. Amazon Aurora prend également en charge la copie simultanée d'instantanés entre régions et entre comptes en une seule action.

¹ L'« élément » d'une restauration au niveau de l'élément varie en fonction de la ressource prise en charge. Par exemple, un élément du système de fichiers est un fichier ou un répertoire, tandis qu'un élément S3 est un objet S3. Un VMware élément est un disque. Pour plus d'informations, consultez la section [Restaurer une sauvegarde par type de ressource](#) sur la ressource prise en charge.

² AWS Backup Audit Manager prend en charge cette ressource pour tous les contrôles, à l'exception de la [copie entre comptes et de la copie entre régions](#).

³ Amazon RDS, Aurora, DocumentDB et Neptune prennent désormais en charge la copie d'instantanés entre régions et entre comptes en une seule action. Les instances de base de données RDS à plusieurs zones de disponibilité (multi-AZ) peuvent être copiées, mais les clusters multi-AZ ne prennent actuellement pas en charge la copie entre régions ou entre comptes. Voir [Considérations relatives à la copie entre régions avec des ressources spécifiques](#) pour plus d'informations.

⁴ Consultez la section [Sauvegardes de zones de multidisponibilité RDS](#) pour les régions où le support de Backup Audit Manager est disponible.

⁵ Dans les [sauvegardes par CloudFormation pile](#), les ressources imbriquées conservent leurs caractéristiques de ressources sources. Cependant, les ressources de la pile ne conservent pas les fonctionnalités de Point-in-Time restauration (PITR) (telles qu'Amazon S3 et Amazon RDS).

⁶ Les instantanés sont complets et une sauvegarde incrémentielle est proposée via PITR.

⁷ Les systèmes de fichiers Amazon FSx for OpenZFS Multi-AZ (zone de disponibilité multiple) ne peuvent être restaurés qu'à partir de la FSx console Amazon ou de la demande d'API [createFileSystemFromBackup](#)

⁸ Est pris en charge dans un test de restauration si, FSx pour Windows, le serveur de fichiers utilise un répertoire actif AWS géré

⁹ N'est actuellement pas disponible dans la région Asie-Pacifique (Jakarta)

¹⁰ Les fonctionnalités pour les sauvegardes de stockage persistantes (par exemple Amazon EBS) prises dans le cadre d'Amazon EKS Backups refléteront la prise en charge des fonctionnalités pour les types de ressources respectifs dans ce tableau.

Disponibilité des fonctionnalités par Région AWS

AWS Backup est disponible dans toutes les versions suivantes Régions AWS. AWS Backup les fonctionnalités sont disponibles dans toutes ces régions, sauf indication contraire dans le tableau suivant.

Certaines régions exigent l'inscription d'un compte, comme indiqué dans le tableau suivant. La disponibilité de certaines fonctionnalités est déterminée par le fait que l'inscription est requise ou non. Pour plus d'informations, consultez la section relative à [Régions AWS votre compte que vous pouvez utiliser](#) dans le Guide de Gestion de compte AWS référence.

Considérations relatives aux régions optionnelles :

- La copie entre comptes n'est pas prise en charge pour Amazon DocumentDB dans les régions où l'inscription est requise.
- La copie entre régions n'est pas prise en charge pour Amazon DocumentDB dans les régions où l'inscription est requise.
- La copie interrégionale des sauvegardes Neptune est actuellement prise en charge en Afrique (Le Cap), en Asie-Pacifique (Hong Kong), en Asie-Pacifique (Jakarta), en Israël (Tel Aviv), au Moyen-Orient (Bahreïn) et au Moyen-Orient (Émirats arabes unis).

La copie interrégionale de FSx pour Lustre, FSx pour Windows File Server, FSx pour ONTAP et FSx pour OpenZFS n'est pas prise en charge dans les régions où l'inscription est requise.

- La copie entre comptes n'est pas prise en charge pour CloudFormation Neptune et Timestream dans les régions où l'inscription est requise.

Considérations et limites relatives à la gestion des comptes multiples dans les régions optionnelles :

- Régions AWS Lorsque l'opt-in est requis, la gestion entre comptes inclut la surveillance entre comptes et l'accès aux politiques de sauvegarde ; les comptes administrateurs délégués peuvent lancer des politiques mais n'ont pas accès aux fonctions de surveillance.

- Les comptes de gestion et leurs comptes enfants peuvent être activés AWS Organizations. Si un compte enfant est activé pour la gestion entre comptes avant que son compte de gestion ne soit activé pour la gestion entre comptes, il y aura un délai (jusqu'à 24 heures) avant que le suivi entre comptes ne montre les statuts des postes au sein de l'organisation.

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
USA Est (Virginie du Nord)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
USA Est (Ohio)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
US West (N. Californie)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
US West (Oregon)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Africa (Cape Town)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Hong Kong)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Hyderabad)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Jakarta)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Malaisie)	Obligatoire	✓	✓	✓			✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Asie-Pacifique (Melbourne)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Mumbai)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Nouvelle Zélande)	Obligatoire	✓		✓				✓	
Asie-Pacifique (Osaka)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Seoul)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Asia Pacific (Singapour)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Asia Pacific (Sydney)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Taïpei)	Obligatoire	✓		✓				✓	✓
Asie-Pacifique (Thaïlande)	Obligatoire	✓		✓			✓	✓	✓
Asie-Pacifique (Tokyo)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Canada (Central)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Canada-Ouest (Calgary)	Obligatoire	✓	✓	✓			✓	✓	✓
Chine (Pékin)	AWS en Chine	✓ ²						✓	
Chine (Ningxia)	AWS en Chine	✓ ²						✓	
Europe (Francfort)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Irlande)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Europe (London)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Milan)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Paris)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
Europe (Espagne)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Stockholm)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Zurich)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Israël (Tel Aviv)	Obligatoire	✓	✓	✓			✓	✓	✓
Mexique (Centre)	Obligatoire	✓		✓			✓	✓	✓
Middle East (Bahrain)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓
Moyen-Orient (EAU)	Obligatoire	✓	✓	✓	✓	✓	✓	✓	✓

AWS Backup soutient	S'inscrire	Copie de sauvegarde entre régions	Gestion entre comptes	Copie de sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration	Recherche de sauvegardes	Hiérarchisation des sauvegardes	Protection contre les logiciels malveillants
South America (São Paulo)	Facultatif	✓	✓	✓	✓	✓	✓	✓	✓
AWS GovCloud (USA Est)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓
AWS GovCloud (US-Ouest)	AWS GovCloud (US)	✓	✓	✓ ⁴	✓ ³		✓	✓	✓

¹ La copie interrégionale et multicompte vers un coffre-fort logiquement espacé n'est actuellement pas disponible dans les régions de l'Ouest du Canada (Calgary), de la Chine (Pékin), de la Chine (Ningxia), (de l'Est des États-Unis) ou AWS GovCloud (de l'Ouest des États-Unis). AWS GovCloud

² La Chine (Pékin) et la Chine (Ningxia) soutiennent la copie interrégionale de l'une de ces deux régions à l'autre. La copie entre régions n'est pas prise en charge depuis ces régions vers d'autres régions ou inversement. La copie entre comptes n'est pas prise en charge pour ces régions.

³ Le tableau de bord des jobs et les rapports organisationnels d' AWS Backup Audit Manager ne sont pas disponibles en AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). L'agrégation

du tableau de bord des jobs n'est disponible que dans les régions qui prennent en charge la gestion multi-comptes et AWS Backup Audit Manager.

⁴AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest) prennent en charge la copie interrégionale de l'une de ces deux régions à l'autre. La copie entre régions n'est pas prise en charge depuis ces régions vers d'autres régions, ni depuis d'autres régions vers ces régions.

Services pris en charge par Région AWS

AWS Backup est disponible pour ces types de ressources dans toutes les régions dans lesquelles AWS Backup la ressource répertoriée fonctionne :

- Aurora
- AWS CloudFormation
- Amazon DocumentDB
- DynamoDB
- DynamoDB avec fonctionnalités avancées AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

AWS Backup le support d'Amazon Neptune est disponible dans la plupart des régions commerciales où Neptune est pris en charge. Backup and restore ne sont actuellement pas disponibles dans la région Europe (Espagne).

AWS Backup le support d'Amazon DocumentDB n'est pas disponible en Afrique (Le Cap), en Asie-Pacifique (Hong Kong), en Israël (Tel Aviv) ou AWS GovCloud (USA Est).

Le tableau suivant indique le AWS Backup soutien aux autres AWS services par région :

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon TimeStream	VMware et passerelle Backup	Amazon EKS
USA Est (Virginie du Nord)	✓	✓	✓	✓	✓	✓	✓	✓
USA Est (Ohio)	✓	✓	✓	✓	✓	✓	✓	✓
USA Ouest (Californie du Nord)		✓	✓	✓	✓		✓	✓
USA Ouest (Oregon)	✓	✓	✓	✓	✓	✓	✓	✓
Afrique (Le Cap)		✓	✓	✓	✓		✓	✓
Asie-Pacifique (Hong Kong)		✓	✓	✓	✓		✓	✓
Asie-Pacifique		✓		✓	✓			✓

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup	Amazon EKS
Asie-Pacifique (Hyderabad)								
Asie-Pacifique (Jakarta)		✓		✓	✓			✓
Asie-Pacifique (Malaisie)				✓				✓
Asie-Pacifique (Melbourne)		Windows Lustre ; ONTAP		✓	✓			✓
Asie-Pacifique (Mumbai)		✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Nouvelle Zélande)				✓				✓

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup	Amazon EKS
Asie-Pacifique (Osaka)	✓	✓	✓	✓	✓		✓	✓
Asia Pacific (Seoul)	✓	✓	✓	✓	✓		✓	✓
Asie-Pacifique (Singapour)		✓	✓	✓	✓		✓	✓
Asie-Pacifique (Sydney)		✓	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Taïpei)				✓				✓
Asie-Pacifique (Thaïlande)				✓				✓

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup	Amazon EKS
Asie-Pacifique (Tokyo)	✓	✓	✓	✓	✓	✓	✓	✓
Canada (Centre)		✓	✓	✓	✓		✓	✓
Canada Ouest (Calgary)				✓				✓
Chine (Pékin)		Windows Lustre		✓ ¹	✓			
Chine (Ningxia)		Windows Lustre		✓ ¹	✓			
Europe (Francfort)	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Irlande)	✓	✓	✓	✓	✓	✓	✓	✓
Europe (Londres)	✓	✓	✓	✓	✓		✓	✓
Europe (Milan)		✓	✓	✓	✓		✓	✓
Europe (Paris)	✓	✓	✓	✓	✓		✓	✓

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup	Amazon EKS
Europe (Espagne)		✓		✓	✓			✓
Europe (Stockholm)		✓	✓	✓	✓		✓	✓
Europe (Zurich)		✓		✓	✓			✓
Israël (Tel Aviv)		✓		✓	✓			✓
Mexique (Centre)				✓				✓
Middle East (Bahrain)		✓	✓	✓	✓		✓	✓
Moyen-Orient (EAU)		✓		✓	✓			✓
Amérique du Sud (São Paulo)		✓	✓	✓	✓		✓	✓

Région et service	Aurora SQL	Amazon FSx	SAP HANA sur les instances EC2	Amazon S3	Storage Gateway	Amazon TimeStream	VMware et passerelle Backup	Amazon EKS
AWS GovCloud (US-Ouest)		Windows Lustre ; ONTAP		✓	✓	✓	✓	✓
AWS GovCloud (USA Est)		Windows Lustre ; ONTAP		✓	✓		✓	✓

Une vérification sur Amazon FSx indique que FSx Windows File Server, Lustre, FSx FSx ONTAP et FSx OpenZFS sont tous pris en charge dans cette région par AWS Backup ; sinon, les configurations prises en charge seront répertoriées.

¹ La copie entre comptes n'est pas prise en charge.

AWS Backup : comment ça marche

AWS Backup est un service de sauvegarde entièrement géré qui facilite la centralisation et l'automatisation de la sauvegarde des données entre les AWS services. Avec AWS Backup, vous pouvez créer des politiques de sauvegarde appelées plans de sauvegarde. Vous pouvez utiliser ces plans pour définir vos besoins en matière de sauvegarde, notamment la fréquence de sauvegarde de vos données et la durée de conservation de ces sauvegardes.

AWS Backup vous permet d'appliquer des plans de sauvegarde à vos AWS ressources en les étiquetant simplement. AWS Backup sauvegarde ensuite automatiquement vos AWS ressources conformément au plan de sauvegarde que vous avez défini.

Les sections suivantes décrivent son AWS Backup fonctionnement, les détails de sa mise en œuvre et les considérations relatives à la sécurité.

Rubriques

- [Comment AWS Backup fonctionne avec les AWS services pris en charge](#)
- [Comptage, coûts et facturation pour AWS Backup](#)
- [AWS Backup blogs, vidéos, didacticiels et autres ressources](#)

Comment AWS Backup fonctionne avec les AWS services pris en charge

Certains AWS services AWS Backup pris en charge proposent leurs propres fonctionnalités de sauvegarde autonomes. Ces fonctionnalités sont à votre disposition, que vous utilisiez ou non AWS Backup. Cependant, les sauvegardes créées par AWS les autres services ne sont pas disponibles pour une gouvernance centralisée AWS Backup.

AWS Backup Pour configurer la gestion centralisée de la protection des données pour tous les services pris en charge, vous devez choisir de gérer ce service avec AWS Backup, créer une sauvegarde à la demande ou planifier des sauvegardes à l'aide d'un plan de sauvegarde, puis stocker vos sauvegardes dans des coffres-forts de sauvegarde.

Consultez la section [Affectation de ressources](#) pour savoir comment choisir les services (types de ressources) que vous souhaitez sauvegarder.

Rubriques

- [Utilisation avec les données Amazon S3](#)
- [Utilisation de machines VMware virtuelles](#)
- [Utilisation d'Amazon DynamoDB](#)
- [Utilisation des systèmes de FSx fichiers Amazon](#)
- [Travailler avec Amazon EC2](#)
- [Utilisation avec Amazon EFS](#)
- [Utilisation avec Amazon EBS](#)
- [Utilisation avec Amazon RDS et Aurora](#)
- [Utilisation d'Aurora DSQL](#)
- [Travailler avec AWS BackInt](#)
- [Travailler avec AWS Storage Gateway](#)
- [Utilisation avec Amazon DocumentDB](#)
- [Utilisation avec Amazon Neptune](#)
- [Travailler avec Amazon Redshift et Amazon Redshift Serverless](#)
- [Utilisation avec Amazon Timestream](#)
- [Travailler avec AWS Organizations](#)
- [Travailler avec CloudFormation](#)
- [Travailler avec AWS BackInt, AWS Systems Manager pour SAP et SAP HANA](#)
- [Travailler avec Amazon EKS](#)
- [Travailler avec Amazon GuardDuty](#)
- [Comment AWS les services sauvegardent leurs propres ressources](#)

Utilisation avec les données Amazon S3

AWS Backup propose une sauvegarde et une restauration entièrement gérées pour les sauvegardes Amazon S3. Pour en savoir plus, veuillez consulter la section [Sauvegardes Amazon S3](#).

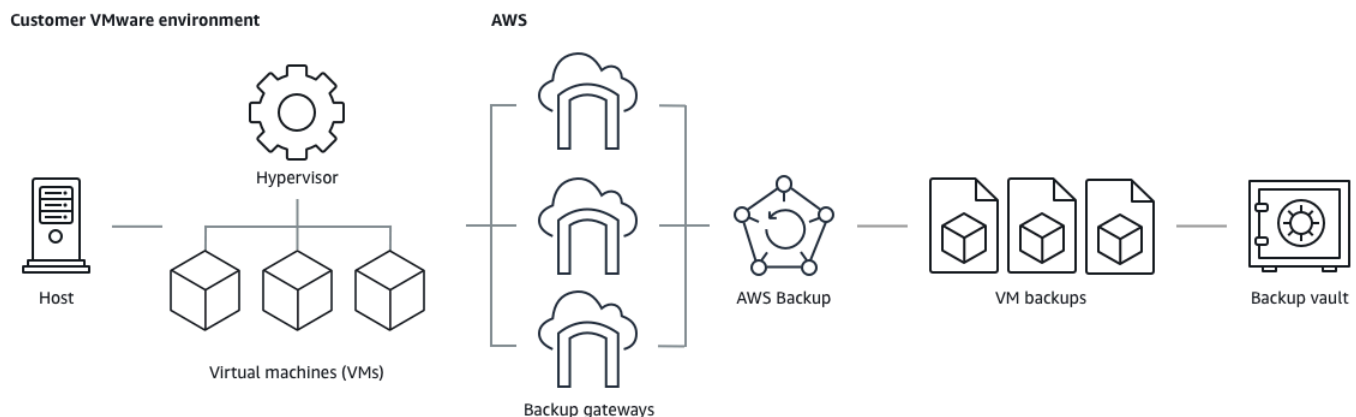
- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer les données Amazon S3 à l'aide de AWS Backup : [Restaurez les données S3 à l'aide de AWS Backup](#)

Pour obtenir des informations détaillées sur les données S3, consultez la [documentation Amazon S3](#).

Utilisation de machines VMware virtuelles

AWS Backup prend en charge la protection des données centralisée et automatisée pour les machines VMware virtuelles sur site (VMs) ainsi que VMs dans le VMware Cloud™ (VMC) sur. AWS Vous pouvez effectuer des sauvegardes depuis vos machines virtuelles sur site et VMC vers AWS Backup. Vous pouvez ensuite effectuer une restauration sur site ou sur VMC. AWS Backup

Backup Gateway est AWS Backup un logiciel téléchargeable que vous déployez sur votre VMware infrastructure pour vous y VMware VMs connecter AWS Backup. La passerelle se connecte à votre serveur de gestion de machines virtuelles pour découvrir vos VMs données, les chiffrer et les transférer efficacement vers. AWS Backup Le schéma suivant montre comment la passerelle Backup se connecte à votre VMs :



- Comment sauvegarder des ressources : [Sauvegardes de machines virtuelles](#)
- Comment restaurer des ressources d'une machine virtuelle : [Restaurez une machine virtuelle à l'aide de AWS Backup](#)

Utilisation d'Amazon DynamoDB

AWS Backup prend en charge la sauvegarde et la restauration des tables Amazon DynamoDB. DynamoDB est un service de base de données NoSQL entièrement géré qui offre des performances rapides et prévisibles avec une capacité de mise à l'échelle simple.

Depuis son lancement, DynamoDB AWS Backup a toujours été compatible. Depuis novembre 2021, des fonctionnalités avancées ont AWS Backup également été introduites pour les sauvegardes

DynamoDB. Ces fonctionnalités avancées incluent la copie de vos sauvegardes entre comptes Régions AWS et comptes, la hiérarchisation des sauvegardes vers un stockage à froid et l'utilisation de balises pour les autorisations et la gestion des coûts.

Les fonctionnalités avancées de sauvegarde DynamoDB seront activées par défaut pour les nouveaux AWS Backup clients qui s'installeront après novembre 2021.

Nous recommandons à tous les AWS Backup clients existants d'activer les fonctionnalités avancées de DynamoDB. Il n'y a aucune différence de tarification du stockage de sauvegarde à chaud après l'activation des fonctionnalités avancées, et vous pouvez économiser de l'argent en hiérarchisant les sauvegardes vers le stockage à froid et optimiser vos coûts en utilisant des balises de répartition des coûts.

Pour obtenir une liste complète des fonctionnalités avancées et savoir comment les activer, consultez [Sauvegarde DynamoDB avancée](#).

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer des ressources DynamoDB : [Restaurer une table Amazon DynamoDB](#)

Pour obtenir des informations détaillées sur DynamoDB, consultez [Qu'est-ce qu'Amazon DynamoDB ?](#) dans le Guide du développeur Amazon DynamoDB.

Utilisation des systèmes de FSx fichiers Amazon

AWS Backup prend en charge la sauvegarde et la restauration des systèmes de FSx fichiers Amazon. Amazon FSx fournit des systèmes de fichiers tiers entièrement gérés avec une compatibilité native et des ensembles de fonctionnalités adaptés aux charges de travail. AWS Backup utilise la fonctionnalité de sauvegarde intégrée d'Amazon FSx. Les sauvegardes effectuées depuis la AWS Backup console présentent donc le même niveau de cohérence et de performance du système de fichiers, ainsi que les mêmes options de restauration que les sauvegardes effectuées via la FSx console Amazon.

Si vous gérez AWS Backup ces sauvegardes, vous bénéficiez de fonctionnalités supplémentaires, telles que des options de conservation illimitées et la possibilité de créer des sauvegardes planifiées toutes les heures. En outre, AWS Backup conserve vos sauvegardes même après la suppression du système de fichiers source. Cela permet d'éviter les suppressions accidentelles ou malveillantes.

AWS Backup À utiliser pour protéger les systèmes de FSx fichiers Amazon si vous souhaitez configurer des politiques de sauvegarde et surveiller les tâches de sauvegarde à partir d'une console de sauvegarde centrale qui étend également la prise en charge d'autres AWS services.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer les FSx ressources Amazon : [Restaurer un système FSx de fichiers](#)

Pour obtenir des informations détaillées sur les systèmes de FSx fichiers Amazon, consultez la [FSx documentation Amazon](#).

Travailler avec Amazon EC2

AWS Backup prend en charge EC2 les instances Amazon.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer les EC2 ressources Amazon : [Restaurer une EC2 instance Amazon](#)

Vous pouvez planifier ou exécuter des tâches de sauvegarde à la demande qui incluent des EC2 instances entières, y compris ses volumes Amazon EBS. Par conséquent, vous pouvez restaurer une EC2 instance Amazon complète à partir d'un point de récupération unique, y compris le volume racine, les volumes de données et certains paramètres de configuration de l'instance, tels que le type d'instance et la paire de clés.

Vous pouvez également sauvegarder et restaurer vos applications Microsoft Windows compatibles avec VSS. Vous pouvez planifier des sauvegardes cohérentes avec les applications, définir des politiques de cycle de vie et effectuer des restaurations cohérentes dans le cadre d'une sauvegarde à la demande ou d'un plan de sauvegarde planifié. Pour de plus amples informations, veuillez consulter [Création de sauvegardes Windows VSS](#).

AWS Backup ne redémarre à aucun moment vos EC2 instances.

Images et instantanés

Lors de la sauvegarde d'une EC2 instance Amazon, AWS Backup prend un instantané du volume de stockage Amazon EBS racine, des configurations de lancement et de tous les volumes EBS associés. AWS Backup stocke certains paramètres de configuration de l' EC2 instance, notamment le type d'instance, les groupes de sécurité, Amazon VPC, la configuration de surveillance et les balises. Les données de sauvegarde sont stockées sous la forme d'une Amazon Machine Image (AMI) basée sur le volume Amazon EBS.

Si l'instance a été lancée à partir d'une AMI AWS Marketplace, elle possède un code produit. Une AMI créée à partir de l'instance possède également un code produit. Avec Amazon EC2, vous ne pouvez pas copier une AMI contenant un code produit sur un autre compte. Par conséquent, cette restriction existe AWS Backup également.

Si vous supprimez un instantané Amazon Machine Image (AMI) ou Amazon EBS géré à l'AWS Backup aide de la corbeille Amazon AWS Backup et que vous avez configuré la EC2 corbeille, l'image ou l'instantané peut entraîner des frais conformément à la politique d'Amazon en matière de EC2 corbeille. Les instantanés et les images placés dans la EC2 corbeille Amazon ne sont plus gérés AWS Backup et ne seront plus gérés par des AWS Backup politiques si vous les restaurez depuis la corbeille.

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une EC2 AMI AWS Backup Amazon gérée auxquels Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut EXPIRED. Ces points de récupération peuvent être [supprimés manuellement](#) si vous choisissez de supprimer d'abord le verrouillage d'instantané Amazon EBS.

AWS Backup peut chiffrer les instantanés EBS associés à une sauvegarde Amazon. EC2 Cela est similaire à la façon dont il chiffre les instantanés EBS. AWS Backup utilise le même chiffrement que celui appliqué aux volumes EBS sous-jacents lors de la création d'un instantané de l'Amazon EC2 AMI, et les paramètres de configuration de l'instance d'origine sont conservés dans les métadonnées de restauration.

Un instantané tire son chiffrement du volume, et le même chiffrement est appliqué aux instantanés correspondants. Les instantanés EBS d'une AMI copiée sont toujours chiffrés. Si vous spécifiez une clé KMS lors de la copie, la clé spécifiée est appliquée. Si vous ne spécifiez pas de clé KMS, une clé KMS par défaut est appliquée.

Pour plus d'informations, consultez les [EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon et le [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Utilisation avec Amazon EFS

AWS Backup prend en charge Amazon Elastic File System (Amazon EFS).

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer des ressources Amazon EFS : [Restaurer un système de fichiers Amazon EFS](#)

Le coffre-fort de sauvegarde automatique Amazon EFS `aws/efs/automatic-backup-vault` est réservé à ces sauvegardes automatiques uniquement.

Ce coffre-fort ne doit pas être utilisé pour créer des copies entre comptes ou comme destination pour les sauvegardes créées par d'autres plans de sauvegarde non automatisés. Si vous l'utilisez comme destination pour d'autres plans de sauvegarde, vous recevrez un message d'erreur « privilèges insuffisants ».

Pour obtenir des informations détaillées sur les systèmes de fichiers Amazon EFS, consultez [Qu'est-ce qu'Amazon Elastic File System ?](#) dans le Guide de l'utilisateur Amazon Elastic File System.

Utilisation avec Amazon EBS

AWS Backup prend en charge les volumes Amazon Elastic Block Store (Amazon EBS).

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une EC2 AMI AWS Backup Amazon gérée auxquels Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut EXPIRED. Ces points de récupération peuvent être [supprimés manuellement](#) si vous choisissez de supprimer d'abord le verrouillage d'instantané Amazon EBS.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer des volumes Amazon EBS : [Restaurer un volume Amazon EBS](#)

Pour en savoir plus, consultez le didacticiel suivant : [Amazon EBS Backup and Restore Using AWS Backup](#).

Pour plus d'informations, consultez les [volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Utilisation avec Amazon RDS et Aurora

AWS Backup prend en charge les moteurs de base de données Amazon RDS et les clusters Aurora.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- [Sauvegardes Amazon Relational Database Service](#)
- Comment restaurer des ressources Amazon RDS : [Restaurer une base de données RDS](#)

- Comment restaurer des clusters Aurora : [Restauration d'un cluster Amazon Aurora](#)

Vous pouvez également apprendre en consultant le guide pratique suivant : [Amazon RDS Backup and Restore Using AWS Backup](#)

Pour plus d'informations sur Amazon RDS, consultez [Qu'est-ce que Amazon Relational Database Service \(Amazon RDS\) ?](#) dans le Guide de l'utilisateur Amazon RDS.

Pour obtenir des informations détaillées sur Aurora, consultez [Qu'est-ce qu'Amazon Aurora ?](#) dans le Guide de l'utilisateur Amazon Aurora..

Si vous lancez une tâche de sauvegarde depuis la console Amazon RDS, cela peut entrer en conflit avec une tâche de sauvegarde des clusters Aurora, provoquant le message d'erreur La tâche de sauvegarde a expiré avant d'être terminée. Dans ce cas, configurez une fenêtre de sauvegarde plus longue dans AWS Backup.

AWS ne facture pas les instantanés Aurora stockés dans un coffre-fort de sauvegarde tant qu'Aurora a activé les sauvegardes automatisées et que la période de conservation des sauvegardes automatisées Aurora est supérieure à la période de conservation des instantanés Aurora. Tous les instantanés contenus dans le coffre de sauvegarde seront facturés si la base de données des instantanés est supprimée (les suppressions peuvent se produire accidentellement ou pendant le déploiement). blue/green

Les instantanés volumineux et les sauvegardes fréquentes à partir d'une base de données supprimée peuvent entraîner des frais de stockage importants. Consultez le [Calculateur AWS Backup](#) pour estimer les frais AWS Backup potentiels.

Utilisation d'Aurora DSQL

AWS Backup prend en charge les clusters Aurora DSQL pour des opérations de sauvegarde et de restauration centralisées. Aurora DSQL est une base de données SQL distribuée et sans serveur qui fournit aux transactions ACID une forte cohérence et une isolation instantanée entre plusieurs Régions AWS

Aurora DSQL prend en charge les configurations de clusters à région unique et multirégionale. Les clusters multirégionaux incluent des régions de cluster liées qui gèrent les opérations de lecture et d'écriture, et des régions témoins qui participent au consensus sans desservir le trafic client.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer des clusters Aurora DSQL : [Restauration Amazon Aurora DSQL](#)

Pour des informations détaillées sur Aurora DSQL, voir [Qu'est-ce qu'Aurora DSQL ?](#) dans le guide de l'utilisateur d'Aurora DSQL.

Lors de la sauvegarde de clusters Aurora DSQL multirégionaux, AWS Backup coordonne les opérations de sauvegarde entre toutes les régions du cluster liées tout en tirant parti des régions témoins pour assurer la cohérence des transactions. Cela garantit que votre sauvegarde capture un état cohérent dans l'ensemble du système de base de données distribué.

Travailler avec AWS BackInt

AWS Backup fonctionne avec AWS Backint pour prendre en charge la sauvegarde et la restauration des bases de données SAP HANA sur les instances Amazon EC2 .

- Instructions pour sauvegarder et restaurer les ressources SAP HANA : [sauvegarde et restauration des EC2 instances Amazon de SAP HANA](#)
- Configurer le AWS Backint Agent [AWS : Backint Agent pour SAP HANA](#)

Travailler avec AWS Storage Gateway

AWS Backup prend en charge Storage Gateway Volume Gateway. Vous pouvez également restaurer des instantanés Amazon EBS sous forme de volumes Storage Gateway.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer des ressources Storage Gateway : [Restaurer un volume Storage Gateway](#).

Utilisation avec Amazon DocumentDB

AWS Backup prend en charge les clusters Amazon DocumentDB.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment restaurer les ressources Amazon DocumentDB : [Restauration d'un cluster DocumentDB](#)

Utilisation avec Amazon Neptune

AWS Backup prend en charge les clusters Amazon Neptune.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)

- Comment restaurer des clusters Amazon Neptune : [Restaurer un cluster Neptune](#).

Travailler avec Amazon Redshift et Amazon Redshift Serverless

AWS Backup prend en charge les clusters provisionnés par Amazon Redshift et les espaces de noms Redshift Serverless.

- Comment [sauvegarder les clusters provisionnés par Amazon Redshift](#).
- Comment [sauvegarder les entrepôts de données Redshift Serverless](#).
- Comment [restaurer Amazon Redshift](#)
- Comment [restaurer Redshift](#) Serverless

Utilisation avec Amazon Timestream

AWS Backup prend en charge les tables Amazon Timestream.

- Comment [sauvegarder des tables Timestream](#).
- Comment [restaurer des tables Timestream](#).

Travailler avec AWS Organizations

AWS Backup fonctionne avec AWS Organizations pour simplifier le suivi et la gestion entre comptes

- [Création d'un compte de gestion dans Organizations](#).
- Activation de la [gestion entre comptes](#).
- Désignation [des comptes d'administrateur délégué et des politiques de délégation](#).

Travailler avec CloudFormation

AWS Backup CloudFormation modèles de support et piles d'applications

- [CloudFormation empiler des sauvegardes](#)

Travailler avec AWS BackInt, AWS Systems Manager pour SAP et SAP HANA

AWS Backup fonctionne avec AWS BackInt et avec SSM pour SAP afin de prendre en charge les fonctions de sauvegarde et de restauration de SAP HANA.

- [Sauvegarde des bases de données SAP HANA sur les EC2 instances Amazon](#)
- [Commencez avec AWS Systems Manager pour SAP](#)
- [AWS Agent de backint pour SAP HANA](#)

Travailler avec Amazon EKS

AWS Backup prend en charge les sauvegardes des clusters Amazon EKS, y compris l'état du cluster Kubernetes et le stockage persistant attaché au cluster EKS via une réclamation de volume persistante (volumes EBS, systèmes de fichiers EFS et compartiments S3).

Une sauvegarde Amazon EKS créera un point de restauration composite, où un point de restauration secondaire sera créé pour chaque ressource sauvegardée.

- Comment sauvegarder des ressources : [Commencer avec AWS Backup](#)
- Comment sauvegarder des clusters Amazon EKS : [Sauvegardes Amazon EKS](#)
- Comment restaurer des clusters Amazon EKS : [Restaurer un cluster Amazon EKS](#)

Pour obtenir des informations détaillées sur Amazon EKS, consultez [Qu'est-ce qu'Amazon EKS ?](#) dans le guide de l'utilisateur Amazon EKS.

Travailler avec Amazon GuardDuty

AWS Backup s'intègre GuardDuty à Amazon pour fournir une analyse automatique des programmes malveillants de vos points de récupération. Cette intégration vous permet de détecter les logiciels malveillants potentiels dans vos sauvegardes EC2, EBS et S3.

- Analyse automatisée - Configurez des plans de sauvegarde pour analyser automatiquement les points de restauration au fur et à mesure de leur création
- Analyse à la demande : lancez manuellement des analyses de points de récupération spécifiques à l'aide de l' `StartScanJob` API

- Analyse incrémentielle : analyse uniquement les données modifiées depuis la dernière analyse afin de réduire les coûts
- Résultats du scan : visualisez l'état et les résultats du scan dans la AWS Backup console et APIs

Pour activer l'analyse des programmes malveillants, vous devez configurer des rôles IAM qui permettent GuardDuty de lire vos points de restauration et AWS Backup de lancer des analyses. Pour de plus amples informations, veuillez consulter [the section called “Politiques gérées”](#).

Comment AWS les services sauvegardent leurs propres ressources

Vous pouvez consulter la documentation technique concernant le processus de sauvegarde et de restauration d'un AWS service spécifique, en particulier lorsque, lors d'une restauration, vous devez configurer une nouvelle instance de ce AWS service. Voici une liste de documentation :

- [Services EC2 associés à Amazon](#)
- [Utilisation AWS Backup avec Amazon EFS](#)
- [Backup et restauration pour DynamoDB](#)
- [Instantanés Amazon EBS](#)
- [Sauvegarde et restauration d'une instance de base de données Amazon RDS](#)
 - [Présentation de la sauvegarde et de la restauration d'un cluster de bases de données Aurora](#)
- [Utilisation AWS Backup de with FSx pour Windows File Server](#)
- [Utiliser AWS Backup avec FSx pour Lustre](#)
- [Sauvegarde de vos volumes](#)
- [Sauvegarde et restauration dans Amazon DocumentDB](#)
- [Sauvegarde et restauration d'un cluster Amazon Neptune](#)

Comptage, coûts et facturation pour AWS Backup

AWS Backup tarification

AWS Backup Les prix actuels sont disponibles au [AWS Backup tarif indiqué](#).

Important

Pour éviter des frais supplémentaires, configurez votre politique de rétention avec une durée de stockage à chaud d'au moins une semaine.

Supposons, par exemple, que vous effectuiez des sauvegardes quotidiennes et que vous les conserviez pendant une journée. Supposons également que vos ressources protégées soient si importantes qu'il vous faudra une journée entière pour terminer votre sauvegarde. AWS Backup met en œuvre votre période de conservation d'un jour et retire votre sauvegarde du stockage à chaud une fois votre travail de sauvegarde terminé. Le lendemain, AWS Backup impossible de créer une sauvegarde incrémentielle car vous n'avez aucune sauvegarde dans un espace de stockage chaud. Cette période de rétention n'étant pas conforme aux bonnes pratiques, vous encourez les risques et les dépenses liés à la création quotidienne d'une sauvegarde complète.

Contactez-nous AWS Support pour obtenir de l'aide supplémentaire.

AWS Backup facturation

Lorsqu'un type de ressource prend en charge AWS Backup la gestion complète, les frais d'AWS Backup activité (y compris le stockage, les transferts de données, les restaurations et les suppressions anticipées) apparaissent dans la section « Backup » de votre Amazon Web Services facture. Pour obtenir la liste des services qui prennent en charge la AWS Backup gestion complète, consultez la section AWS Backup Gestion complète du [Disponibilité des fonctionnalités par ressource](#) tableau.

Lorsqu'un type de ressource ne prend pas en charge AWS Backup la gestion complète, certaines de vos AWS Backup activités, telles que les coûts de stockage pour vos sauvegardes, sont facturées par le AWS service concerné.

Échecs des tâches de copie

Vous ne serez débité qu'une fois qu'un point de récupération aura été créé dans le coffre-fort de destination. Aucun frais n'est facturé en cas d'échec d'une tâche de copie et si aucun point de récupération n'est créé.

Balises d'allocation des coûts

Vous pouvez utiliser des balises de répartition des coûts pour suivre et optimiser AWS Backup les coûts de manière détaillée, ainsi que pour afficher et filtrer ces balises à l'aide de AWS Cost Explorer.

Pour utiliser des balises de répartition des coûts, consultez [Automating backups and optimizing backup costs for Amazon EFS using AWS Backup](#) et [Utilisation des balises de répartition des coûts](#).

AWS Backup Tarification d'Audit Manager

AWS Backup Audit Manager facture l'utilisation en fonction du nombre d'évaluations de contrôle. Une évaluation de contrôle est l'évaluation d'une ressource par rapport à un contrôle. Les frais d'évaluation du contrôle apparaissent sur votre AWS Backup facture. Pour connaître les tarifs actuels des évaluations de contrôle, consultez [Tarification d'AWS Backup](#).

Pour utiliser les contrôles AWS Backup d'Audit Manager, vous devez activer AWS Config l'enregistrement afin de suivre votre activité de sauvegarde. AWS Config des frais pour chaque élément de configuration enregistré, et ces frais apparaissent sur votre AWS Config facture. Pour connaître la tarification actuelle des éléments de configuration enregistrés, consultez [Tarification d'AWS Config](#).

Tarification d'Amazon Aurora

Pendant la période de rétention configurée pour les sauvegardes continues Aurora (jusqu'à 35 jours), les instantanés ne sont pas soumis à des frais de stockage. Les instantanés conservés après cette période sont facturés en tant que sauvegardes complètes.

AWS Backup blogs, vidéos, didacticiels et autres ressources

Pour plus d'informations sur AWS Backup, consultez les rubriques suivantes :

- [AWS Backup ajoute une nouvelle approbation multipartite pour les coffres-forts à espacement logique par Veliswa Boya](#) (juin 2025)
- [Simplifiez la recherche et la récupération au niveau des articles avec AWS Backup](#). Avec Bisman Sethi (décembre 2024).
- [Renforcer la cyber-résilience grâce à un coffre-fort à AWS Backup espacement logique](#). Avec Sushmitha Srinivasa Murthy et Sabith Venkitachalopathy (août 2024).
- [Associez une paire de EC2 clés Amazon à la AWS Backup restauration d'une machine VMware virtuelle](#). Avec Olumuyiwa Koya et Kenie Ogunsemowo (août 2024).
- [Rationalisez et automatisez la surveillance de la conformité et le reporting avec AWS Backup Audit Manager](#). Avec Sabith Venkitachalopathy, Glenn Chia et Mark Rowland (juin 2024).
- [Sauvegarde cohérente avec les applications Windows sur Amazon EC2 avec AWS Backup](#) Avec Bhaskar Mazumdar et Karthikeyan KM (mai 2024).

- [Optimisation AWS Backup des coûts](#). Avec Kenneth Hui (avril 2024).
- [Conception d'une stratégie de sauvegarde résiliente et rentable pour Amazon S3](#). Avec Mojgan Toth et Harish Mandhadi (mars 2024).
- [Automatisez la livraison des rapports AWS Backup d'Audit Manager par e-mail](#). Avec Ezekiel Oyerinde, Charles Meruwoma et Sri Gudavalli. (janvier 2024)
- [Streamlining Point-in-Time Recovery \(PITR\) pour Aurora](#) avec. AWS Backup Avec Enrique Ramirez (janvier 2024)
- [Backup et restaurez des machines VMware virtuelles sur site à l'aide AWS Backup de](#). Avec Olumuyiwa Koya et Ezekiel Oyerinde (juin 2022).
- [À utiliser AWS Backup pour protéger les bases de données Amazon Aurora](#). Avec Chris Hendon, Brandon Rubadou et Thomas Liddle (mai 2022).
- [Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups](#). Avec Evan Peck et Sabith Venkitachalapathy (mai 2022).
- [Automatisez et améliorez votre posture de sécurité à l'aide AWS Backup de et AWS PrivateLink](#). Avec Bilal Alam (avril 2022).
- [Obtenez des rapports quotidiens agrégés entre comptes et multirégions. AWS Backup](#) Avec Wali Akbari et Sabith Venkitachalapathy (février 2022).
- [Automatisez la visibilité des résultats de sauvegarde à l'aide AWS Backup de et AWS Security Hub CSPM](#). Avec Kanishk Mahajan (janvier 2022).
- [Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS](#). Avec Ibukun Oyewumi (janvier 2022).
- [Optimisation de SAS Grid AWS avec FSx pour Lustre \(et optimisation de la reprise après sinistre en utilisant AWS Backup\)](#). Avec Matt Saeger et Shea Lutton (janvier 2022).
- [Centralisation de la protection des données et de la conformité dans Amazon Neptune AWS Backup](#) avec. Avec Brian O'Keefe (novembre 2021).
- [Manage backup and restore of Amazon DocumentDB \(with MongoDB compatibility\) with AWS Backup](#). Avec Karthik Vijayraghavan (novembre 2021).
- [Simplifiez l'audit de vos politiques de protection des données avec AWS Backup Audit Manager](#). Avec Jordan Bjorkman et Harshitha Putta (novembre 2021).
- [Améliorez le niveau de sécurité de vos sauvegardes avec AWS Backup Vault Lock](#). Avec Rolland Miller (octobre 2021).
- [Comment conserver les balises de ressources dans les tâches de AWS Backup restauration](#). Avec Ibukun Oyewumi, Ameer Shah et Sabith Venkitachalapathy (septembre 2021).

- [Gestion de l'accès aux sauvegardes à l'aide de politiques de contrôle des services avec AWS Backup](#). Avec Sabith Venkitachalapathy et Ibukun Oyewumi (août 2021).
- [Automatisez la sauvegarde centralisée à grande échelle sur l'ensemble AWS des services à l'aide de AWS Backup](#). Avec Ibukun Oyewumi et Sabith Venkitachalapathy (juillet 2021).
- [Blog : Comment simplifier la sauvegarde de Microsoft SQL Server à l'aide AWS Backup de VSS](#). Avec Siavash Irani et Sepehr Samiei (juillet 2021).
- [Automatisez la validation de la récupération des données avec AWS Backup](#). Avec Mahanth Jayadeva (juin 2021).
- [Configuration des notifications pour surveiller les AWS Backup tâches](#). Avec Virgil Ennes (juin 2021).
- [Automating backups and optimizing backup costs for Amazon EFS using AWS Backup](#). Avec Prachi Gupta et Rohit Verma (juin 2021).
- [Gestion des coûts de sauvegarde Amazon EFS : AWS Backup prise en charge des balises de répartition des coûts](#). Avec Aditya Maruvada (mai 2021).
- [Créez et partagez des sauvegardes chiffrées entre les comptes et les régions à l'aide de AWS Backup](#). Avec Prachi Gupta (mai 2021).
- [AWS Backup est désormais approuvé par FedRAMP High pour vos besoins en matière de conformité et de protection des données](#). Avec Andy Grimes (mai 2021).
- [ZS Associates améliore l'efficacité des sauvegardes grâce à AWS Backup](#). Avec Mitesh Naik, Hiranand Mulchandani et Sushant Jadhav (mai 2021).
- [Tutoriel : utilisation AWS Backup d'Amazon EBS Backup and Restore](#). Avec Fathima Kamal (avril 2021).
- [Didacticiel vidéo : Managing cross-Region copies of backups](#). Avec David DeLuca (avril 2021).
- [Supprimez plusieurs points AWS Backup de récupération à l'aide AWS des outils pour PowerShell](#). Avec Sherif Talaat (avril 2021).
- [Sauvegardes entre régions et entre comptes pour Amazon FSx](#). AWS Backup Avec Adam Hunter et Fathima Kamal (avril 2021).
- [Amazon CloudWatch Events and Metrics pour AWS Backup](#). Avec Rolland Miller (mars 2021).
- [Tutoriel : Sauvegarde et restauration d'Amazon Relational Database Service \(RDS\) à l'aide de AWS Backup](#) Avec Fathima Kamal (mars 2021).
- [Point-in-time restauration et sauvegarde continue pour Amazon RDS avec AWS Backup](#). Avec Kelly Griffin (mars 2021).
- [Automatisez AWS Backup avec AWS Service Catalog](#). avec John Husemoller (janvier 2021).

- [Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup](#). Avec Cher Simon (janvier 2021).
- [AWS Récapitulatif de re:Invent : Protection des données et conformité](#) avec. AWS Backup Avec Nancy Wang (décembre 2020).
- [AWS Backup fournit une protection centralisée des données pour l'ensemble de vos AWS ressources](#). Avec Nancy Wang (novembre 2020).
- [Tech Talk: Data protection at scale with AWS Backup](#). Avec Kareem Behairy (septembre 2020).
- [Gestion centralisée entre comptes avec utilisation de copies interrégionales](#). AWS Backup Avec Cher Simon (septembre 2020).
- [Tutoriel vidéo : Gérer les sauvegardes à grande échelle AWS Organizations selon votre utilisation AWS Backup](#). Avec Ildar Sharafiev (juillet 2020).
- [Gérez les sauvegardes à grande échelle AWS Organizations selon votre utilisation AWS Backup](#). Avec Nancy Wang, Avi Drabkin, Ganesh Sundaresan et Vikas Shah (juin 2020).
- [Récupérez les fichiers et dossiers Amazon EFS avec AWS Backup](#). Avec Abrar Hussain et Gurudath Pai (mai 2020).
- [Scheduling automated backups using Amazon EFS and AWS Backup](#). Avec Rob Barnes (décembre 2019).
- [Re:Invent Recording : AWS re:Invent 2019 : Une plongée approfondie sur pieds AWS Backup Rackspace](#). Avec Nancy Wang et Jason Pavao (décembre 2019).
- [Protégez vos données avec AWS Backup](#). Avec Anthony Fiore (juillet 2019).
- [Vidéo marketing : Introducing AWS Backup](#). Janvier 2019.
- [Vidéo : Introduction to AWS Backup](#). Avec AWS formation et certification.

Commencer avec AWS Backup

Ce didacticiel décrit les étapes génériques d'utilisation des AWS Backup fonctionnalités. Comme pour toute partie de cette documentation technique, vous devez suivre la console AWS de gestion dans l'autre fenêtre.

Prérequis

Avant de commencer, vérifiez que vous disposez des éléments suivants :

- Un Compte AWS. Pour plus d'informations, consultez la section [Création d'un AWS compte](#).
- Au moins une ressource prise en charge par AWS Backup. Consultez la liste des [ressources et des applications tierces prises en charge par AWS](#).

Lorsque de nouveaux AWS services sont disponibles, activez AWS Backup l'option d'utilisation de ces services.

- Si vous avez l'intention d'inclure plusieurs types de ressources, tels que des volumes Amazon EBS et des compartiments Amazon S3, dans le même plan de sauvegarde, vérifiez que ces ressources sont identiques. Région AWS

Pour configurer les AWS services à utiliser avec AWS Backup

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Activation du service, choisissez Configurer les ressources.
4. Sur la page Configurer les ressources, utilisez les commutateurs à bascule pour activer ou désactiver les services utilisés avec AWS Backup. Choisissez Confirmer lorsque vos services sont configurés. Assurez-vous que le AWS service que vous choisissez est disponible dans votre Région AWS.

Voir pour plus d'informations. La AWS Backup console permet à un utilisateur d'attribuer un type de ressource à un plan de sauvegarde ; celui-ci sera inclus même si l'opt-in n'est pas activé pour ce service en particulier.

Pour terminer ce didacticiel, vous pouvez utiliser votre utilisateur Compte AWS root pour vous connecter au AWS Management Console. Gestion des identités et des accès AWS (IAM) recommande toutefois de ne pas utiliser l'utilisateur Compte AWS root. Au lieu de cela, créez un administrateur dans votre compte et utilisez ces informations d'identification pour gérer les ressources de votre compte.

La AWS Backup console propose différentes options pour sauvegarder vos ressources. Vous pouvez créer une sauvegarde à la demande, planifier et configurer la manière dont vous souhaitez que la ressource soit sauvegardée ou configurer les ressources pour qu'elles soient sauvegardées automatiquement lors de leur création.

Inscription au service

La AWS Backup console dispose de deux méthodes pour inclure des types de ressources dans un plan de sauvegarde : attribuer explicitement le type de ressource dans un plan de sauvegarde ou inclure toutes les ressources. Consultez les points ci-dessous pour comprendre comment ces sélections fonctionnent avec les activations de service.

- Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués.
- Si un type de ressource est explicitement attribué à un plan de sauvegarde, il sera inclus dans la sauvegarde même si l'opt-in n'est pas activé pour ce service en particulier. Cela ne s'applique pas à Aurora, Neptune et Amazon DocumentDB. Pour que ces services soient inclus, l'opt-in doit être activé.
- Si le type de ressource et les balises sont spécifiés dans une attribution de ressource, les types de ressources spécifiés sont d'abord filtrés, puis les balises filtrent davantage ces ressources.

Les paramètres d'abonnement au service sont ignorés pour la plupart des types de ressources. Aurora, Neptune et Amazon DocumentDB nécessitent toutefois un abonnement au service.

- Pour Amazon FSx for NetApp ONTAP, lorsque vous utilisez la sélection de ressources basée sur des balises, appliquez des balises à des volumes individuels plutôt qu'à l'ensemble du système de fichiers.

Les choix d'opt-in s'appliquent au compte spécifique et Région AWS. Lorsqu'un compte utilise AWS Backup (crée un coffre de sauvegarde ou un plan de sauvegarde) dans une région, il est automatiquement activé pour tous les types de ressources pris AWS Backup en charge par la région à ce moment-là. Les services pris en charge ajoutés ultérieurement à cette région ne seront pas

automatiquement inclus dans un plan de sauvegarde. Vous pouvez choisir d'opter pour ces types de ressources une fois qu'ils seront pris en charge.

Comme il AWS Backup prend en charge de plus en plus de AWS services et d'applications tierces, vous devrez peut-être revoir cette étape pour accéder à ces ressources nouvellement prises en charge.

AWS Backup ne régit ni ne gère les sauvegardes effectuées dans AWS des environnements autres que AWS Backup.

À activer pour protéger tous les types AWS Backup de ressources pris en charge

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Activation du service, choisissez Configurer les ressources.
4. Accédez à toutes les ressources AWS Backup prises en charge en déplaçant tous les boutons vers la droite.
5. Choisissez Confirmer.

Plans de sauvegarde

Dans AWS Backup, un plan de sauvegarde est une expression de politique qui définit quand et comment vous souhaitez sauvegarder vos AWS ressources, telles que les tables Amazon DynamoDB ou les systèmes de fichiers Amazon Elastic File System (Amazon EFS). Vous pouvez affecter des ressources à des plans de sauvegarde, puis sauvegarder et conserver AWS Backup automatiquement les sauvegardes de ces ressources conformément au plan de sauvegarde. Vous pouvez créer plusieurs plans de sauvegarde si vous avez des charges de travail avec des exigences de sauvegarde différentes. Par défaut, les fenêtres de sauvegarde sont optimisées par AWS Backup. Vous pouvez personnaliser la fenêtre de sauvegarde dans la console ou par programmation.

AWS Backup stocke efficacement vos sauvegardes périodiques de manière incrémentielle. La première sauvegarde d'une ressource AWS sauvegarde une copie complète de vos données. Pour chaque sauvegarde incrémentielle successive, seules les modifications apportées à vos AWS ressources sont sauvegardées. Les sauvegardes incrémentielles vous permettent de bénéficier de la protection des données grâce aux sauvegardes fréquentes tout en minimisant les coûts de stockage.

AWS Backup gère également de manière fluide le cycle de vie de votre plan de sauvegarde en fonction de vos paramètres de conservation, ce qui vous permet de procéder à des restaurations en cas de besoin.

Les sections suivantes présentent les principes de base de la gestion de votre stratégie de sauvegarde dans AWS Backup.

Rubriques

- [Création d'un plan de sauvegarde](#)
- [Comprendre le résumé du plan de sauvegarde](#)
- [Sélectionnez AWS les services à sauvegarder](#)

Création d'un plan de sauvegarde

Vous pouvez créer un plan de sauvegarde à l'aide de la AWS Backup console, de l'API, de la CLI, du SDK ou d'un AWS CloudFormation modèle.

Rubriques

- [Création de plans de sauvegarde à l'aide de la AWS Backup console](#)
- [Créez des plans de sauvegarde à l'aide du AWS CLI](#)

- [Options et configuration d'un plan de sauvegarde](#)
- [CloudFormation modèles de plans de sauvegarde](#)
- [Supprimer un plan de sauvegarde](#)
- [Mettre à jour un plan de sauvegarde](#)

Création de plans de sauvegarde à l'aide de la AWS Backup console

Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>. Dans le tableau de bord, choisissez Gérer les plans de sauvegarde. Ou, dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.

Options de démarrage

Trois options s'offrent à vous pour votre nouveau plan de sauvegarde :

- Création d'un plan de sauvegarde basé sur un plan existant
- Créez un nouveau plan
- [Créez un plan de sauvegarde à l'aide du AWS CLI](#)

Dans le cadre de cette procédure, nous élaborons un nouveau plan. Chaque partie de la configuration comporte un lien vers une section développée plus loin sur la page où vous pouvez naviguer pour plus de détails.

1. Entrez le nom du plan dans [Nom du plan de sauvegarde](#). Vous ne pouvez pas modifier le nom d'un plan une fois celui-ci créé.

Si vous essayez de créer un plan de sauvegarde identique à un plan existant, vous recevez un `AlreadyExistsException` message d'erreur.

2. Vous pouvez éventuellement ajouter des balises à votre plan de sauvegarde.
3. Configuration de règle de backup : dans la section de configuration des règles de sauvegarde, vous allez définir le calendrier, la fenêtre et le cycle de vie des sauvegardes.
4. Planification :
 - a. Entrez le nom de la règle de sauvegarde dans le champ de texte.
 - b. Dans le menu du coffre-fort de sauvegarde, choisissez Default ou choisissez Create new Backup vault pour créer un coffre-fort.

- c. Dans le menu de fréquence de sauvegarde, choisissez la fréquence à laquelle vous souhaitez que ce plan crée une sauvegarde.
5. Fenêtre de backup :
 - a. L'heure de début par défaut est 00h30 (00h30 dans les 24 heures) dans le fuseau horaire local de votre système.
 - b. Commencer dans est défini sur 8 heures par défaut. Vous pouvez modifier ce paramètre pour spécifier une fenêtre de temps pendant laquelle la sauvegarde doit démarrer.
 - c. Terminer dans est défini sur 7 jours par défaut. Assurez-vous que la sauvegarde est suffisamment longue, même si la tâche commence à la fin de la fenêtre de démarrage.
6. [Sauvegardes et point-in-time restauration continues \(PITR\)](#): vous pouvez sélectionner Activer les sauvegardes continues pour la point-in-time restauration (PITR). Pour vérifier quelles ressources sont prises en charge pour ce type de sauvegarde, consultez la matrice [Disponibilité des fonctionnalités par ressource](#).
7. Cycle de vie
 - a. Stockage à froid : cochez cette case pour permettre aux types de ressources éligibles de passer au stockage à froid conformément au calendrier que vous spécifiez dans la période de rétention totale. Pour utiliser le stockage à froid, vous devez avoir une période de rétention totale de 90 jours ou plus.
 - b. Le stockage à froid pour Amazon EBS est l'[archive d'instantanés Amazon EBS](#). Les instantanés transférés vers le niveau de stockage d'archives s'afficheront dans la console en tant que niveau froid. Si le stockage à froid est activé et si votre fréquence de sauvegarde est tous les mois ou moins souvent, votre plan de sauvegarde peut transférer des instantanés EBS.
 - c. La période totale de conservation est le nombre de jours pendant lesquels vous stockez votre ressource dans AWS Backup. Il s'agit du nombre total de jours de stockage au chaud plus le stockage au froid.
8. (Facultatif) Vous pouvez choisir de créer un index de sauvegarde à chaque sauvegarde périodique d'un type de ressource pris en charge (les sauvegardes continues entraîneront la création d'index quotidiens). Seuls les points de restauration (sauvegardes) associés à un index peuvent être inclus dans une [recherche de sauvegarde](#).

Par exemple, chaque fois que votre plan de sauvegarde crée une sauvegarde S3, vous pouvez également créer un index de sauvegarde pour cette sauvegarde. Cela permettra d'inclure cette sauvegarde particulière dans une future recherche.

Cochez le ou les types de ressources pour lesquels vous souhaitez créer des index.

9. (Facultatif) Activez l'analyse des programmes malveillants pour analyser automatiquement les sauvegardes après leur création. Lorsque vous configurez la protection contre les programmes malveillants, spécifiez les types de ressources à analyser (Amazon EC2, Amazon EBS, Amazon S3 ou toutes les ressources prises en charge) ainsi que les types d'analyse (complète ou incrémentielle). L'analyse des programmes malveillants s'applique uniquement aux types de ressources que vous avez sélectionnés. Par exemple, si votre plan de sauvegarde inclut à la fois des EC2 ressources Amazon S3 et Amazon, mais que vous activez l'analyse des programmes malveillants uniquement pour Amazon EC2, le service analysera uniquement vos EC2 sauvegardes. Pour chaque règle de sauvegarde, vous pouvez configurer le type de numérisation à utiliser. Le calendrier de la règle de sauvegarde déterminera la fréquence du type de numérisation.

 Important

Avant d'activer la protection contre les programmes malveillants, assurez-vous que vos rôles de sauvegarde et de scanner disposent des autorisations requises. Pour plus d'informations, consultez [la documentation sur les autorisations](#).

10. (Facultatif) Utilisez Copier vers la destination pour créer une copie inter-régions des ressources éligibles si vous souhaitez stocker une copie d'une sauvegarde dans une autre Région AWS.
11. (Facultatif) Balises ajoutées aux points de récupération.
12. Lorsque toutes les sections sont définies selon vos spécifications, choisissez Enregistrer la règle de backup.

Créez des plans de sauvegarde à l'aide du AWS CLI

Vous pouvez également définir votre plan de sauvegarde dans un document JSON et le fournir à l'aide de la console AWS Backup ou de l' AWS CLI. Le document JSON suivant contient un exemple de plan de sauvegarde qui crée une sauvegarde quotidienne à 1 h 00, heure du Pacifique (l'heure locale s'ajuste aux conditions d'heure du jour, de l'heure normale ou de l'heure d'été, le cas échéant). Il supprime automatiquement une sauvegarde au bout d'un an.

```
{
  "BackupPlan": {
    "BackupPlanName": "test-plan",
```

```

"Rules":[
  {
    "RuleName":"test-rule",
    "TargetBackupVaultName":"test-vault",
    "ScheduleExpression":"cron(0 1 ? * * *)",
    "ScheduleExpressionTimezone":"America/Los_Angeles",
    "StartWindowMinutes":integer, // Value is in minutes
    "CompletionWindowMinutes":integer, // Value is in minutes
    "IndexActions": [
      {
        "ResourceTypes": [ "string" ]
      }
    ],
    "Lifecycle":{
      "DeleteAfterDays":integer, // Value is in days
    }
  }
]
}
}

```

Vous pouvez stocker votre document JSON sous le nom de votre choix. La commande de l'interface de ligne de commande suivante affiche [create-backup-plan](#) avec un document JSON nommé `test-backup-plan.json` :

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

Notez que si certains systèmes numérotent les jours de la semaine de 0 à 6, nous les numérotons de 1 à 7. Pour plus d'informations, consultez [Cron et expressions de taux](#). Pour plus d'informations sur les fuseaux horaires, consultez [TimeZone](#) la référence de l'API Amazon Location Service.

Options et configuration d'un plan de sauvegarde

Lorsque vous définissez un plan de sauvegarde dans la AWS Backup console, vous configurez les options suivantes :

Nom du plan de sauvegarde

Vous devez donner un nom à votre plan de sauvegarde. Les noms sont limités à 50 caractères, y compris les caractères alphanumériques, les tirets, les traits de soulignement et les points.

Règles de sauvegarde

Les plans de sauvegarde comportent une ou plusieurs règles de sauvegarde. Pour ajouter des règles de sauvegarde à un plan de sauvegarde ou pour modifier des règles existantes dans un plan de sauvegarde :

1. Dans le volet de navigation de gauche de la AWS Backup console, sélectionnez Backup plans.
2. Sous Nom du plan de sauvegarde, sélectionnez un plan de sauvegarde.
3. Dans la section Règles de sauvegarde :
 - Pour ajouter une règle de sauvegarde, choisissez Ajouter une règle de sauvegarde.
 - Pour modifier une règle de sauvegarde existante, sélectionnez une règle, puis choisissez Modifier.

Note

Si vous disposez d'un plan de sauvegarde comportant plusieurs règles et que les délais des deux règles se chevauchent, AWS Backup optimise la sauvegarde et effectue une sauvegarde pour la règle dont la durée de conservation est la plus longue. L'optimisation prend en compte la fenêtre de démarrage complète, pas seulement le moment où la sauvegarde quotidienne est effectuée.

Chaque règle de sauvegarde comprend les éléments suivants.

Nom de la règle de sauvegarde

Les noms des règles de sauvegarde sont sensibles à la casse. Il doivent contenir entre 1 et 50 caractères alphanumériques ou traits d'union.

Backup frequency (Fréquence de sauvegarde)

La fréquence de sauvegarde détermine la fréquence à AWS Backup laquelle une sauvegarde instantanée est créée. Avec la console, vous pouvez choisir comme fréquence toutes les heures, toutes les 12 heures, une fois par jour, une fois par semaine ou une fois par mois. Vous pouvez également créer une expression cron qui crée des sauvegardes d'instantanés toutes les heures. À l'aide de la AWS Backup CLI, vous pouvez planifier des sauvegardes de snapshots toutes les heures.

Si vous sélectionnez une sauvegarde hebdomadaire, vous pouvez indiquer le jour de la semaine où elle doit avoir lieu. Si vous sélectionnez une sauvegarde mensuelle, vous pouvez choisir un jour spécifique du mois.

Vous pouvez également cocher la case Activer les sauvegardes continues pour les ressources prises en charge pour créer une règle de sauvegarde continue compatible avec la point-in-time restauration (PITR). Contrairement aux sauvegardes instantanées, les sauvegardes continues vous permettent d'effectuer des point-in-time restaurations. Pour en savoir plus sur les sauvegardes continues, consultez la section [Point-in-Time Restoration](#).

Fenêtre de sauvegarde

Une fenêtre de sauvegarde se compose de l'heure à laquelle la fenêtre de sauvegarde commence et de la durée en heures de cette fenêtre. Les tâches de sauvegarde sont démarrées dans cette fenêtre. Les paramètres par défaut de la console sont les suivants :

- 0 h 30, heure locale au fuseau horaire de votre système (0 h 30 dans les systèmes fonctionnant 24 heures sur 24)
- Commencer dans 8 heures
- Terminer dans 7 jours

(complet dans les limites du paramètre ne s'applique pas aux FSx ressources Amazon)

Vous pouvez personnaliser la fréquence de sauvegarde et l'heure de début de la fenêtre de sauvegarde à l'aide d'une expression cron. Pour voir les six champs des expressions AWS cron, consultez les expressions [cron et rate dans le guide](#) de EventBridge l'utilisateur Amazon. Deux exemples d'expressions AWS cron sont 15 * ? * * * (effectuer une sauvegarde toutes les heures 15 minutes après l'heure) et 0 12 * * ? * (effectuer une sauvegarde tous les jours à midi UTC). Pour consulter un tableau d'exemples, cliquez sur le lien précédent et faites défiler la page vers le bas.

AWS Backup évalue les expressions cron entre 00:00 et 23:59. Si vous créez une règle de sauvegarde pour « toutes les 12 heures », mais que vous indiquez une heure de début ultérieure à 11 h 59, elle ne sera exécutée qu'une fois par jour.

Les plans de sauvegarde dans un fuseau horaire respectant l'heure d'été peuvent être affectés par le décalage horaire suivant. Vous pouvez passer en UTC ou créer une sauvegarde manuelle le jour où l'heure avance. Pour plus d'informations, voir l'[heure d'été sur le EventBridge planificateur](#).

Les sauvegardes et point-in-time restaurations continues (PITR) font référence aux modifications enregistrées au fil du temps ; elles ne peuvent donc pas être planifiées à l'aide d'une expression temporelle ou cron.

En général, les services AWS de base de données ne peuvent pas démarrer les sauvegardes 1 heure avant ou pendant leur fenêtre de maintenance et Amazon FSx ne peut pas démarrer les sauvegardes 4 heures avant ou pendant leur fenêtre de maintenance ou leur fenêtre de sauvegarde automatique (Amazon Aurora est exempté de cette restriction de fenêtre de maintenance). Les sauvegardes d'instantanés planifiées pendant ces périodes échoueront. Une exception se produit lorsque vous choisissez d'utiliser AWS Backup à la fois pour les sauvegardes d'instantanés et pour les sauvegardes continues d'un service pris en charge. AWS Backup planifie automatiquement les fenêtres de sauvegarde pour éviter les conflits. Consultez [Point-in-Time la section Restauration](#) pour obtenir une liste des services pris en charge et des instructions sur la façon de AWS Backup les utiliser pour effectuer des sauvegardes continues.

Règles de sauvegarde se chevauchant

Il peut arriver qu'un plan de sauvegarde contienne plusieurs règles qui se chevauchent. Lorsque les fenêtres de démarrage de différentes règles se chevauchent, AWS Backup conserve la sauvegarde conformément à la règle avec la période de conservation la plus longue. Par exemple, considérez un plan de sauvegarde comportant deux règles :

1. Sauvegarde toutes les heures, avec une fenêtre de démarrage sous 1 heure et une rétention pendant 1 jour.
2. Sauvegarde toutes les 12 heures, avec une fenêtre de démarrage sous 8 heures et une rétention pendant 1 semaine.

Après 24 heures, la deuxième règle crée deux sauvegardes (car la période de rétention est plus longue). La première règle crée huit sauvegardes (car la fenêtre de démarrage sous 8 heures de la seconde règle empêche l'exécution de plusieurs sauvegardes toutes les heures). En particulier :

Au cours de cette fenêtre de démarrage	Cette règle crée 1 sauvegarde
De minuit à 8 h	12 heures
8 à 9	Par heure
9 à 10	Par heure

Au cours de cette fenêtre de démarrage	Cette règle crée 1 sauvegarde
10 à 11	Par heure
11 à 12	Par heure
De midi à 20 h	12 heures
8 à 9	Par heure
9 à 10	Par heure
10 à 11	Par heure
11 h à minuit	Par heure

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste **CREATED** jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à **RUNNING**) ou jusqu'à ce que le statut de la tâche passe à **EXPIRED** (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Cycle de vie et niveaux de stockage

Les sauvegardes sont stockées pendant le nombre de jours que vous spécifiez, connu sous le nom de cycle de vie des sauvegardes. Les sauvegardes peuvent être restaurées jusqu'à la fin de leur cycle de vie.

Il s'agit de la période de rétention totale définie dans la section du cycle de vie de la configuration des règles de sauvegarde dans la AWS Backup console.

Si vous l'utilisez AWS CLI, cela est défini à l'aide du paramètre [DeleteAfterDays](#). La période de rétention des instantanés peut aller de 1 jour à 100 ans (ou indéfiniment si vous n'en entrez pas), tandis que celle des sauvegardes continues peut aller de 1 jour à 35 jours. La date de création d'une sauvegarde est la date de début de la tâche de sauvegarde, et non la date à laquelle elle s'est terminée. Si votre tâche de sauvegarde ne se termine pas à la même date de début, utilisez la date à laquelle elle a commencé pour calculer les périodes de rétention.

Les sauvegardes sont conservées dans un niveau de stockage. Chaque niveau entraîne des coûts de stockage et de restauration différents, comme indiqué dans la [Tarification d’AWS Backup](#). Chaque sauvegarde est créée et stockée dans un espace de stockage à chaud. En fonction de la durée de conservation de votre sauvegarde, vous souhaitez peut-être passer à un niveau moins coûteux appelé stockage à froid. [Disponibilité des fonctionnalités par ressource](#) affiche les ressources dotées de cette fonctionnalité facultative.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Créez ou modifiez un plan de sauvegarde.
3. Dans la section sur le cycle de vie de la configuration des règles de sauvegarde, cochez la case Déplacer les sauvegardes du stockage à chaud au stockage à froid.
4. (Facultatif) Si Amazon EBS est l’une des ressources que vous sauvegardez et que votre fréquence de sauvegarde est tous les mois ou moins souvent, vous pouvez les faire passer au niveau froid à l’aide de l’archivage des instantanés EBS.
5. Entrez une valeur (en jours) indiquant que vous souhaitez que vos sauvegardes restent dans un espace de stockage chaud. AWS Backup recommande au moins 8 jours.
6. Entrez une valeur (en jours) pour la période totale de conservation. La différence entre la période totale de conservation et le temps passé en stockage à chaud sera le nombre de jours pendant lesquels les sauvegardes resteront en stockage à froid.

AWS CLI

1. Utiliser [create-backup-plan](#) ou [update-backup-plan](#).
- 2.
3. Incluez le paramètre booléen [OptInToArchiveForSupportedResources](#) pour les ressources EBS.
4. Incluez le paramètre [MoveToColdStorageAfterdays](#).
5. Utilisez le DeleteAfterDays paramètre. Cette valeur doit être 90 (jours) plus la valeur que vous avez saisie pour MoveToColdStorageAfterDays.

Le stockage à froid est actuellement disponible pour les types de ressources suivants :

Type de ressource	Sauvegarde incrémentielle ou complète en stockage à froid
AWS CloudFormation	Incrémentielle
DynamoDB avec les fonctionnalités avancées	Complète ; aucune sauvegarde incrémentielle à aucun niveau
Amazon EBS (à l'aide de l'archive d'instantanés EBS)	Complète ; les sauvegardes incrémentielles deviendront complètes après la transition.
Amazon EFS	Incrémentielle
Bases de données SAP HANA exécutées sur des instances Amazon EC2	Incrémentielle
Amazon Timestream	Incrémentielle
VMware machines virtuelles	Incrémentielle

Une fois que vous avez activé la transition vers le stockage à froid via la console ou la ligne de commande, les conditions suivantes sont remplies pour les sauvegardes en stockage à froid (ou en archive) :

- Les sauvegardes transférées doivent être stockées dans un entrepôt frigorifique pendant au moins 90 jours, en plus du temps passé dans un stockage à chaud. AWS Backup exige que la durée de conservation soit prolongée de 90 jours par rapport au réglage « transition au froid après plusieurs jours ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.
- Certains services prennent en charge les sauvegardes incrémentielles. Pour les sauvegardes incrémentielles, vous devez disposer d'au moins une sauvegarde complète à chaud. AWS Backup vous recommande de définir vos paramètres de cycle de vie de manière à ne pas déplacer votre sauvegarde vers un stockage à froid avant au moins 8 jours. Si la sauvegarde complète est transférée trop tôt vers le stockage à froid (par exemple, une transition vers le stockage à froid après 1 jour), une autre sauvegarde complète à chaud AWS Backup sera créée.
- Pour les types de ressources qui prennent en charge les sauvegardes incrémentielles, AWS Backup transfère les données du stockage à chaud vers le stockage à froid si les données

transférées ne sont plus référencées par les sauvegardes à chaud. Les données des sauvegardes conservées dans un stockage à froid qui ne sont référencées que par d'autres sauvegardes à froid sont facturées au prix du niveau de stockage à froid. Les autres sauvegardes continuent au tarif du niveau de stockage à chaud.

Coffre-fort de sauvegarde

Un coffre de sauvegarde est un conteneur dans lequel vous pouvez organiser vos sauvegardes. Les sauvegardes créées par une règle de sauvegarde sont organisées dans le coffre-fort de sauvegarde que vous spécifiez dans la règle de sauvegarde. Vous pouvez utiliser les coffres-forts de sauvegarde pour définir la clé de chiffrement AWS Key Management Service (AWS KMS) qui est utilisée pour chiffrer les sauvegardes dans le coffre-fort de sauvegarde et pour contrôler l'accès aux sauvegardes dans le coffre-fort de sauvegarde. Vous pouvez également ajouter des balises aux coffres-forts de sauvegarde pour vous aider à les organiser. Si vous ne souhaitez pas utiliser le coffre-fort par défaut, vous pouvez en créer un. Pour step-by-step obtenir des instructions sur la création d'un coffre-fort de sauvegarde, consultez [Création et suppression d'un coffre-fort de sauvegarde](#).

Copier vers les régions

Dans le cadre de votre plan de sauvegarde, vous pouvez éventuellement créer une copie de sauvegarde dans le même plan ou dans un autre Région AWS. Ces copies peuvent être effectuées sur le même compte ou sur un autre compte. Pour plus d'informations sur les copies de sauvegardes, consultez [Création de copies de sauvegardes entre Régions AWS](#).

Lorsque vous définissez une copie de sauvegarde, vous configurez les options suivantes :

Région de destination

La région de destination de la copie de sauvegarde.

(Paramètres avancés) Coffre-fort de sauvegarde

Le coffre-fort de sauvegarde de destination pour la copie.

(Paramètres avancés) Rôle IAM

Rôle IAM AWS Backup utilisé lors de la création de la copie. Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS Backup permet d'assumer le rôle. Si vous choisissez Par défaut et que le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.

(Paramètres avancés) Cycle de vie

Spécifie le moment d'effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d'expiration (suppression) de la copie. Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid .

Si la valeur pour [Lifecycle:DeleteAfterDays](#)(affichée sous la forme Expire dans la console) n'est pas spécifiée dans les paramètres de copie, la copie suivra les paramètres du cycle de vie de la sauvegarde à partir de laquelle elle est copiée.

Balises ajoutées aux points de récupération

Les balises que vous répertoriez ici sont automatiquement ajoutées aux sauvegardes lorsqu'elles sont créées.

Balises ajoutées aux plans de sauvegarde

Ces balises sont associées au plan de sauvegarde lui-même afin de vous aider à organiser et effectuer le suivi de votre plan de sauvegarde.

Paramètres de sauvegarde avancés

Les paramètres de sauvegarde avancés vous permettent de configurer des options de sauvegarde spécifiques aux ressources pour différents AWS services.

Paramètres de sauvegarde EC2 avancés d'Amazon

Permet des sauvegardes cohérentes des applications pour les applications tierces qui s'exécutent sur EC2 des instances Amazon. Actuellement, AWS Backup prend en charge les sauvegardes Windows VSS. AWS Backup exclut certains types d' EC2 instances Amazon des sauvegardes Windows VSS. Pour de plus amples informations, veuillez consulter [Création de sauvegardes Windows VSS](#).

Paramètres de sauvegarde avancés d'Amazon S3

AWS Backup fournit des paramètres avancés pour contrôler les métadonnées incluses dans vos sauvegardes Amazon S3. Vous pouvez éventuellement exclure les listes de contrôle d'accès (ACLs) et les balises d'objet de vos sauvegardes, conformément aux meilleures pratiques d'Amazon S3 qui consistent à utiliser des autorisations au niveau du compartiment plutôt qu'au niveau de l'objet. ACLs

Pour obtenir des informations détaillées sur la configuration des options de sauvegarde Amazon S3 ACLs et des balises d'objet, consultez [Paramètres de sauvegarde avancés d'Amazon S3](#).

Important

Lorsque vous les excluez ACLs des sauvegardes, les objets restaurés sans ces ACLs éléments utiliseront les paramètres de propriété par défaut du compartiment de destination. Le compartiment de destination doit avoir une configuration de propriété d'objet appropriée.

Note

Lorsqu'une tâche de sauvegarde continue est en cours d'exécution pour un compartiment Amazon S3 et que vous lancez une tâche de sauvegarde instantanée, celle-ci utilise les mêmes paramètres d'ACL et de balise d'objet que la sauvegarde continue, quels que soient les paramètres spécifiés pour la tâche de capture instantanée.

Analyse des logiciels malveillants

AWS Backup s'intègre GuardDuty à Amazon pour fournir une analyse automatique des programmes malveillants de vos points de récupération. Lorsque vous activez l'analyse des programmes malveillants dans votre plan de sauvegarde, elle analyse AWS Backup automatiquement vos sauvegardes pour détecter les malwares et fournit des résultats d'analyse pour vous aider à prendre des décisions éclairées concernant la restauration de vos données.

Pour configurer l'analyse des programmes malveillants pour votre plan de sauvegarde, procédez comme suit :

1. Créez un rôle IAM qui approuve `malware-protection.guardduty.amazonaws.com` et associe la politique AWS `AWSBackupGuardDutyRolePolicyForScans` gérée.
2. Associez la politique AWS gérée `AWSBackupServiceRolePolicyForScans` au rôle IAM de votre sélection de sauvegarde.
3. Dans la configuration de votre plan de sauvegarde, ajoutez des paramètres de numérisation qui spécifient :
 - Le service de numérisation (GuardDuty)
 - Les types de ressources à scanner (Amazon EC2, Amazon EBS, Amazon S3)

- Le rôle IAM (ARN) GuardDuty à assumer
4. Configurez les actions de scan dans vos règles de sauvegarde pour spécifier :
- Le service de numérisation (GuardDuty)
 - Type de numérisation (analyse incrémentielle ou complète)

Pour plus d'informations sur les politiques gérées, reportez-vous aux sections [the section called “AWSBackupGuardDutyRolePolicyForScans”](#) et [the section called “AWSBackupServiceRolePolicyForScans”](#).

CloudFormation modèles de plans de sauvegarde

Nous fournissons deux exemples de CloudFormation modèles à titre de référence. Le premier modèle crée un plan de sauvegarde simple. Le second modèle autorise les sauvegardes VSS dans un plan de sauvegarde.

Note

Si vous utilisez le rôle de service par défaut, remplacez-le *service-role* par `AWSBackupServiceRolePolicyForBackup`.

Description: backup plan template to back up all resources daily at 5am UTC, and tag all recovery points with backup:daily.

Resources:

KMSKey:

Type: `AWS::KMS::Key`

Properties:

Description: "Encryption key for daily"

EnableKeyRotation: `True`

Enabled: `True`

KeyPolicy:

Version: "2012-10-17"

Statement:

- Effect: `Allow`

Principal:

"AWS": { "Fn::Sub": "arn:\${AWS::Partition}:iam:\${AWS::AccountId}:root" }

Action:

- kms:*


```
Resource: "*"

```

```
BackupVaultWithDailyBackups:

```

```
  Type: "AWS::Backup::BackupVault"

```

```
  Properties:

```

```
    BackupVaultName: "BackupVaultWithDailyBackups"

```

```
    EncryptionKeyArn: !GetAtt KMSKey.Arn

```

```
BackupPlanWithDailyBackups:

```

```
  Type: "AWS::Backup::BackupPlan"

```

```
  Properties:

```

```
    BackupPlan:

```

```
      BackupPlanName: "BackupPlanWithDailyBackups"

```

```
      BackupPlanRule:

```

```
        - RuleName: "RuleForDailyBackups"

```

```
          TargetBackupVault: !Ref BackupVaultWithDailyBackups

```

```
          ScheduleExpression: "cron(0 5 ? * * *)"

```

```
  DependsOn: BackupVaultWithDailyBackups

```

```
DDBTableWithDailyBackupTag:

```

```
  Type: "AWS::DynamoDB::Table"

```

```
  Properties:

```

```
    TableName: "TestTable"

```

```
    AttributeDefinitions:

```

```
      - AttributeName: "Album"

```

```
        AttributeType: "S"

```

```
    KeySchema:

```

```
      - AttributeName: "Album"

```

```
        KeyType: "HASH"

```

```
    ProvisionedThroughput:

```

```
      ReadCapacityUnits: "5"

```

```
      WriteCapacityUnits: "5"

```

```
    Tags:

```

```
      - Key: "backup"

```

```
        Value: "daily"

```

```
BackupRole:

```

```
  Type: "AWS::IAM::Role"

```

```
  Properties:

```

```
    AssumeRolePolicyDocument:

```

```
      Version: "2012-10-17"

```

```
      Statement:

```

```
        - Effect: "Allow"

```

```
        Principal:

```

```

      Service:
        - "backup.amazonaws.com"
      Action:
        - "sts:AssumeRole"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/service-role/service-role"

    TagBasedBackupSelection:
      Type: "AWS::Backup::BackupSelection"
      Properties:
        BackupSelection:
          SelectionName: "TagBasedBackupSelection"
          IamRoleArn: !GetAtt BackupRole.Arn
          ListOfTags:
            - ConditionType: "STRINGEQUALS"
              ConditionKey: "backup"
              ConditionValue: "daily"
          BackupPlanId: !Ref BackupPlanWithDailyBackups
      DependsOn: BackupPlanWithDailyBackups

```

Description: backup plan template to enable Windows VSS and add backup rule to take backup of assigned resources daily at 5am UTC.

```

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:

```

```
BackupVaultName: "BackupVaultWithDailyBackups"
EncryptionKeyArn: !GetAtt KMSKey.Arn

BackupPlanWithDailyBackups:
  Type: "AWS::Backup::BackupPlan"
  Properties:
    BackupPlan:
      BackupPlanName: "BackupPlanWithDailyBackups"
      AdvancedBackupSettings:
        - ResourceType: EC2
          BackupOptions:
            WindowsVSS: enabled
      BackupPlanRule:
        - RuleName: "RuleForDailyBackups"
          TargetBackupVault: !Ref BackupVaultWithDailyBackups
          ScheduleExpression: "cron(0 5 ? * * *)"

  DependsOn: BackupVaultWithDailyBackups
```

Supprimer un plan de sauvegarde

Vous ne pouvez supprimer un plan de sauvegarde qu'une fois que toutes les sélections de ressources associées ont été supprimées. Ces sélections sont également appelées affectations de ressources. S'ils n'ont pas été supprimés avant la suppression du plan de sauvegarde, la console affiche le message d'erreur suivant : « Les sélections de plan de sauvegarde associées doivent être supprimées avant la suppression du plan de sauvegarde ». Utilisez la console ou utilisez [DeleteBackupSelection](#).

La suppression d'un plan de sauvegarde supprime la version actuelle du plan. Les versions actuelles et précédentes, le cas échéant, existent toujours, mais elles ne sont plus répertoriées sur la console sous plans de sauvegarde.

Note

La suppression d'un plan de sauvegarde n'implique pas la suppression des sauvegardes existantes. Les sauvegardes existantes doivent être supprimées dans le coffre-fort de sauvegarde en suivant les étapes dans [Suppression des sauvegardes](#).

Pour supprimer un plan de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation de gauche, sélectionnez Backup plans (Plans de sauvegarde).
3. Choisissez votre plan de sauvegarde dans la liste.
4. Sélectionnez toutes les affectations de ressources qui sont associées au plan de sauvegarde.
5. Sélectionnez Delete (Supprimer).

Mettre à jour un plan de sauvegarde

Après avoir créé un plan de sauvegarde, vous pouvez modifier le plan : vous pouvez, par exemple, ajouter des balises, ou vous pouvez ajouter, modifier ou supprimer des règles de sauvegarde. Les modifications que vous apportez à un plan de sauvegarde n'ont aucun effet sur les sauvegardes existantes créées par le plan de sauvegarde. Les modifications s'appliquent uniquement aux sauvegardes qui seront créés ultérieurement.

Par exemple, lorsque vous mettez à jour la période de rétention dans une règle de sauvegarde, la période de rétention des sauvegardes créées avant la mise à jour ne change pas. Toutes les sauvegardes créées par cette règle à partir de la modification reflètent la mise à jour de la période de rétention.

Vous ne pouvez pas modifier le nom d'un plan une fois celui-ci créé.

Pour modifier un plan de sauvegarde à l'aide de la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Dans le deuxième volet, Backup plans, les backplans existants sont affichés. Sélectionnez le lien souligné dans la colonne Nom du plan de sauvegarde pour voir les détails du plan de sauvegarde choisi.
4. Vous pouvez modifier une règle de sauvegarde, afficher les affectations de ressources, consulter les tâches de sauvegarde, gérer les balises ou modifier les paramètres Windows VSS.
5. Pour mettre à jour une règle de sauvegarde, sélectionnez le nom de la règle de sauvegarde.

Sélectionnez Gérer les balises pour ajouter ou supprimer des balises.

Sélectionnez **Modifier** à côté de **Paramètres de sauvegarde avancés** pour activer ou désactiver Windows VSS.

6. Modifiez le ou les paramètres que vous préférez, puis sélectionnez **Enregistrer**.

Comprendre le résumé du plan de sauvegarde

La fonction récapitulative du plan de sauvegarde fournit une vue complète de la configuration de votre plan de sauvegarde afin de vous aider à vérifier que votre stratégie de sauvegarde répond à vos exigences. Le résumé inclut trois composants clés qui répondent aux défis courants des clients lors de la gestion de configurations de sauvegarde complexes sur plusieurs AWS services.

Composants récapitulatifs

Chaque résumé du plan de sauvegarde contient les informations suivantes :

- 10 prochaines exécutions de sauvegarde planifiées : indique quand vos règles de sauvegarde seront exécutées, y compris les règles fusionnées et la gestion appropriée des fuseaux horaires
- Remarques sur la compatibilité des fonctionnalités : informations sur les services qui prennent en charge la point-in-time restauration (PITR) et le stockage à froid s'ils font partie de la règle de votre plan de sauvegarde.

Aperçu des exécutions de sauvegarde planifiées

L'aperçu des exécutions planifiées affiche jusqu'à 10 futures exécutions de sauvegarde en fonction des règles de votre plan de sauvegarde. Cet aperçu vous aide à comprendre à quel moment les sauvegardes auront lieu et comment plusieurs règles interagissent les unes avec les autres.

Comment plusieurs règles sont fusionnées

Lorsqu'un plan comporte plusieurs règles de sauvegarde, AWS Backup applique une logique de fusion pour déterminer le comportement de sauvegarde final :

- Fenêtres de sauvegarde qui se chevauchent : il est recommandé de ne pas avoir deux règles contradictoires. Lorsque deux règles doivent s'exécuter en même temps, en AWS Backup sélectionne une.
- Combinaisons PITR et instantanés : le PITR s'applique aux ressources prises en charge, tandis que les instantanés s'appliquent à toutes les ressources de la sélection

- Fuseaux horaires multiples : chaque règle respecte son fuseau horaire configuré pour la planification de l'exécution
- Actions de copie entre régions : les actions de copie sont conservées et affichées avec leurs informations de destination. Notez que si une règle de copie est attachée à une règle de planification conflictuelle, la règle de copie ne s'exécutera que si la règle de planification a été exécutée.

Exemple Exemple de fusion de règles

Envisagez un plan de sauvegarde comportant deux règles :

- Règle 1 : Instantané quotidien à 8 h PDT, conservation pendant 35 jours
- Règle 2 : Instantané hebdomadaire à 8 h PDT, conservation pendant 90 jours

Lorsque les deux règles s'exécutent le même jour (par exemple le dimanche), l'aperçu affiche la règle 2 car elle est plus longue (90 jours contre 35 jours).

Types d'exécution

L'aperçu des exécutions planifiées affiche différents types d'exécution en fonction de la configuration de vos règles :

- CONTINUOUS: sauvegardes continues pour les services pris en charge
- SNAPSHOTs: sauvegardes instantanées (périodiques) de toutes les ressources de la sélection
- CONTINUOUS_AND_SNAPSHOTs: Point-in-time-restore (PITR) pour les types de ressources qui le prennent en charge ; instantané (périodique) pour tous les autres types de ressources.

Validation de compatibilité des fonctionnalités

Le résumé inclut des rappels de compatibilité pour vous aider à comprendre quels AWS services prennent en charge les fonctionnalités de sauvegarde avancées. Cela permet d'éviter les erreurs de configuration et les coûts imprévus.

Point-in-time aide au rétablissement

Lorsque vous activez les sauvegardes continues dans une règle, le résumé vous rappelle que le PITR n'est pris en charge que pour :

- Bases de données Aurora
- Bases de données Amazon RDS
- Bases de données SAP HANA
- Compartiments Amazon S3

Support pour le stockage à froid

Lorsque vous configurez des transitions de niveau froid, le résumé indique quels services prennent en charge cette fonctionnalité :

- Tables Amazon DynamoDB
- Systèmes de fichiers Amazon Elastic File System
- Bases de données SAP HANA
- Bases de données Amazon Timestream
- VMware machines virtuelles

Accès aux résumés des plans de sauvegarde

Vous pouvez consulter les résumés des plans de sauvegarde dans la AWS Backup console après avoir créé ou mis à jour un plan de sauvegarde. Le résumé apparaît sur la page des détails du plan et fournit des informations immédiates sur votre configuration.

Pour consulter le résumé d'un plan de sauvegarde

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup/>.
2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Choisissez le plan de sauvegarde que vous souhaitez revoir.
4. Le résumé du plan de sauvegarde apparaît sur la page des détails du plan. Développez le résumé pour voir les exécutions planifiées et les notes de compatibilité.

Vous pouvez également récupérer les informations du plan de sauvegarde à l'aide de AWS CLI :

```
aws backup get-backup-plan --backup-plan-id 012345678
```

Sélectionnez AWS les services à sauvegarder

Inscrivez-vous aux services, puis attribuez des ressources

AWS Backup fonctionne avec de nombreux [AWS services différents](#). Avant de décider quels services inclure dans le plan de sauvegarde, utilisez la [AWS Backup console](#) ou [AWS CLI](#) choisissez de les utiliser AWS Backup pour travailler avec ces services.

Ensuite, dans chaque plan de sauvegarde, spécifiez dans la [console](#) ou via la [CLI](#) les types de ressources à inclure dans ce plan.

Par exemple, vous pouvez opter pour tous les services compatibles, AWS Backup puis inclure uniquement les buckets Amazon S3 et les clusters Aurora dans un plan de sauvegarde.

Rubriques

- [AWS Backup inscription au service](#)
- [Affectation des ressources du plan de sauvegarde](#)
- [Attribuer des ressources à l'aide de la AWS Backup console](#)
- [Attribuez des ressources avec AWS CLI](#)
- [Attribuez AWS Backup des ressources via CloudFormation](#)
- [Quotas d'affectation des ressources du plan de sauvegarde](#)

AWS Backup inscription au service

Inscription au service via la console AWS Backup

Pour configurer les AWS services à utiliser avec AWS Backup

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Activation du service, choisissez Configurer les ressources.
4. Sur la page Configurer les ressources, utilisez les commutateurs pour activer ou désactiver les services utilisés avec AWS Backup. Choisissez Confirmer lorsque vos services sont configurés. Assurez-vous que le AWS service que vous choisissez est disponible dans votre Région AWS.

Inscription au service via AWS CLI

Utilisez la [aws backup update-region-settings](#) commande pour modifier les services (types de ressources) que votre compte ou votre organisation utilisera AWS Backup pour orchestrer la création de sauvegardes. Utilisez la [aws backup describe-region-settings](#) commande pour déterminer les services auxquels vous avez souscrit dans une région spécifique.

Affectation des ressources du plan de sauvegarde

Par le biais de la [AWS Backup console](#) ou par le biais de la console [AWS CLI](#), l'affectation des ressources dans votre plan de sauvegarde indique AWS Backup les ressources à inclure. AWS Backup fournit à la fois des paramètres par défaut simples et des contrôles précis pour affecter les ressources.

Vous pouvez affecter des ressources de différentes manières :

- Attribuer explicitement des types de ressources au plan de sauvegarde
- Inclure toutes les ressources (AWS Backup recherchera ensuite tous les types de ressources pris en charge)
- Utiliser des balises pour inclure ou exclure des ressources

Si vous n'utilisez des balises que pour l'attribution de ressources, les paramètres d'adhésion au service s'appliqueront toujours.

Vous pouvez affiner davantage l'attribution des ressources à l'aide de conditions et de balises. Certaines limites s'appliquent au nombre de ARNs conditions et de balises pouvant être utilisées dans le cadre d'une affectation de ressource unique.

La sélection des ressources par le biais de la CLI est basée sur les noms de service et les types de ressources. Voir [Attribuez des ressources avec AWS CLI](#) pour les considérations relatives au choix des ressources.

Attribuer des ressources à l'aide de la AWS Backup console

Pour accéder à la page Attribuer des ressources :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Choisissez Plans de sauvegarde.
3. Choisissez Créer un plan de sauvegarde.

4. Sélectionnez un modèle dans la liste déroulante Choisir un modèle, puis choisissez Créer un plan.
5. Saisissez un Nom du plan de sauvegarde.
6. Choisissez Créer un plan.
7. Choisissez Attribuer des ressources.

Pour commencer l'attribution des ressources dans la section Général :

1. Saisissez un Nom d'attribution de ressource.
2. Choisissez le Rôle par défaut ou Sélectionner un rôle IAM.

 Note

Si vous choisissez un rôle IAM, vérifiez qu'il dispose des autorisations nécessaires pour sauvegarder toutes les ressources que vous allez attribuer. Si votre rôle trouve une ressource qui n'est pas autorisée à sauvegarder, votre plan de sauvegarde échoue.

Pour attribuer vos ressources, dans la section Attribuer des ressources, choisissez l'une des deux options sous Définir la sélection des ressources :

- Inclure tous les types de ressources. Cette option configure votre plan de sauvegarde afin de protéger toutes les ressources AWS Backup prises en charge actuelles et futures attribuées à votre plan de sauvegarde. Utilisez cette option pour protéger rapidement et facilement votre parc de données.

Lorsque vous choisissez cette option, vous pouvez également Affiner la sélection à l'aide de balises à l'étape suivante.

- Inclure des types de ressources spécifiques. Lorsque vous choisissez cette option, vous devez Sélectionner des types de ressources spécifiques en suivant les étapes suivantes :
 1. À l'aide du menu déroulant Sélectionner des types de ressource, attribuez un ou plusieurs types de ressources.

Une fois que vous avez terminé, vous AWS Backup présente la liste des types de ressources que vous avez sélectionnés et son paramètre par défaut, qui est de protéger toutes les ressources pour chaque type de ressource sélectionné.

2. (Facultatif) Si vous souhaitez exclure des ressources spécifiques d'un type de ressource que vous avez sélectionné :
 1. Utilisez le menu déroulant Choisir des ressources et désélectionnez l'option par défaut.
 2. Sélectionnez les ressources spécifiques à attribuer à votre plan de sauvegarde.
3. Vous pouvez éventuellement exclure une ressource spécifique IDs des types de ressources sélectionnés. Utilisez cette option si vous souhaitez exclure une ou plusieurs ressources, car cela peut être plus rapide que de sélectionner de nombreuses ressources à l'étape précédente. Vous devez inclure un type de ressource avant de pouvoir exclure des ressources de ce type de ressource. Excluez un ID de ressource en procédant comme suit :
 1. Sous Exclure une ressource spécifique des types IDs de ressources sélectionnés, choisissez un ou plusieurs des types de ressources que vous avez inclus à l'aide de l'option Sélectionner les types de ressources.
 2. Pour chaque type de ressource, utilisez le menu Choisir les ressources pour sélectionner une ou plusieurs ressources à exclure.

Outre vos choix précédents, vous pouvez effectuer des sélections encore plus détaillées à l'aide de la fonctionnalité facultative Affiner la sélection à l'aide de balises. Cette fonctionnalité vous permet d'affiner votre sélection actuelle pour inclure un sous-ensemble de vos ressources à l'aide de balises.

Les balises sont des paires clé-valeur que vous pouvez attribuer à des ressources spécifiques pour vous aider à identifier, organiser et filtrer vos ressources. Les balises sont sensibles à la casse. Pour plus d'informations sur les balises, consultez la section [Marquage de vos AWS ressources](#).

Lorsque vous affinez votre sélection à l'aide de deux balises ou plus, l'effet est une condition AND. Par exemple, si vous affinez votre sélection à l'aide de deux balises, `env: prod` et `role: application`, vous attribuez uniquement des ressources comportant LES DEUX balises à votre plan de sauvegarde.

Pour affiner votre sélection à l'aide de balises :

1. Sous Affiner la sélection à l'aide de balises, choisissez une clé dans la liste.
2. Choisissez une condition pour la valeur dans la liste.
 - La Valeur fait référence à l'entrée suivante, la valeur de votre paire clé-valeur.

- La Condition peut être Equals, Contains, Begins with ou Ends with, ou leur inverse : Does not equal, Does not contain, Does not begin with ou Does not end with.
3. Choisissez une valeur dans la liste.
 4. Pour affiner davantage à l'aide d'une autre balise, choisissez Ajouter une balise.

Attribuez des ressources avec AWS CLI

Filtrer par services ou types de ressources

La sélection des ressources est basée sur les noms des services et les types de ressources. La méthode de sélection des ressources détermine si une ressource est incluse dans la sauvegarde. Cette inclusion dépend des noms des services, des types de ressources et des paramètres d'inscription.

Sélection par nom de service

Lorsque vous spécifiez uniquement un nom de service dans la sélection des ressources, l'inclusion de la sauvegarde dépend du paramètre d'opt-in pour les types de ressources sous-jacents. Par exemple, les EC2 instances avec `arn:aws:ec2:*`, ne seront incluses dans la sauvegarde que si le paramètre d'opt-in pour le type de EC2 ressource est activé.

Sélection par type de ressource

Si vous spécifiez la sélection de ressources directement avec le type de ressource, elle sera incluse dans la sauvegarde quel que soit le paramètre d'opt-in pour ce service en particulier. Par exemple, avec `arn:aws:ec2:::instance/*`, EC2 les instances seront sauvegardées quel que soit le paramètre d'opt-in.

Types de ressources partagées

Lorsque plusieurs ressources partagent le même type de ressource, vous devez activer les paramètres d'opt-in pour des types de ressources spécifiques afin de lancer des sauvegardes.

Exemple

Les clusters Aurora et RDS partagent le format ARN `arn:aws:rds:::cluster:*`. Pour sauvegarder les bases de données Aurora, vous devez activer le paramètre d'opt-in pour Aurora.

FSx et FSx pour OpenZFS, partagez le format ARN. `arn:aws:fsx::file-system/*` Activez les paramètres d'opt-in respectifs pour sauvegarder ces systèmes de fichiers.

Utiliser un JSON pour définir l'affectation des ressources du plan de sauvegarde

Vous pouvez définir une attribution de ressources dans un document JSON.

Vous pouvez spécifier des conditions, des balises ou des ressources pour définir ce qui sera inclus dans votre plan de sauvegarde. Pour plus d'informations qui vous aideront à déterminer les paramètres à inclure, consultez [BackupSelection](#).

Cet exemple d'attribution de ressources affecte toutes les EC2 instances Amazon au plan **BACKUP-PLAN-ID** de sauvegarde :

```
{
  "BackupPlanId": "BACKUP-PLAN-ID",
  "BackupSelection": {
    "SelectionName": "resources-list-selection",
    "IamRoleArn": "arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

En supposant que ce JSON est stocké sous le nom `backup-selection.json`, vous pouvez attribuer ces ressources à votre plan de sauvegarde à l'aide de la commande d'interface de ligne de commande suivante :

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

Vous trouverez ci-dessous des exemples d'attribution de ressources, ainsi que le document JSON correspondant. Pour faciliter la lecture de ce tableau, les exemples omettent les champs "BackupPlanId", "SelectionName" et "IamRoleArn". Le caractère générique `*` représente zéro ou plusieurs caractères autres que des espaces blancs.

Exemple Exemple : sélectionner toutes les ressources de mon compte

```
{
  "BackupSelection": {
```

```
    "Resources": [
      "*"
    ]
  }
}
```

Exemple Exemple : sélectionner toutes les ressources de mon compte, mais exclure les volumes EBS

```
{
  "BackupSelection": {
    "Resources": [
      "*"
    ],
    "NotResources": [
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Exemple Exemple : sélectionnez toutes les ressources étiquetées avec "backup": "true", mais excluez les volumes EBS

```
{
  "BackupSelection": {
    "Resources": [
      "*"
    ],
    "NotResources": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "aws:ResourceTag/backup",
          "ConditionValue": "true"
        }
      ]
    }
  }
}
```

⚠ Important

RDS, Aurora, Neptune et DocumentDB commencent ARNs par `arn:aws:rds:`. Affinez votre sélection à l'aide de balises et d'opérateurs conditionnels si vous n'avez pas l'intention d'inclure tous ces types.

Exemple Exemple : sélectionnez tous les volumes EBS et les instances de base de données RDS marqués avec les deux balises et `"backup":"true""stage":"prod"`

L'arithmétique booléenne est similaire à celle des politiques IAM, celles dans "Resources" étant combinées à l'aide d'une valeur booléenne OR et celles dans "Conditions" combinées avec une valeur booléenne ET.

L'expression `"Resources" "arn:aws:rds:*:*:db:*"` sélectionne uniquement les instances de base de données RDS, car il n'existe aucune ressource Aurora, Neptune ou DocumentDB correspondante.

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Exemple Exemple : sélectionnez tous les volumes EBS et les instances RDS marqués avec mais non "backup":"true" "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Exemple Exemple : sélectionnez toutes les ressources étiquetées avec "key1" et une valeur commençant par "include" mais pas par "key2" et une valeur contenant le mot "exclude"

Vous pouvez utiliser le caractère générique au début, à la fin et au milieu d'une chaîne. Notez l'utilisation du caractère générique (*) dans `include*` et `*exclude*` dans l'exemple ci-dessus. Vous pouvez également utiliser le caractère générique au milieu d'une chaîne, comme indiqué dans l'exemple précédent, `arn:aws:rds:*:*:db:*`.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
```



```

        "ConditionKey": "aws:ResourceTag/key1",
        "ConditionValue": "include*"
    }
],
"StringNotLike": [
    {
        "ConditionKey": "aws:ResourceTag/key2",
        "ConditionValue": "*exclude*"
    }
]
}
}
}
}

```

Exemple Exemple : sélectionnez toutes les ressources étiquetées avec, à "backup": "true" l'exception des systèmes de FSx fichiers et des ressources RDS, Aurora, Neptune et DocumentDB

Les éléments dans NotResources sont combinés à l'aide de la valeur booléenne OR.

```

{
  "BackupSelection": {
    "Resources": [
      "*"
    ],
    "NotResources": [
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "aws:ResourceTag/backup",
          "ConditionValue": "true"
        }
      ]
    }
  }
}
}

```

Exemple Exemple : sélectionnez toutes les ressources étiquetées avec un tag "backup" et une valeur quelconque

```

{

```

```

"BackupSelection":{
  "Resources":[
    "*"
  ],
  "Conditions":{
    "StringLike":[
      {
        "ConditionKey":"aws:ResourceTag/backup",
        "ConditionValue":"*"
      }
    ]
  }
}
}

```

Exemple Exemple : sélectionnez tous les systèmes de FSx fichiers, le cluster "my-aurora-cluster" Aurora et toutes les ressources étiquetées avec "backup":"true", à l'exception des ressources étiquetées avec "stage":"test"

```

{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}

```

Exemple Exemple : sélectionnez toutes les ressources étiquetées avec une balise, **"backup": "true"** à l'exception des volumes EBS étiquetés avec **"stage": "test"**

Utilisez deux commandes de l'interface de ligne de commande pour créer deux sélections afin de sélectionner ce groupe de ressources. La première sélection s'applique à toutes les ressources à l'exception des volumes EBS. La deuxième sélection s'applique aux volumes EBS.

```
{
  "BackupSelection": {
    "Resources": [
      "*"
    ],
    "NotResources": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "aws:ResourceTag/backup",
          "ConditionValue": "true"
        }
      ]
    }
  }
}
```

```
{
  "BackupSelection": {
    "Resources": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "aws:ResourceTag/backup",
          "ConditionValue": "true"
        }
      ],
      "StringNotEquals": [
        {
          "ConditionKey": "aws:ResourceTag/stage",
          "ConditionValue": "test"
        }
      ]
    }
  }
}
```

```

    }
  ]
}
}
}

```

Attribuez AWS Backup des ressources via CloudFormation

Ce end-to-end CloudFormation modèle crée une attribution de ressource, un plan de sauvegarde et un coffre de sauvegarde de destination :

- Un coffre de sauvegarde nommé *CloudFormationTestBackupVault*.
- Un plan de sauvegarde nommé *CloudFormationTestBackupPlan*. Ce plan exécutera deux règles de sauvegarde, qui effectuent toutes deux des sauvegardes tous les jours à midi (UTC) et les conservent pendant 210 jours.
- Une sélection de ressources nommée *BackupSelectionName*.
- L'attribution des ressources sauvegarde les ressources suivantes :
 - Toute ressource balisée avec la paire clé-valeur `backupplan:dsi-sandbox-daily`.
 - Toute ressource balisée avec la valeur `prod` ou des valeurs commençant par `prod/`.
- L'attribution des ressources ne sauvegarde pas les ressources suivantes :
 - Tout cluster RDS, Aurora, Neptune ou DocumentDB.
 - Toute ressource balisée avec la valeur `test` ou des valeurs commençant par `test/`.

Description: "Template that creates Backup Selection and its dependencies"

Parameters:

BackupVaultName:

Type: String

Default: "CloudFormationTestBackupVault"

BackupPlanName:

Type: String

Default: "CloudFormationTestBackupPlan"

BackupSelectionName:

Type: String

Default: "CloudFormationTestBackupSelection"

BackupPlanTagValue:

Type: String

Default: "test-value-1"

RuleName1:

```

    Type: String
    Default: "TestRule1"
RuleName2:
    Type: String
    Default: "TestRule2"
ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
StartWindowMinutes:
    Type: Number
    Default: 60
CompletionWindowMinutes:
    Type: Number
    Default: 120
RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays

```

```

    - RuleName: !Ref RuleName2
      TargetBackupVault: !Ref BackupVaultName
      ScheduleExpression: !Ref ScheduleExpression
      StartWindowMinutes: !Ref StartWindowMinutes
      CompletionWindowMinutes: !Ref CompletionWindowMinutes
      RecoveryPointTags:
        test-recovery-point-key-1: !Ref RecoveryPointTagValue
      Lifecycle:
        MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
        DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
      DependsOn: CloudFormationTestBackupVault

TestRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
    BasicBackupSelection:
      Type: 'AWS::Backup::BackupSelection'
      Properties:
        BackupPlanId: !Ref BasicBackupPlan
        BackupSelection:
          SelectionName: !Ref BackupSelectionName
          IamRoleArn: !GetAtt TestRole.Arn
          ListOfTags:
            - ConditionType: STRINGEQUALS
              ConditionKey: backupplan
              ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:

```

```
- ConditionKey: 'aws:ResourceTag/path'
  ConditionValue: prod
StringNotEquals:
- ConditionKey: 'aws:ResourceTag/path'
  ConditionValue: test
StringLike:
- ConditionKey: 'aws:ResourceTag/path'
  ConditionValue: prod/*
StringNotLike:
- ConditionKey: 'aws:ResourceTag/path'
  ConditionValue: test/*
```

Quotas d'affectation des ressources du plan de sauvegarde

Les quotas suivants s'appliquent à une seule attribution de ressources :

- 500 noms de ressources Amazon (ARNs) sans caractères génériques
- 30 ARNs avec des expressions génériques
- 30 conditions
- 30 balises par attribution de ressource (et un nombre illimité de ressources par balise)

Coffres-forts de sauvegarde

Dans AWS Backup, un coffre de sauvegarde est un conteneur qui stocke et organise vos sauvegardes.

Lorsque vous créez un coffre-fort de sauvegarde, vous devez spécifier la clé de chiffrement AWS Key Management Service (AWS KMS) qui chiffre certaines des sauvegardes placées dans ce coffre-fort. Le chiffrement des autres sauvegardes est géré par leurs AWS services sources. Pour plus d'informations sur le chiffrement, consultez le graphique dans [Chiffrement pour les sauvegardes dans AWS](#).

Les sections suivantes fournissent une vue d'ensemble de la gestion de vos coffres-forts de sauvegarde dans AWS Backup.

Rubriques

- [Création et suppression d'un coffre-fort de sauvegarde](#)
- [Coffre-fort à isolation logique](#)
- [Stratégies d'accès aux coffres](#)
- [AWS Backup Verrou de coffre-fort](#)

Création et suppression d'un coffre-fort de sauvegarde

Vous devez créer au moins un coffre-fort avant de créer un plan de sauvegarde ou de démarrer une tâche de sauvegarde.

Lorsque vous utilisez pour la première fois la page Backup Vaults de la AWS Backup console dans un Région AWS, la console crée automatiquement un coffre-fort par défaut pour la région.

Toutefois, si vous utilisez AWS Backup le AWS CLI AWS SDK ou CloudFormation, aucun coffre par défaut n'est créé. Vous devez créer votre propre coffre-fort.

Autorisations requises

Vous devez disposer des autorisations suivantes pour créer un coffre-fort de sauvegarde à l'aide de AWS Backup.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Sid": "AllowCreateBackupVault",
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:us-east-1:444455556666:backup-vault:*"
    },
    {
      "Sid": "AllowMountCapsule",
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

Création d'un coffre-fort de sauvegarde (console)

Au lieu d'utiliser le coffre-fort de sauvegarde par défaut qui est créé automatiquement pour vous sur la console AWS Backup, vous pouvez créer des coffres-forts de sauvegarde spécifiques pour enregistrer et organiser les groupes de sauvegardes dans le même coffre-fort.

Pour créer un coffre-fort de sauvegarde

1. Sur la AWS Backup console, dans le volet de navigation, sélectionnez Backup vaults.

Note

Si le volet de navigation n'est pas visible sur le côté gauche, vous pouvez l'ouvrir en choisissant l'icône du menu dans le coin supérieur gauche de la AWS Backup console.

2. Choisissez Create backup vault (Créer un coffre-fort de sauvegarde).
3. Saisissez un nom pour votre coffre-fort de sauvegarde. Le nom de votre coffre-fort peut refléter ce que vous allez y stocker, ou faciliter la recherche des sauvegardes dont vous avez besoin. Vous pouvez par exemple nommer le coffre-fort **FinancialBackups**.
4. Sélectionnez une touche AWS Key Management Service (AWS KMS). Vous pouvez utiliser une clé que vous avez déjà créée ou sélectionner la clé AWS Backup KMS par défaut.

Note

La AWS KMS clé spécifiée ici s'applique uniquement aux sauvegardes de services prenant en charge le chiffrement AWS Backup indépendant. Pour consulter la liste des types de ressources qui prennent en charge le chiffrement AWS Backup indépendant, consultez la section « AWS Backup Gestion complète » du [Disponibilité des fonctionnalités par ressource](#) tableau.

5. Vous pouvez également ajouter des balises qui vous aideront à rechercher et identifier vos coffres-forts de sauvegarde. Par exemple, vous pouvez ajouter une balise **BackupType:Financial**.
6. Choisissez Créer un coffre-fort de sauvegarde.
7. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde) et vérifiez que votre coffre-fort a été ajouté.

 Note

Vous pouvez maintenant modifier une règle de sauvegarde dans l'un de vos plans de sauvegarde, afin de stocker les sauvegardes créées par cette règle dans le coffre-fort de sauvegarde que vous venez de créer.

Création d'un coffre-fort de sauvegarde (par programmation)

La AWS Command Line Interface commande suivante crée un coffre de sauvegarde :

```
aws backup create-backup-vault --backup-vault-name test-vault
```

Vous pouvez également préciser les configurations suivantes pour un coffre-fort de sauvegarde.

Nom du coffre-fort de sauvegarde

Les noms des coffres-forts de sauvegarde sont sensibles à la casse. Ils doivent contenir entre 2 et 50 caractères alphanumériques, traits d'union ou traits de soulignement.

AWS KMS clé de chiffrement

La clé de AWS KMS chiffrement protège vos sauvegardes dans ce coffre de sauvegarde. Par défaut, AWS Backup crée une clé KMS pour vous avec l'alias `aws/backup`. Vous pouvez choisir cette clé ou n'importe quelle autre clé de votre compte (les clés KMS entre comptes peuvent être utilisées via l'interface de ligne de commande).

Vous pouvez créer une nouvelle clé de chiffrement en suivant la procédure [Création de clés](#) dans le Guide du développeur AWS Key Management Service .

Une fois que vous avez créé un coffre-fort de sauvegarde et défini la clé de AWS KMS chiffrement, vous ne pouvez plus modifier la clé de ce coffre-fort de sauvegarde.

La clé de chiffrement spécifiée dans un AWS Backup coffre s'applique aux sauvegardes de certains types de ressources. Pour plus d'informations sur le chiffrement des sauvegardes, consultez [Chiffrement pour les sauvegardes dans AWS Backup](#) dans la section Sécurité. Les sauvegardes de tous les autres types de ressources sont sauvegardées à l'aide de la clé utilisée pour chiffrer la ressource source.

Balises du coffre-fort de sauvegarde

Ces balises sont associées au coffre-fort de sauvegarde afin de vous aider à organiser et effectuer le suivi de votre coffre-fort de sauvegarde.

Suppression d'un coffre

Pour vous protéger contre les suppressions massives accidentelles ou malveillantes, vous ne pouvez supprimer un coffre-fort de sauvegarde dans AWS Backup qu'après avoir supprimé (ou après avoir supprimé le cycle de vie de votre plan de sauvegarde) tous les points de récupération de votre coffre-fort de sauvegarde. Pour supprimer vos points de récupération manuellement, consultez la section [Nettoyer les ressources](#).

Lorsque vous supprimez un coffre-fort de sauvegarde, mettez à jour vos plans de sauvegarde afin qu'ils pointent vers les nouveaux coffres-forts de sauvegarde. La création de la sauvegarde échoue si un plan de sauvegarde pointe vers un coffre-fort de sauvegarde supprimé.

Vous ne pouvez pas supprimer le coffre de sauvegarde par défaut ou le coffre de sauvegarde automatique Amazon EFS à l'aide du AWS Management Console. Vous pouvez supprimer un coffre de sauvegarde par défaut en utilisant le AWS CLI bouton s'il est vide. Toutefois, si vous ouvrez la AWS Backup console et sélectionnez cette région, la console recrée le coffre de sauvegarde par défaut. Vous pouvez supprimer les instantanés non utilisés dans le coffre de sauvegarde automatique Amazon EFS.

Pour supprimer un coffre-fort de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez le nom du coffre de sauvegarde pour ouvrir sa page de détails.
4. Choisissez et supprimer toutes les sauvegardes associées au coffre-fort de sauvegarde.
5. Choisissez Supprimer le coffre. Lorsque vous êtes invité à confirmer, entrez le nom du coffre-fort, puis choisissez Delete Backup vault.

Coffre-fort à isolation logique

Vue d'ensemble des coffres-forts à espacement logique

AWS Backup propose un type de coffre-fort secondaire qui permet de stocker les sauvegardes dans un conteneur doté de fonctionnalités de sécurité supplémentaires. Un coffre-fort logiquement isolé est un coffre-fort spécialisé qui offre une sécurité accrue par rapport à un coffre-fort de sauvegarde standard, ainsi que la possibilité de partager l'accès au coffre-fort avec d'autres comptes afin que les objectifs de temps de restauration (RTOs) puissent être plus rapides et plus flexibles en cas d'incident nécessitant une restauration rapide des ressources.

[Les coffres-forts hermétiques sont dotés de fonctionnalités de protection supplémentaires ; chaque coffre-fort est chiffré avec une clé AWS détenue \(par défaut\) ou éventuellement avec une clé KMS gérée par le client, et chaque coffre-fort est équipé AWS Backup du mode de conformité de Vault Lock.](#) Les informations relatives au type de clé de chiffrement sont visibles via AWS Backup APIs une console pour des raisons de transparence et de conformité.

Vous pouvez intégrer vos coffres-forts logiquement à l'[approbation multipartite](#) (MPA) pour permettre la restauration des sauvegardes présentes dans les coffres-forts même si le compte propriétaire du coffre-fort est inaccessible, ce qui contribue à maintenir la continuité des activités. [En outre, vous pouvez choisir de l'intégrer à AWS Resource Access Manager \(RAM\) pour partager un coffre-fort logiquement isolé avec d'autres AWS comptes \(y compris des comptes d'autres organisations\) afin que les sauvegardes stockées dans le coffre-fort puissent être restaurées à partir d'un compte avec lequel le coffre-fort est partagé, si nécessaire pour la récupération des données perdues ou les tests de restauration.](#) Dans le cadre de cette sécurité accrue, un coffre-fort isolé de manière logique stocke ses sauvegardes dans un compte appartenant au AWS Backup service (ce qui se traduit par des sauvegardes affichées comme partagées en dehors de votre organisation dans les éléments d'attribut de modification dans les journaux). AWS CloudTrail

Pour une meilleure résilience, nous vous recommandons de créer des copies interrégionales dans des coffres-forts logiquement espacés, dans des comptes identiques ou distincts. Toutefois, si vous souhaitez réduire les coûts de stockage en ne conservant qu'une seule copie, vous pouvez utiliser les [sauvegardes principales dans des coffres-forts espacés de manière logique](#), après avoir intégré MPA.

AWS

[Vous pouvez consulter les tarifs de stockage pour les sauvegardes des services pris en charge dans un coffre-fort isolé de manière logique sur la AWS Backup page de tarification.](#)

Consultez [Disponibilité des fonctionnalités par ressource](#) les types de ressources que vous pouvez copier dans un coffre-fort isolé de manière logique.

Rubriques

- [Cas d'utilisation pour les coffres-forts à espacement logique](#)
- [Comparaison et contraste avec un coffre-fort de sauvegarde standard](#)
- [Créez un coffre hermétique de manière logique](#)
- [Afficher les détails des coffres-forts ventilés de manière logique](#)
- [Création de sauvegardes dans un coffre-fort isolé de manière logique](#)
- [Partagez un coffre-fort isolé de manière logique](#)
- [Restaurez une sauvegarde à partir d'un coffre-fort isolé de manière logique](#)
- [Supprimer un coffre-fort isolé de manière logique](#)
- [Options programmatiques supplémentaires pour les coffres-forts à espacement logique](#)
- [Comprendre les types de clés de chiffrement pour les coffres-forts séparés de manière logique](#)
- [Résoudre un problème lié à un coffre hermétique](#)
- [Sauvegardes principales vers des coffres-forts à isolation logique](#)
- [Approbation multipartite pour les coffres-forts à espacement logique](#)

Cas d'utilisation pour les coffres-forts à espacement logique

Un coffre-fort à isolation logique est un coffre-fort secondaire qui fait partie d'une stratégie de protection des données. Ce coffre-fort peut aider à améliorer la stratégie de rétention et de restauration de votre entreprise lorsque vous souhaitez un coffre-fort pour vos sauvegardes qui

- Est automatiquement configuré avec un verrou de coffre-fort en [mode de conformité](#)
- Propose par défaut le chiffrement avec une clé AWS détenue. Vous pouvez éventuellement fournir une clé gérée par le client
- Contient des sauvegardes qui, via AWS RAM ou MPA, peuvent être partagées et restaurées à partir d'un compte différent de celui qui a créé la sauvegarde

Considérations et restrictions

- La copie entre régions vers ou depuis un coffre-fort logiquement espacé n'est actuellement pas disponible pour les sauvegardes contenant Amazon Aurora, Amazon DocumentDB et Amazon Neptune.
- Une sauvegarde contenant un ou plusieurs volumes Amazon EBS copiés dans un coffre-fort logiquement espacé doit être inférieure à 16 To ; les sauvegardes de plus grande taille pour ce type de ressource ne sont pas prises en charge.
- EC2 Offres Amazon [EC2 autorisées AMIs](#). Si ce paramètre est activé dans votre compte, ajoutez l'alias `aws-backup-vault` à votre liste d'autorisation.

Si cet alias n'est pas inclus, les opérations de copie d'un coffre-fort à espacement logique vers un coffre-fort de sauvegarde et les opérations de restauration des EC2 instances à partir d'un coffre-fort à espacement logique échoueront avec un message d'erreur tel que « AMI source ami-xxxxxx introuvable dans la région ».

- L'ARN (Amazon Resource Name) d'un point de récupération stocké dans un coffre-fort logiquement isolé remplacera le type backup de ressource sous-jacent. Par exemple, si l'ARN d'origine commence par `arn:aws:ec2:region::image/ami-*`, l'ARN du point de récupération dans le coffre à espacement logique sera `arn:aws:backup:region:account-id:recovery-point:*`

Vous pouvez utiliser la commande CLI [list-recovery-points-by-backup-vault](#) pour déterminer l'ARN.

Comparaison et contraste avec un coffre-fort de sauvegarde standard

Un coffre-fort de sauvegarde est le type de coffre-fort principal et standard utilisé dans AWS Backup. Chaque sauvegarde est stockée dans un coffre-fort de sauvegarde lors de sa création. Vous pouvez attribuer des politiques basées sur les ressources pour gérer les sauvegardes stockées dans le coffre-fort, telles que le cycle de vie des sauvegardes stockées dans le coffre-fort.

Un coffre-fort à isolation logique est un coffre-fort spécialisé offrant plus de sécurité et un partage flexible pour un délai de reprise (RTO) plus rapide. Ce coffre-fort stocke les sauvegardes principales ou des copies de sauvegardes initialement créées et stockées dans un coffre-fort de sauvegarde standard.

Les coffres-forts de sauvegarde sont chiffrés à l'aide d'une clé, un mécanisme de sécurité qui limite l'accès aux utilisateurs visés. Ces clés peuvent être gérées par le client ou AWS gérées. Reportez-

vous à la section [Chiffrement](#) des copies pour connaître le comportement du chiffrement lors des tâches de copie, notamment lors de la copie dans un coffre-fort séparé de manière logique.

En outre, un coffre-fort de sauvegarde peut être doté d'une sécurité supplémentaire grâce à un verrou de coffre-fort ; de manière logique, les coffres-forts ventilés sont équipés d'un verrou de coffre-fort en mode conformité.

À l'instar des coffres-forts de sauvegarde, les coffres-forts à espacement logique prennent également en charge les [balises](#) restreintes pour les sauvegardes Amazon. EC2

Fonctionnalité	Coffre-fort de sauvegarde	Coffre-fort à isolation logique
AWS Backup Audit Manager	Vous pouvez utiliser AWS Backup Audit Manager Contrôles et mesures correctives pour surveiller vos coffres-forts de sauvegarde.	Assurez-vous qu'une sauvegarde d'une ressource spécifique est stockée dans au moins un coffre-fort logiquement espacé selon un calendrier que vous déterminez, en plus des contrôles disponibles pour les coffres-forts standard.
Facturation	Les frais de stockage et de transfert de données pour les ressources entièrement gérées AWS Backup par sont indiqués sous « AWS Backup ». Des frais de stockage et de transfert de données pour d'autres types de ressources seront facturés dans le cadre de leurs services respectifs. Par exemple, les sauvegardes Amazon EBS apparaîtront sous « Amazon EBS » ; les sauvegardes Amazon S3	Tous les frais de facturation liés à ces coffres-forts (stockage ou transfert de données) sont indiqués sous « AWS Backup ».

Fonctionnalité	Coffre-fort de sauvegarde	Coffre-fort à isolation logique
	apparaîtront sous « »AWS Backup.	
Régions	Disponible dans toutes les régions dans lesquelles AWS Backup elle opère	Disponible dans la plupart des régions prises en charge par AWS Backup. Non disponible actuellement en Asie-Pacifique (Malaisie), au Canada Ouest (Calgary), au Mexique (Centre), en Asie-Pacifique (Thaïlande), en Asie-Pacifique (Taipei), en Asie-Pacifique (Nouvelle Zélande), en Chine (Pékin), en Chine (Ningxia), (USA Est) ou AWS GovCloud (USA Ouest). AWS GovCloud
Ressources	Peut stocker des copies de sauvegarde pour la plupart des types de ressources qui prennent en charge la copie entre comptes.	Consultez la colonne du coffre à espacement logique Disponibilité des fonctionnalités par ressource pour les ressources qui peuvent être copiées dans ce coffre-fort.
Restaurer	Les sauvegardes peuvent être restaurées par le même compte auquel appartient le coffre-fort.	Les sauvegardes peuvent être restaurées par un compte différent de celui auquel appartient le coffre-fort si celui-ci est partagé avec ce compte distinct.

Fonctionnalité	Coffre-fort de sauvegarde	Coffre-fort à isolation logique
<u>Sécurité</u>	(Facultatif) Peut être chiffré avec une clé (gérée par le client ou par AWS) Peut éventuellement utiliser un verrou de coffre-fort en mode conformité ou gouvernance	Peut être chiffré avec une cléAWS propre ou une clé gérée par le client Est toujours verrouillé à l'aide d'un verrouillage de coffre-fort en mode conformité Les informations sur le type de clé de chiffrement sont préservées et visibles lorsque les coffres-forts sont partagés via AWS RAM ou MPA
<u>Partage</u>	L'accès peut être géré via des politiques et AWS Organisations Non compatible avec AWS RAM	(Facultatif) Peut être partagé entre comptes avec AWS RAM

Créez un coffre hermétique de manière logique

Vous pouvez créer un coffre-fort isolé de manière logique soit par le biais de la AWS Backup console, soit à l'aide d'une combinaison de commandes et de la AWS Backup CLI AWS RAM .

Chaque appareil logiquement ventilé est équipé d'un verrou de coffre-fort en mode conformité. Consultez [AWS Backup Verrou de coffre-fort](#) pour vous aider à déterminer les valeurs de période de conservation les plus adaptées à votre activité

Console

Création d'un coffre-fort à isolation logique à partir de la console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, sélectionnez Coffres-forts.

3. Les deux types de coffres-forts s'affichent. Sélectionnez Créer un nouveau coffre-fort.
4. Saisissez un nom pour votre coffre-fort de sauvegarde. Le nom de votre coffre-fort peut refléter ce que vous allez y stocker, ou faciliter la recherche des sauvegardes dont vous avez besoin. Vous pouvez par exemple nommer le coffre-fort `FinancialBackups`.
5. Sélectionnez le bouton radio pour Logic AirGapped Vault.
6. (Facultatif) Choisissez une clé de chiffrement. Vous pouvez sélectionner une clé KMS gérée par le client pour un contrôle accru du chiffrement, ou utiliser la clé AWS détenue par défaut (recommandé).
7. Définissez la Période de conservation minimale.

Cette valeur (en jours, mois ou années) correspond à la durée la plus courte pendant laquelle une sauvegarde peut être conservée dans ce coffre-fort. Les sauvegardes dont la période de rétention est inférieure à cette valeur ne peuvent pas être copiées dans ce coffre-fort.

La valeur minimale autorisée est de 7 jours. Les valeurs pour les mois et les années respectent ce minimum.

8. Définissez la Période de conservation maximale.

Cette valeur (en jours, mois ou années) correspond à la durée la plus longue pendant laquelle une sauvegarde peut être conservée dans ce coffre-fort. Les sauvegardes dont la période de rétention est supérieure à cette valeur ne peuvent pas être copiées dans ce coffre-fort.

9. (Facultatif) Définissez la clé de chiffrement.

Spécifiez la clé à utiliser avec votre coffre-fort. Vous pouvez choisir une clé AWS détenue (gérée par AWS Backup) ou saisir l'ARN d'une clé gérée par le client qui appartient de préférence à un autre compte auquel vous avez accès. AWS Backup recommande d'utiliser une clé AWS détenue.

10. (Facultatif) Ajoutez des balises qui vous aideront à rechercher et à identifier votre coffre-fort à isolation logique. Par exemple, vous pouvez ajouter une balise `BackupType: Financial`.
11. Sélectionnez Créer un verrouillage de coffre.
12. Passez en revue les paramètres. Si tous les paramètres s'affichent comme prévu, sélectionnez Créer un coffre-fort logiquement isolé.
13. La console vous redirigera vers la page de détails de votre nouveau coffre-fort. Vérifiez que les détails du coffre-fort sont conformes aux attentes.

14. Sélectionnez Coffres-forts pour afficher les coffres-forts de votre compte. Votre coffre hermétique sera affiché de manière logique. La clé KMS sera disponible environ 1 à 3 minutes après la création du coffre-fort. Actualisez la page pour voir la clé associée. Une fois que la clé est visible, le coffre est disponible et peut être utilisé.

AWS CLI

Créez un coffre-fort isolé de manière logique à partir de la CLI

Vous pouvez l'utiliser AWS CLI pour effectuer des opérations de manière programmatique pour des coffres-forts à espacement logique. Chaque CLI est spécifique au AWS service dont elle provient. Les commandes liées au partage sont précédées par `aws ram` ; toutes les autres commandes doivent être précédées par `aws backup`.

Utilisez la commande CLI [create-logically-air-gapped-backup-vault](#), modifiée avec les paramètres suivants :

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1 // optional
--backup-vault-name sampleName // required
--min-retention-days 7 // required Value must be an integer 7 or greater
--max-retention-days 35 // required
--encryption-key-arn arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012 // optional
--creator-request-id 123456789012-34567-8901 // optional
```

Le `--encryption-key-arn` paramètre facultatif vous permet de spécifier une clé KMS gérée par le client pour le chiffrement du coffre-fort. Si elle n'est pas fournie, le coffre-fort utilisera une clé AWS appartenant à l'utilisateur.

Exemple de commande CLI pour créer un coffre-fort isolé de manière logique :

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1
--backup-vault-name sampleName
--min-retention-days 7
--max-retention-days 35
--creator-request-id 123456789012-34567-8901 // optional
```

Exemple de commande CLI pour créer un coffre-fort isolé de manière logique avec un chiffrement géré par le client :

```
aws backup create-logically-air-gapped-backup-vault
--region us-east-1
--backup-vault-name sampleName
--min-retention-days 7
--max-retention-days 35
--encryption-key-arn arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012
--creator-request-id 123456789012-34567-8901 // optional
```

Consultez les [éléments de réponse de l>CreateLogicallyAirGappedBackupVault API](#) pour plus d'informations après l'opération de création. Si l'opération est réussie, le nouveau coffre logiquement espacé portera le code de. VaultState CREATING

Une fois la création terminée et la clé cryptée KMS attribuée, la VaultState transition vers AVAILABLE. Une fois disponible, le coffre peut être utilisé. VaultState peut être récupéré en appelant [DescribeBackupVault](#) ou [ListBackupVaults](#).

Afficher les détails des coffres-forts ventilés de manière logique

Vous pouvez consulter les détails du coffre tels que le résumé, les points de récupération, les ressources protégées, le partage de compte, la politique d'accès et les balises via la AWS Backup console ou la AWS Backup CLI.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.
3. Sous les descriptions des coffres-forts figurent trois listes : les coffres-forts créés par ce compte, les coffres-forts partagés via la RAM et les coffres-forts accessibles via une approbation multipartite. Sélectionnez l'onglet souhaité pour afficher les coffres-forts.
4. Sous Nom du coffre-fort, cliquez sur le nom du coffre-fort pour ouvrir la page de détails. Vous pouvez consulter le résumé, les points de récupération, les ressources protégées, le partage de compte, la stratégie d'accès et les détails des balises.

Les détails s'affichent en fonction du type de compte : les comptes qui possèdent un coffre-fort peuvent consulter le partage des comptes ; les comptes qui ne possèdent pas de coffre-fort ne pourront pas consulter le partage de compte. Pour les coffres-forts partagés, le type

de clé de chiffrement (clé KMS AWS détenue ou gérée par le client) est affiché dans le résumé du coffre-fort.

AWS CLI

Afficher les détails d'un coffre-fort isolé de manière logique via la CLI

La commande CLI [describe-backup-vault](#) peut être utilisée pour obtenir des informations sur un coffre. Le paramètre `backup-vault-name` est obligatoire ; `region` il est facultatif.

```
aws backup describe-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

Exemple de réponse :

```
{
  "BackupVaultName": "LOG-AIR-GAP-VAULT-TEST",
  "BackupVaultArn": "arn:aws:backup:us-east-1:234567890123:backup-vault:IAD-LAGV-01",
  "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
  "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
  "CreationDate": "2024-07-25T16:05:23.554000-07:00",
  "NumberOfRecoveryPoints": 0,
  "Locked": true,
  "MinRetentionDays": 8,
  "MaxRetentionDays": 30,
  "LockDate": "2024-07-25T16:05:23.554000-07:00"
}
```

Création de sauvegardes dans un coffre-fort isolé de manière logique

Logiquement, les coffres-forts ventilés peuvent être la cible d'une tâche de copie dans un plan de sauvegarde ou une cible pour une tâche de copie à la demande. Il peut également être utilisé comme cible de sauvegarde principale. Consultez la section [Sauvegardes principales vers des coffres-forts séparés de manière logique](#).

Chiffrement compatible

Une tâche de copie réussie d'un coffre-fort de sauvegarde vers un coffre-fort logiquement isolé nécessite une clé de chiffrement déterminée par le type de ressource copié.

Lorsque vous créez ou copiez une sauvegarde d'un [type de ressource entièrement géré](#), la ressource source peut être chiffrée par une clé gérée par le client ou par une clé AWS gérée.

Lorsque vous créez ou copiez une sauvegarde d'autres types de ressources (celles qui [ne sont pas entièrement gérées](#)), la source doit être chiffrée à l'aide d'une clé gérée par le client. AWS les clés gérées pour les ressources non entièrement gérées ne sont pas prises en charge.

Créez ou copiez des sauvegardes dans un coffre-fort isolé de manière logique par le biais d'un plan de sauvegarde

Vous pouvez copier une sauvegarde (point de restauration) d'un coffre-fort de sauvegarde standard vers un coffre-fort isolé de manière logique en [créant un nouveau plan de sauvegarde ou en mettant à jour un plan existant](#) dans la AWS Backup console ou via les AWS CLI commandes et [create-backup-planupdate-backup-plan](#). Vous pouvez également créer des sauvegardes directement dans un coffre-fort isolé de manière logique en l'utilisant comme cible principale. Pour plus de détails, reportez-vous [à la section Sauvegardes principales vers des coffres-forts séparés de manière logique](#).

Vous pouvez copier une sauvegarde d'un coffre-fort logiquement espacé vers un autre coffre-fort logiquement espacé à la demande (ce type de sauvegarde ne peut pas être planifié dans un plan de sauvegarde). Vous pouvez copier une sauvegarde d'un coffre-fort isolé de manière logique vers un coffre-fort de sauvegarde standard, à condition que la copie soit chiffrée à l'aide d'une clé gérée par le client.

Copie de sauvegarde à la demande vers un coffre-fort isolé de manière logique

Pour créer une copie unique [à la demande](#) d'une sauvegarde dans un coffre-fort logiquement isolé, vous pouvez effectuer une copie à partir d'un coffre-fort de sauvegarde standard. Des copies entre régions ou entre comptes sont disponibles si le type de ressource prend en charge le type de copie.

Disponibilité des copies

Une copie d'une sauvegarde peut être créée à partir du compte auquel appartient le coffre-fort. Les comptes avec lesquels le coffre a été partagé ont la possibilité de consulter ou de restaurer une sauvegarde, mais pas d'en créer une copie.

Seuls les [types de ressources prenant en charge la copie entre régions ou entre comptes](#) peuvent être inclus.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.
3. Sur la page détaillée du coffre-fort, tous les points de récupération de ce coffre-fort sont affichés. Cochez la case à côté du point de récupération que vous souhaitez copier.
4. Puis sélectionnez Actions et Copier dans le menu déroulant.
5. Sur l'écran suivant, saisissez les détails de la destination.
 - a. Spécifiez la région de destination.
 - b. Le menu déroulant du coffre-fort de sauvegarde de destination affiche les coffres-forts de destination éligibles. Sélectionnez-en un avec le type `logically air-gapped vault`
6. Sélectionnez Copier une fois que tous les détails sont définis selon vos préférences.

Sur la page Tâches de la console, vous pouvez sélectionner des tâches de copie pour voir les tâches de copie en cours.

AWS CLI

Utilisez [start-copy-job](#) pour copier une sauvegarde existante dans un coffre-fort de sauvegarde vers un coffre-fort à isolation logique.

Exemple d'entrée de l'interface de ligne de commande :

```
aws backup start-copy-job
--region us-east-1
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567
--source-backup-vault-name sourcevaultname
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-vault:destinationvaultname
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

Pour plus d'informations, consultez [Copie d'une sauvegarde](#), [Sauvegarde entre régions](#) et [Sauvegarde entre comptes](#).

Partagez un coffre-fort isolé de manière logique

Vous pouvez utiliser AWS Resource Access Manager (RAM) pour partager un coffre-fort logiquement séparé avec d'autres comptes que vous désignez. Lors du partage de coffres-forts, les informations relatives au type de clé de chiffrement (clé KMS AWS détenue ou gérée par le client) sont préservées et visibles pour les comptes avec lesquels le coffre-fort est partagé.

Un coffre-fort peut être partagé avec un compte de son organisation ou avec un compte d'une autre organisation. Le coffre-fort ne peut pas être partagé avec l'ensemble d'une organisation, mais uniquement avec des comptes au sein de l'organisation.

Seuls les comptes dotés de privilèges IAM spécifiques peuvent partager et gérer le partage de coffres-forts.

Pour partager en utilisant AWS RAM, assurez-vous de disposer des éléments suivants :

- Deux comptes ou plus pouvant accéder AWS Backup
- Le compte propriétaire du coffre-fort qui a l'intention de partager dispose des autorisations de RAM nécessaires. L'autorisation `ram:CreateResourceShare` est nécessaire pour cette procédure. La politique `AWSResourceAccessManagerFullAccess` contient toutes les autorisations nécessaires liées à la RAM :
 - `backup:DescribeBackupVault`
 - `backup:DescribeRecoveryPoint`
 - `backup:GetRecoveryPointRestoreMetadata`
 - `backup:ListProtectedResourcesByBackupVault`
 - `backup:ListRecoveryPointsByBackupVault`
 - `backup:ListTags`
 - `backup:StartRestoreJob`
- Au moins un coffre-fort à isolation logique

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.

3. Sous les descriptions des coffres-forts figurent deux listes, Coffres-forts appartenant à ce compte et Coffres-forts partagés avec ce compte. Les coffres-forts appartenant au compte peuvent être partagés.
4. Sous Nom du coffre-fort, cliquez sur le nom du coffre-fort à isolation logique pour ouvrir la page de détails.
5. Le volet Partage de comptes indique avec quels comptes le coffre-fort est partagé.
6. Pour commencer à partager avec un autre compte ou pour modifier des comptes déjà partagés, sélectionnez Gérer le partage.
7. La AWS RAM console s'ouvre lorsque l'option Gérer le partage est sélectionnée. Pour savoir comment partager une ressource à l'aide de la AWS RAM, reportez-vous à la section [Création d'un partage de ressources dans la AWS RAM](#) dans le Guide de l'utilisateur de la AWS RAM.
8. Le compte invité à accepter une invitation afin de recevoir un partage dispose de 12 heures pour accepter l'invitation. Consultez [Acceptation et rejet des invitations de partage de ressources](#) dans le Guide de l'utilisateur AWS RAM.
9. Si les étapes de partage sont terminées et acceptées, la page récapitulative du coffre-fort s'affichera sous Partage de compte = « Partagé – voir le tableau de partage de compte ci-dessous ».

AWS CLI

AWS RAM utilise la commande CLI `create-resource-share`. L'accès à cette commande n'est disponible que pour les comptes disposant d'autorisations suffisantes. Consultez [Création d'un partage de ressources dans AWS RAM](#) pour les étapes de l'interface de ligne de commande.

Les étapes 1 à 4 sont effectuées avec le compte propriétaire du coffre-fort à isolation logique. Les étapes 5 à 8 sont effectuées avec le compte avec lequel le coffre-fort à isolation logique sera partagé.

1. Connectez-vous au compte propriétaire OU demandez à un utilisateur de votre organisation disposant d'informations d'identification suffisantes d'accéder au compte source afin d'effectuer ces étapes.
 - Si un partage de ressources a déjà été créé et que vous souhaitez y ajouter une ressource supplémentaire, utilisez plutôt la commande `associate-resource-share` de l'interface de ligne de commande avec l'ARN du nouveau coffre-fort.

2. Récupérez les informations d'identification d'un rôle disposant d'autorisations suffisantes pour les partager via RAM. [Saisissez-les dans l'interface de ligne de commande](#).
 - L'autorisation `ram:CreateResourceShare` est nécessaire pour cette procédure. La politique [AWSResourceAccessManagerFullAccess](#) contient toutes les autorisations liées à la RAM.
3. Utilisez [create-resource-share](#).
 - a. Incluez l'ARN du coffre-fort à isolation logique.
 - b. Exemple d'entrée :

```
aws ram create-resource-share
--name MyLogicallyAirGappedVault
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
--principals 123456789012
--region us-east-1
```

- c. Exemple de sortie :

```
{
  "resourceShare":{
    "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
    "name":"MyLogicallyAirGappedVault",
    "owningAccountId":"123456789012",
    "allowExternalPrincipals":true,
    "status":"ACTIVE",
    "creationTime":"2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
  }
}
```

4. Copiez l'ARN du partage de ressources dans la sortie (nécessaire pour les étapes suivantes). Donnez l'ARN à l'opérateur du compte que vous invitez à recevoir le partage.
5. Obtenir l'ARN du partage de ressources
 - a. Si vous n'avez pas effectué les étapes 1 à 4, obtenez-les auprès `resourceShareArn` de la personne qui l'a fait.

- b. Exemple : `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`
6. Dans l'interface de ligne de commande, utilisez les informations d'identification du compte du destinataire.
7. Recevez une invitation à partager des ressources avec [get-resource-share-invitations](#). Pour plus d'informations, consultez [Acceptation et refus des invitations](#) dans le Guide de l'utilisateur AWS RAM .
8. Acceptez l'invitation sur le compte de destination (de récupération).
 - Utiliser [accept-resource-share-invitation](#) (ou également [reject-resource-share-invitation](#)).

Vous pouvez utiliser les commandes AWS RAM CLI pour afficher les éléments partagés :

- Ressources que vous avez partagées :

```
aws ram list-resources --resource-owner SELF --resource-type  
backup:backup-vault --region us-east-1
```

- Afficher le principal :

```
aws ram get-resource-share-associations --association-type PRINCIPAL  
--region us-east-1
```

- Ressources partagées par d'autres comptes :

```
aws ram list-resources --resource-owner OTHER-ACCOUNTS --resource-type  
backup:backup-vault --region us-east-1
```

Restaurez une sauvegarde à partir d'un coffre-fort isolé de manière logique

Vous pouvez restaurer une sauvegarde stockée dans un coffre-fort isolé de manière logique à partir du compte propriétaire du coffre-fort ou de tout compte avec lequel le coffre-fort est partagé.

[Reportez-vous à la section Restauration d'une sauvegarde](#) pour savoir comment restaurer un point de restauration via la AWS Backup console.

Une fois qu'une sauvegarde a été partagée depuis un coffre-fort logiquement isolé vers votre compte, vous pouvez l'utiliser [start-restore-job](#) pour la restaurer.

Un exemple d'entrée CLI peut inclure la commande et les paramètres suivants :

```
aws backup start-restore-job
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID
--metadata {"availabilityzone\\":\\"us-east-1d\\"}
--idempotency-token TokenNumber
--resource-type ResourceType
--iam-role arn:aws:iam::number:role/service-role/servicerole
--region us-east-1
```

Supprimer un coffre-fort isolé de manière logique

Consultez la section [Supprimer un coffre-fort](#). Les coffres-forts ne peuvent pas être supprimés s'ils contiennent encore des sauvegardes (points de récupération). Assurez-vous que le coffre-fort ne contient aucune sauvegarde avant de lancer une opération de suppression.

La suppression d'un coffre-fort entraîne également la suppression de la clé associée au coffre-fort sept jours après sa suppression, conformément à la politique de suppression des clés.

L'exemple de commande de l'interface de ligne de commande suivant [delete-backup-vault](#) peut être utilisé pour supprimer un coffre-fort.

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

Options programmatiques supplémentaires pour les coffres-forts à espacement logique

La commande [list-backup-vaults](#) de l'interface de ligne de commande peut être modifiée pour répertorier tous les coffres-forts détenus par le compte et présents dans celui-ci :

```
aws backup list-backup-vaults
--region us-east-1
```

Pour répertorier uniquement les coffres-forts à isolation logique, ajoutez le paramètre

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Incluez le paramètre `by-shared` permettant de filtrer la liste renvoyée des coffres-forts afin d'afficher uniquement les coffres-forts partagés logiquement espacés. La réponse inclura les informations relatives au type de clé de chiffrement pour chaque coffre-fort partagé.

```
aws backup list-backup-vaults
--region us-east-1
--by-shared
```

Exemple de réponse indiquant les informations relatives au type de clé de chiffrement :

```
{
  "BackupVaultList": [
    {
      "BackupVaultName": "shared-logically air-gapped-vault",
      "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:shared-logically air-gapped-vault",
      "VaultType": "LOGICALLY_AIR_GAPPED_BACKUP_VAULT",
      "EncryptionKeyType": "AWS_OWNED_KMS_KEY",
      "CreationDate": "2024-07-25T16:05:23.554000-07:00",
      "Locked": true,
      "MinRetentionDays": 7,
      "MaxRetentionDays": 30
    }
  ]
}
```

Comprendre les types de clés de chiffrement pour les coffres-forts séparés de manière logique

Les coffres-forts à espacement logique prennent en charge différents types de clés de chiffrement, et ces informations sont visibles via la console. AWS Backup APIs Lorsque les coffres-forts sont partagés via AWS RAM MPA, les informations relatives au type de clé de chiffrement sont préservées et rendues visibles aux comptes avec lesquels le coffre-fort est partagé. Cette transparence vous aide à comprendre la configuration de chiffrement des coffres-forts et à prendre des décisions éclairées concernant les opérations de sauvegarde et de restauration.

Valeurs des types de clés de chiffrement

Le `EncryptionKeyType` champ peut avoir les valeurs suivantes :

- **AWS_OWNED_KMS_KEY**- Le coffre-fort est chiffré à l'aide d'une clé AWS appartenant à l'utilisateur. Il s'agit de la méthode de chiffrement par défaut pour les coffres-forts séparés de manière logique lorsqu'aucune clé gérée par le client n'est spécifiée.
- **CUSTOMER_MANAGED_KMS_KEY**- Le coffre-fort est chiffré à l'aide d'une clé KMS gérée par le client que vous contrôlez. Cette option fournit un contrôle supplémentaire sur les clés de chiffrement et les politiques d'accès.

Note

- AWS Backup recommande d'utiliser des clés AWS détenues dans des coffres-forts séparés de manière logique. Toutefois, si la politique de votre entreprise exige l'utilisation d'une clé gérée par le client, il est recommandé d'utiliser les clés d'un autre compte d'une organisation secondaire dédiée à la restauration. Vous pouvez consulter le blog [Encrypt AWS Backup sur des coffres-forts à espacement logique avec des clés gérées par le client pour obtenir plus d'informations sur la configuration de coffres-forts à espacement logique basés sur CMK](#).
- Vous ne pouvez sélectionner une clé de chiffrement AWS KMS que lors de la création du coffre-fort. Une fois créées, toutes les sauvegardes contenues dans le coffre seront chiffrées avec cette clé. Vous ne pouvez pas modifier ou migrer vos coffres-forts pour utiliser une autre clé de chiffrement.

Politique clé pour la création de coffres-forts chiffrés et logiquement espacés par CMK

Lorsque vous créez un coffre-fort isolé de manière logique à l'aide d'une clé gérée par le client, vous devez appliquer la politique `AWSBackupFullAccess` de AWS gestion gérée au rôle de votre compte. Cette politique inclut des `Allow` actions qui permettent AWS Backup d'interagir avec AWS KMS les clés KMS pour créer des autorisations lors des opérations de sauvegarde, de copie et de stockage. En outre, vous devez vous assurer que votre politique de clé gérée par le client (si elle est utilisée) inclut les autorisations spécifiques requises.

- La clé CMK doit être partagée avec le compte sur lequel se trouve le coffre logiquement isolé

```
{  
  "Sid": "Allow use of the key to create a logically air-gapped vault",  
  "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "arn:aws:iam::[account-id]:role/TheRoleToAccessAccount"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "backup.*.amazonaws.com"
      }
    }
  }
}

```

Politique clé en matière de copie/restauration

Pour éviter les échecs, passez en revue votre politique AWS KMS clé pour vous assurer qu'elle inclut toutes les autorisations requises et qu'elle ne contient aucune déclaration de refus susceptible de bloquer les opérations. Les conditions suivantes s'appliquent :

- Pour tous les scénarios de copie, le CMKs doit être partagé avec le rôle de copie source

```

{
  "Sid": "Allow use of the key for copy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole"    //[Source copy role]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "backup.*.amazonaws.com"
    }
  }
}

```



```

    }
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole" //[Source copy role]
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      },
      "StringLike": {
        "kms:ViaService": "backup.*.amazonaws.com"
      }
    }
  }
}

```

- Lors de la copie d'un coffre-fort crypté CMK logiquement espacé vers un coffre-fort de sauvegarde, la clé CMK doit également être partagée avec le compte SLR de destination

```

{
  "Sid": "Allow use of the key for copy from a CMK encrypted logically air-gapped
vault to normal backup vault",
  "Effect": "Allow",
  "Principal": {
    "AWS": ["arn:aws:iam::[source-account-id]:role/service-role/
AWSBackupDefaultServiceRole",      //[Source copy role]
           "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"], //[Destination SLR]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::[source-account-id]:role/service-role/AWSBackupDefaultServiceRole", // [Source copy role]
        "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup", // [Destination SLR]
      ],
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  }
}

```

- Lors de la copie ou de la restauration à partir d'un compte de récupération à l'aide d'un coffre-fort RAM/MPA partagé logiquement séparé

```

{
  "Sid": "Allow use of the key for copy/restore from a recovery account",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::[recovery-account-id]:role/service-role/AWSBackupDefaultServiceRole", // [Recovery account copy/restore role]
      "arn:aws:iam::[destination-account-id]:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup" // [Destination SLR]
    ],
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
}

```

```

    "Resource": "*"
  },
  {
    "Sid": "Allow AWS Backup to create grant on the key for copy",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam::[recovery-account-id]:role/service-role/
AWSBackupDefaultServiceRole" // [Recovery account copy/restore role]
            "arn:aws:iam::[destination-account-id]:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup"], // [Destination SLR]
    },
    "Action": [
      "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  }
}

```

IAM Role

Lorsqu'ils effectuent des opérations de copie de coffres-forts logiquement espacées, les clients peuvent utiliser `AWSBackupDefaultServiceRole` ce qui inclut la AWS politique de gestion. `AWSBackupServiceRolePolicyForBackup` Toutefois, si les clients préfèrent mettre en œuvre une approche de politique du moindre privilège, leur politique IAM doit inclure une exigence spécifique :

- Le rôle de copie du compte source doit disposer d'autorisations d'accès à la fois à la source et à la destination CMKs.

```

{
  "Version": "2012-10-17"
  ,
  "Statement": [
    {
      "Sid": "KMSPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",

```

```

        "Resource": [
            "arn:aws:kms:*: [source-account-id]:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*: [destination-account-id]:key/*". - Destination
logically air-gapped vault CMK -
        ]
    },
    {
        "Sid": "KMSCreateGrantPermissions",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": [
            "arn:aws:kms:*: [source-account-id]:key/*", - Source logically air-
gapped vault CMK -
            "arn:aws:kms:*: [destination-account-id]:key/*". - Destination
logically air-gapped vault CMK -
        ]
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
]
}

```

Par conséquent, l'une des erreurs les plus courantes des clients se produit lors de la copie lorsque les clients ne fournissent pas les autorisations suffisantes sur leurs rôles CMKs et sur les rôles de copie.

Affichage des types de clés de chiffrement

Vous pouvez consulter les informations relatives au type de clé de chiffrement à la fois par le biais de la AWS Backup console et par programmation à l'aide du AWS CLI ou. SDKs

Console : lorsque vous visualisez des coffres-forts séparés de manière logique dans la AWS Backup console, le type de clé de chiffrement est affiché sur la page des détails du coffre-fort, sous la section des informations de sécurité.

AWS CLI/API : le type de clé de chiffrement est renvoyé en réponse aux opérations suivantes lors de l'interrogation de coffres-forts espacés de manière logique :

- `list-backup-vaults`(y compris `--by-shared` pour les coffres-forts partagés)

- `describe-backup-vault`
- `describe-recovery-point`
- `list-recovery-points-by-backup-vault`
- `list-recovery-points-by-resource`

Considérations relatives au chiffrement des coffres-forts

Lorsque vous travaillez avec des coffres-forts séparés de manière logique et des types de clés de chiffrement, tenez compte des points suivants :

- Sélection de la clé lors de la création : vous pouvez éventuellement spécifier une clé KMS gérée par le client lors de la création d'un coffre-fort logiquement espacé. Si elle n'est pas spécifiée, une clé AWS appartenant à l'utilisateur sera utilisée.
- Visibilité du coffre-fort partagé : les comptes avec lesquels un coffre-fort est partagé peuvent voir le type de clé de chiffrement mais ne peuvent pas modifier la configuration du chiffrement.
- Informations sur les points de récupération : le type de clé de chiffrement est également disponible lors de l'affichage des points de restauration dans des coffres-forts séparés de manière logique.
- Opérations de restauration : la compréhension du type de clé de chiffrement vous aide à planifier les opérations de restauration et à comprendre les éventuels besoins d'accès.
- Conformité : les informations relatives au type de clé de chiffrement répondent aux exigences en matière de rapports de conformité et d'audit en fournissant une transparence quant aux méthodes de chiffrement utilisées pour les données de sauvegarde.

Résoudre un problème lié à un coffre hermétique

Si vous rencontrez des erreurs au cours de votre flux de travail, consultez les exemples d'erreurs suivants et les solutions suggérées :

AccessDeniedException

Erreur: An error occurred (AccessDeniedException) when calling the `[command]` operation: Insufficient privileges to perform this action."

Cause possible : Le paramètre `--backup-vault-account-id` a pas été inclus lorsque l'une des requêtes suivantes a été exécutée sur un coffre partagé par RAM :

- `describe-backup-vault`

- `describe-recovery-point`
- `get-recovery-point-restore-metadata`
- `list-protected-resources-by-backup-vault`
- `list-recovery-points-by-backup-vault`

Solution : Réessayez la commande qui a renvoyé l'erreur, mais incluez le paramètre `--backup-vault-account-id` qui indique le compte propriétaire du coffre-fort.

OperationNotPermittedException

Erreur : `OperationNotPermittedException` est renvoyé après un `CreateResourceShare` appel.

Cause possible : si vous avez tenté de partager une ressource, telle qu'un coffre-fort isolé de manière logique, avec une autre organisation, vous pouvez obtenir cette exception. Un coffre-fort peut être partagé avec un compte d'une autre organisation, mais il ne peut pas être partagé avec l'autre organisation elle-même.

Solution : Réessayez l'opération, mais spécifiez un compte comme valeur au principaux lieu d'une organisation ou d'une unité d'organisation.

Type de clé de chiffrement non affiché

Problème : le type de clé de chiffrement n'est pas visible lorsque vous consultez un coffre-fort isolé de manière logique ou ses points de récupération.

Causes possibles :

- Vous consultez un ancien coffre-fort créé avant l'ajout de la prise en charge des types de clés de chiffrement
- Vous utilisez une ancienne version du SDK AWS CLI or
- La réponse de l'API n'inclut pas le champ de type de clé de chiffrement

Résolution :

- Mettez AWS CLI à jour votre version
- Pour les anciens coffres-forts, le type de clé de chiffrement sera renseigné automatiquement et devrait apparaître dans les appels d'API suivants

- Vérifiez que vous utilisez les opérations d'API correctes qui renvoient des informations sur le type de clé de chiffrement
- Pour les coffres-forts partagés, vérifiez que le coffre-fort est correctement partagé via AWS Resource Access Manager

« ÉCHEC » VaultState AccessDeniedException dans les CloudTrail journaux

Erreur dans CloudTrail : "User: <assumed role> is not authorized to perform: kms:CreateGrant on this resource because the resource does not exist in this Region, no resource-based policies allow access, or a resource-based policy explicitly denies access"

Causes possibles :

- Le coffre-fort a été créé à l'aide d'une clé gérée par le client, mais le rôle assumé n'est pas CreateGrant autorisé par la politique de clé requise pour utiliser la clé pour la création du coffre-fort

Résolution :

- Accordez les autorisations spécifiées dans la [the section called “Politique clé pour la création de coffres-forts chiffrés et logiquement espacés par CMK”](#) section, puis réessayez le processus de création du coffre-fort.

Sauvegardes principales vers des coffres-forts à isolation logique

Aperçu

La fonction de sauvegarde principale du coffre-fort logiquement espacé vous permet de spécifier un coffre-fort logiquement espacé comme destination de sauvegarde principale au sein du même compte, pour les tâches de sauvegarde planifiées et à la demande. Il n'est donc plus nécessaire de conserver des copies séparées à la fois dans un coffre-fort de sauvegarde standard et dans un coffre-fort à espacement logique, ce qui réduit les coûts et simplifie les flux de travail tout en préservant les avantages de sécurité liés à l'espacement logique.

Vous pouvez attribuer un coffre-fort logiquement isolé comme cible principale dans les plans de sauvegarde, les politiques à l'échelle de l'entreprise ou les sauvegardes à la demande. Auparavant, pour effectuer une sauvegarde dans un coffre-fort à espacement logique, vous deviez d'abord créer

une sauvegarde dans un coffre-fort de sauvegarde, puis la copier dans un coffre-fort à espacement logique. Cette fonctionnalité permet, selon le type de ressource, de AWS Backup créer des sauvegardes directement dans votre coffre-fort logiquement espacé ou de gérer automatiquement des sauvegardes temporaires qui sont copiées dans votre coffre-fort logiquement espacé puis supprimées.

Le comportement dépend de deux facteurs :

- Si le type de ressource est pris en charge par un coffre-fort à espacement logique.
- Si le type de ressource prend en charge [AWS Backup la gestion complète](#).

Warning

Nous vous recommandons d'intégrer vos coffres-forts à espacement logique avec l'[approbation multipartite](#) (MPA) si vous optez pour cette fonctionnalité. Cela permet de récupérer les sauvegardes dans le coffre-fort même si le compte propriétaire du coffre-fort est inaccessible.

Il n'y a pas de nouveau prix pour cette fonctionnalité. Vous êtes uniquement facturé pour les sauvegardes stockées dans des coffres-forts hermétiques et pour les instantanés temporaires (pendant leur période de conservation dans le système) pour les ressources applicables aux tarifs en vigueur. Consultez [AWS Backup Tarification](#) pour plus d'informations.

Rubriques

- [Comment ça marche](#)
- [Considérations de coût](#)
- [Configuration de la sauvegarde principale du coffre-fort ventilé de manière logique](#)
- [Surveillez de manière logique la sauvegarde principale du coffre-fort ventilé](#)
- [Intégration et migration](#)
- [Résolution des problèmes](#)

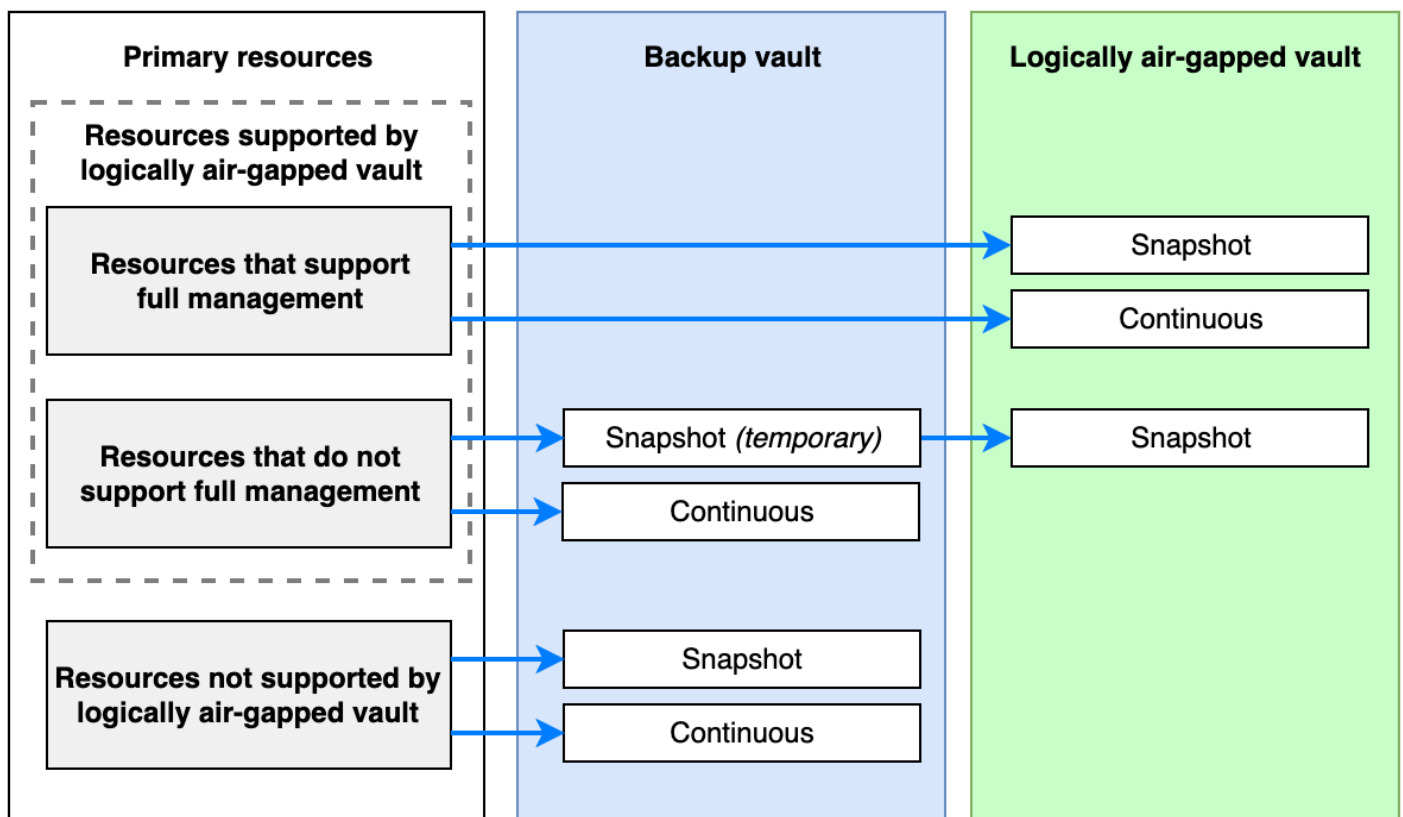
Comment ça marche

Vous pouvez intégrer cette fonctionnalité en mettant à jour votre plan de sauvegarde existant ou en en créant un nouveau et en ajoutant un ARN de coffre-fort logiquement espacé (nom du

champ :TargetLogicallyAirGappedBackupVaultArn) comme cible de sauvegarde principale. Vous pouvez effectuer cette opération via la AWS Backup console ou via les commandes de la AWS Backup CLI.

```
"TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:AirGappedVault",
```

Lorsque vous spécifiez à la fois un coffre-fort de sauvegarde et un coffre-fort logiquement espacé comme cibles pour vos tâches de sauvegarde, AWS Backup détermine le flux de travail approprié en fonction du type de ressource et de la configuration de chiffrement.



Ressources prises en charge pour la sauvegarde principale vers des coffres-forts logiquement espacés

[Pour consulter la liste complète des ressources prises en charge pour les coffres-forts à espacement logique, consultez la section Disponibilité des fonctionnalités. AWS Backup](#) Toutes les ressources qui prennent en charge les coffres-forts à espacement logique suivent le principe qui consiste à ne conserver qu'une seule copie de votre sauvegarde, plutôt que d'en stocker deux copies distinctes lorsque cette fonctionnalité est utilisée.

 Warning

Le support des ressources qui ne sont pas actuellement prises en charge pour cette fonctionnalité sera peut-être activé à l'avenir. Lorsque cela se produit, votre ressource nouvellement prise en charge commencera automatiquement à être sauvegardée dans le coffre-fort logiquement isolé en utilisant le flux de travail illustré ci-dessus.

Considérations et limites :

- **Même compte et même région uniquement** : votre coffre-fort logiquement isolé doit se trouver dans le même AWS compte et dans la même région que vos ressources pour utiliser cette fonctionnalité. Vous ne pouvez pas créer de sauvegardes directement entre comptes ou entre régions. Nous vous recommandons de sauvegarder vos données dans un coffre-fort isolé de manière logique situé dans la même région afin de permettre une restauration plus rapide sans avoir besoin d'une copie. Si vous avez besoin d'une copie de vos données dans une deuxième région à des fins de reprise après sinistre (DR), nous recommandons soit une réplication interrégionale de vos ressources principales pour un basculement rapide, soit des copies des points de restauration entre régions vers un coffre-fort de sauvegarde verrouillé.
- **Contraintes liées à l'utilisation de clés AWS gérées** — Les ressources ne supportant pas AWS Backup la gestion complète et chiffrées AWS à l'aide de clés gérées (par exemple `aws/ebs`, `aws/rds`) ne peuvent pas être copiées dans des coffres-forts séparés de manière logique. Ces ressources doivent être chiffrées à l'aide d'une clé KMS gérée par le client ou ne pas être chiffrées. Les ressources permettant une AWS Backup gestion complète ne sont pas soumises à cette contrainte.
- **Fréquence des sauvegardes et copies simultanées** : pour les ressources ne permettant pas une AWS Backup gestion complète, assurez-vous que votre fréquence de sauvegarde laisse suffisamment de temps pour que les copies soient effectuées. Si les sauvegardes sont planifiées plus fréquemment que les copies ne peuvent être terminées, les tâches de copie seront mises en file d'attente et risquent d'échouer. Pour obtenir des conseils sur les limites de copies simultanées, [consultez la section Quotas](#).
- **Compatibilité avec le cycle de vie** : la période de conservation spécifiée dans votre plan de sauvegarde doit être compatible avec les périodes de conservation minimale et maximale configurées pour votre coffre-fort à espacement logique.

- Coffres-forts de sauvegarde verrouillés : si le verrouillage du coffre-fort de sauvegarde cible est activé, les points de restauration temporaires ne peuvent pas être supprimés manuellement et seront conservés jusqu'à ce que la copie soit terminée ou que la période de conservation expire.
- Tests de restauration, indexation et analyse : les tests de restauration, l'indexation des points de restauration et l'analyse des programmes malveillants ignorent les points de restauration temporaires ayant un DELETE_AFTER_COPY cycle de vie. L'indexation des points de restauration ne prend pas en charge les points de récupération dans un coffre-fort logiquement espacé. L'analyse des programmes malveillants ne prend pas en charge les analyses planifiées des points de restauration copiés, y compris les copies automatiques effectuées dans le cadre des sauvegardes principales vers un coffre-fort isolé de manière logique.

Ressources permettant une AWS Backup gestion complète

Certains types de ressources, tels qu'Amazon EFS, Amazon S3, Amazon DynamoDB [AWS Backup doté de fonctionnalités avancées](#), etc., qui prennent en charge la gestion AWS Backup complète, peuvent être sauvegardés directement dans votre coffre-fort logiquement espacé. Aucun point de récupération n'est créé dans votre coffre-fort de sauvegarde et aucune opération de copie n'est requise. Toutes les actions de copie planifiées dans votre plan de sauvegarde utilisent le point de récupération de votre coffre-fort logiquement isolé comme source.

Les ressources qui prennent en charge la sauvegarde continue, telles qu'Amazon S3, peuvent également effectuer une sauvegarde continue directement dans un coffre-fort isolé de manière logique.

Pour obtenir une liste des types de ressources prenant en charge AWS Backup la gestion complète et les coffres-forts à espacement logique, voir [Disponibilité des fonctionnalités par ressource](#) dans les colonnes intitulées « Gestion complète » et « Coffre-fort à espacement logique ».

Ressource ne prenant pas en charge AWS Backup la gestion complète

Les ressources telles qu'Amazon EBS/EC2, Amazon Aurora et Amazon FSx ne peuvent pas être sauvegardées directement dans des coffres-forts espacés de manière logique. Pour ces types de ressources, AWS Backup crée un point de restauration temporaire dans votre coffre-fort de sauvegarde, puis le copie automatiquement dans votre coffre-fort isolé de manière logique.

Le point de restauration temporaire possède un paramètre de cycle de vie spécial appelé DELETE_AFTER_COPY. Une fois que la copie vers votre coffre-fort logiquement espacé est terminée avec succès, le point de récupération temporaire est AWS Backup automatiquement

supprimé. Toutes les autres actions de copie planifiées de votre plan de sauvegarde démarrent en parallèle avec la copie vers votre coffre-fort logiquement espacé et n'ont aucune incidence sur votre expérience de copie actuelle.

Si la copie vers votre coffre-fort logiquement espacé échoue, le point de restauration temporaire est conservé dans votre coffre-fort de sauvegarde conformément à la période de conservation que vous avez spécifiée. Cela garantit que vous disposez toujours d'un point de restauration utilisable après la fin d'une tâche de sauvegarde. Si le point de récupération est ensuite copié manuellement dans le coffre-fort isolé de manière logique, il est automatiquement nettoyé conformément à la règle. `DELETE_AFTER_COPY`

 Warning

Les ressources chiffrées AWS à l'aide de clés gérées (par exemple, `aws/ebs`) ne sont pas prises en charge pour la copie vers des coffres-forts logiquement espacés. Ces ressources doivent être chiffrées à l'aide d'une clé gérée par le AWS Key Management Service client ou non chiffrées. Les ressources permettant une AWS Backup gestion complète ne sont pas soumises à cette contrainte.

Supprimer après le cycle de vie de la copie

Les points de restauration temporaires ont un nouvel attribut de cycle de vie appelé `DeleteAfterEvent` avec une valeur de `DELETE_AFTER_COPY`. Cet attribut indique que le point de récupération sera automatiquement supprimé une fois toutes les tâches de copie terminées ou après la période de conservation que vous avez spécifiée, selon la première éventualité.

Un point de récupération temporaire est supprimé lorsque toutes les conditions suivantes sont réunies :

- Toutes les tâches de copie automatiques et planifiées sont terminées.
- Une tâche de copie est terminée vers votre coffre-fort cible logiquement espacé avec une période de conservation au moins aussi longue que le point de récupération de la source.

Si vous devez empêcher la suppression manuelle du point de restauration temporaire pendant que les copies sont en cours, envisagez d'utiliser un coffre-fort de sauvegarde verrouillé comme coffre-fort de sauvegarde cible.

Sauvegarde continue pour les ressources ne prenant pas en charge AWS Backup la gestion complète

Pour les ressources telles qu'Amazon Aurora, si vous activez la sauvegarde continue, si vous AWS Backup créez un point de restauration continu dans votre coffre-fort de sauvegarde et que vous prenez un instantané temporaire qui est copié dans votre coffre-fort à espacement logique. L'instantané temporaire est toujours supprimé une fois la copie terminée, que la copie soit réussie ou non, car vous conservez un point de restauration continu dans votre coffre-fort de sauvegarde.

Si vous ne souhaitez pas créer de point de restauration continue pour Amazon Aurora dans votre coffre-fort de sauvegarde, mais souhaitez un point de restauration continu pour Amazon S3 dans votre coffre-fort isolé de manière logique, vous pouvez désactiver le paramètre de sauvegarde continue (`EnableContinuousBackup`) dans le plan actuel et activer S3 Continuous à partir d'un autre plan.

Pour en savoir plus sur le stockage de sauvegarde Aurora, consultez [Comprendre l'utilisation du stockage de sauvegarde Amazon Aurora](#).

Ressources non prises en charge

Si un type de ressource n'est pas pris en charge par des coffres-forts séparés de manière logique, ou si une ressource non entièrement gérée est chiffrée à l'aide d'une clé AWS gérée, AWS Backup crée la sauvegarde uniquement dans votre coffre-fort de sauvegarde. Aucune copie vers votre coffre-fort logiquement espacé n'est tentée. La tâche de sauvegarde s'achève correctement avec un message indiquant pourquoi la sauvegarde n'a pas été transférée dans votre coffre-fort logiquement espacé.

Considérations de coût

- Cette fonctionnalité n'entraîne pas de nouveaux frais. Vous ne payez que pour le stockage dans vos coffres-forts.
- Pour les ressources permettant une AWS Backup gestion complète, la conservation des sauvegardes uniquement dans votre coffre-fort à espacement logique peut entraîner des économies importantes par rapport à la conservation de deux copies de sauvegarde à la fois dans un coffre-fort de sauvegarde et dans un coffre-fort à espacement logique.
- Pour les ressources ne permettant pas une AWS Backup gestion complète, vous êtes facturé à la fois pour le point de restauration temporaire dans votre coffre-fort de sauvegarde et pour les points de restauration dans votre coffre-fort à espacement logique.

- Vous pouvez toujours réaliser d'importantes économies en conservant une seule copie de sauvegarde, mais ces économies peuvent varier en fonction de la fréquence des sauvegardes et du taux de modification.
- Des fréquences de sauvegarde plus faibles permettent généralement de réaliser des économies plus importantes, car les points de restauration temporaires occupent le stockage pendant un pourcentage plus court de votre période de facturation.
- Certaines ressources ont des durées de facturation minimales, ce qui augmente les coûts liés aux points de récupération temporaires.
- Désactivez les balises ou la récupération de ACLs métadonnées dans votre configuration de sauvegarde si vous n'utilisez pas ces fonctionnalités S3. Cela permet de réduire les appels d'API et les frais associés pour les vérifications de métadonnées lors des opérations de copie.

Configuration de la sauvegarde principale du coffre-fort ventilé de manière logique

Vous pouvez configurer une sauvegarde principale du coffre-fort logiquement espacée par le biais de la AWS Backup console, de ou AWS Organizations des AWS CLI politiques AWS CloudFormation de sauvegarde.

Configuration d'un plan de sauvegarde

Console

Pour configurer une sauvegarde principale du coffre-fort à espacement logique pour un plan de sauvegarde

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Backup plans, puis Create backup plan ou sélectionnez un plan de sauvegarde existant à modifier.
3. Dans la section Configuration des règles de sauvegarde, spécifiez les paramètres de vos règles de sauvegarde.
4. Pour Backup Vault, choisissez le coffre-fort de sauvegarde dans lequel les points de restauration temporaires seront stockés (pour les ressources non entièrement gérées) ou où les sauvegardes seront stockées si elles ne peuvent pas être placées dans votre coffre-fort logiquement isolé.
5. Pour le coffre-fort à espacement logique (facultatif), choisissez le coffre-fort à espacement logique dans lequel vous souhaitez stocker vos sauvegardes.

Note

Le coffre-fort logiquement isolé doit se trouver dans le même compte et dans la même région que votre coffre-fort de sauvegarde.

6. Configurez les autres paramètres des règles de sauvegarde, y compris les options de cycle de vie et de copie.
7. Choisissez Créer un plan ou Enregistrer les modifications.

AWS CLI

Utilisez la commande CLI [create-backup-plan](#) pour créer un nouveau plan ou [update-backup-plan](#) pour mettre à jour un plan existant, et incluez le `TargetLogicallyAirGappedBackupVaultArn` paramètre dans votre règle de sauvegarde.

Exemple de commande CLI pour créer un plan de sauvegarde à l'aide d'un document JSON :

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

Exemple de commande CLI pour créer un plan de sauvegarde directement dans la CLI :

```
aws backup create-backup-plan --backup-plan '{
  "BackupPlanName": "MyPlan",
  "Rules": [
    {
      "RuleName": "MyRule",
      "TargetBackupVaultName": "MyBackupVault",
      "TargetLogicallyAirGappedBackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:MyLagVault",
      "ScheduleExpression": "cron(0 1 ? * * *)",
      "ScheduleExpressionTimezone": "America/Los_Angeles",
      "StartWindowMinutes": 60,
      "CompletionWindowMinutes": 120,
      "Lifecycle": {
        "DeleteAfterDays": 35
      }
    }
  ]
}
```

```
}'
```

Configuration de la sauvegarde à la demande

Console

Pour configurer une sauvegarde principale du coffre-fort à espacement logique pour une sauvegarde à la demande

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Sur la page Ressources protégées, choisissez Créer une sauvegarde à la demande.
4. Sélectionnez le type de ressource et l'ARN de ressource que vous souhaitez sauvegarder.
5. Pour Backup vault, choisissez le coffre de sauvegarde.
6. Pour le coffre-fort à espacement logique (facultatif), choisissez le coffre-fort à espace d'air logique dans lequel vous souhaitez stocker la sauvegarde.
7. Configurez les autres paramètres et choisissez Créer une sauvegarde à la demande.

AWS CLI

Utilisez la start-backup-job commande avec le nouveau --logically-air-gapped-backup-vault-arn paramètre :

```
aws backup start-backup-job \  
  --backup-vault-name MyBackupVault \  
  --logically-air-gapped-backup-vault-arn arn:aws:backup:us-  
east-1:123456789012:backup-vault:MyLagVault \  
  --resource-arn arn:aws:ec2:us-east-1:123456789012:volume/vol-abcd1234 \  
  --iam-role-arn arn:aws:iam::123456789012:role/service-role/  
AWSBackupDefaultServiceRole \  
  --lifecycle DeleteAfterDays=35
```

Surveillez de manière logique la sauvegarde principale du coffre-fort ventilé

Vous pouvez surveiller l'état de vos sauvegardes et de vos tâches de copie à l'aide de la AWS Backup console ou EventBridge des événements Amazon. AWS CLI

Surveiller les tâches de sauvegarde

Surveillez l'état des tâches de sauvegarde ([DescribeBackupJob](#)) pour vous assurer que vos ressources restent protégées. L'échec d'une tâche de sauvegarde indique qu'aucun point de restauration n'a été créé.

- Vérifiez l'emplacement de création du point de récupération : lorsqu'une tâche de sauvegarde est terminée avec succès, vous disposez d'un point de restauration dans votre coffre-fort de sauvegarde cible ou dans votre coffre-fort cible logiquement séparé. Vérifiez le `BackupVaultArn` champ pour déterminer où le point de récupération a été créé.
- Vérifier l'état de la tâche : si une ressource n'est pas prise en charge par des coffres-forts espacés de manière logique, la tâche de sauvegarde se termine par un « `MessageCategory` de » `LOGICALLY_AIR_GAPPED_BACKUP_VAULT_NOT_SUPPORTED` et un message d'état expliquant pourquoi la sauvegarde a plutôt été créée dans votre coffre-fort de sauvegarde.
- Vérifier le type de point de récupération temporaire : pour vérifier si un point de récupération est temporaire, recherchez le `RecoveryPointLifecycle.DeleteAfterEvent` champ dont la valeur est `deDELETE_AFTER_COPY`.

Surveiller les tâches de copie

Surveillez les tâches de copie ([ListCopyJobs](#)) vers votre coffre-fort hermétique de manière logique pour détecter les défaillances. En cas d'échec d'une tâche de copie, votre point de restauration reste dans votre coffre-fort de sauvegarde standard, sans protection logique du coffre-fort.

- Vérifier l'état de la tâche de copie : vous pouvez surveiller l'état de la tâche de copie à l'aide de l'`Copy Job State Change EventBridge` événement existant. Vous pouvez éventuellement filtrer sur le coffre-fort de destination (`destinationBackupVaultArn`) pour vous concentrer sur les copies du coffre-fort espacées de manière logique.
- Vérifier les copies pour un point de récupération source : utilisez l'[ListCopyJobs](#) API avec le nouveau `BySourceRecoveryPointArn` filtre pour rechercher toutes les tâches de copie associées à un point de récupération spécifique, y compris les copies automatiques vers votre coffre-fort logiquement espacé et les copies planifiées vers d'autres destinations.
- Vérifier la suppression du point de récupération temporaire : suivre l'achèvement de la suppression du point de récupération temporaire. Si l'état de la tâche de copie est `RUNNING` défini, le point de récupération n'a pas encore été supprimé. Si la copie se trouve dans votre coffre-fort logiquement espacé `FAILED`, le point de récupération sera conservé pendant la période de conservation que vous avez spécifiée.

 Note

Les enregistrements des tâches de copie expirent et sont supprimés 30 jours après leur fin. Après cette période, vous ne pourrez plus l'utiliser `ListCopyJobs` pour déterminer le statut historique de la copie.

Surveiller le point de récupération

Surveillez les points de EXPIRED récupération ([ListRecoveryPointsByBackupVault](#)), ce qui peut indiquer que vous n'avez pas AWS Backup pu les supprimer (peut-être en raison d'autorisations manquantes). EXPIRED les points de récupération peuvent avoir des répercussions financières.

- Vérifier l'état du point de récupération : utilisez l' `EventBridge` événement de changement d'état du point de restauration existant pour surveiller les expirations.
- Vérifier la suppression du point de récupération temporaire : si un point de récupération n'`DeleteAfterEvent: DELETE_AFTER_COPY` a pas été supprimé, utilisez l'`ListCopyJobsAPI` pour en déterminer la raison, comme indiqué ci-dessus.

Intégration et migration

Si vous utilisez actuellement des actions de copie pour copier des sauvegardes vers un coffre-fort à espacement logique, vous pouvez migrer vers une sauvegarde principale du coffre-fort à espacement logique afin de réduire les coûts. Vous pouvez également migrer vos sauvegardes continues Amazon S3 existantes d'un coffre-fort de sauvegarde vers un coffre-fort à espacement logique. Ce guide explique les conditions préalables et les étapes requises pour migrer vers la fonction de sauvegarde principale du coffre-fort logiquement espacé.

Conditions préalables et meilleures pratiques

Avant de pouvoir utiliser efficacement la fonction de sauvegarde principale du coffre-fort logiquement espacé, il existe des conditions préalables et des meilleures pratiques recommandées.

Conditions préalables

À l'heure actuelle, un coffre-fort isolé logiquement utilisé comme cible de sauvegarde principale ne prend en charge que les sauvegardes effectuées au sein du même AWS compte et de la même AWS région que vos ressources de sauvegarde. Logiquement, les sauvegardes des coffres-forts

sont stockées dans des comptes de service distincts, ce qui permet de les isoler entre comptes et entre organisations sans qu'il soit nécessaire de les copier sur des comptes distincts. Si vous avez besoin de sauvegardes interrégionales, continuez à utiliser le coffre-fort isolé de manière logique comme destination de copie. Avant de migrer vers cette fonctionnalité, assurez-vous de répondre aux exigences suivantes :

- Exigences relatives à la région et au compte
 - Votre coffre hermétique doit se trouver dans le même AWS compte et dans la même région que vos ressources
- Compatibilité des ressources
 - Vérifiez que vos ressources sont prises en charge par des coffres-forts espacés de manière logique dans Disponibilité des [fonctionnalités](#) par ressource.
 - Vérifiez si vos ressources prennent en charge [AWS Backup la gestion complète](#) ou non. L'expérience de création de sauvegardes séparées diffère entre ces deux types de ressources, même si le résultat est similaire pour les deux.
- Exigences en matière de chiffrement
 - Les ressources qui ne prennent pas en charge AWS Backup la gestion complète doivent être déchiffrées ou chiffrées à l'aide de clés gérées par le client (CMKs). AWS Les ressources chiffrées par clé gérée (AMK) ne sont pas prises en charge par un coffre-fort logiquement espacé.

Bonnes pratiques

- Commencez par une migration pilote de ressources non critiques.
- Vérifiez et ajustez les fréquences de sauvegarde en fonction des performances des tâches de copie.
- Mettez en œuvre une surveillance complète avant la migration complète.
- Vérifiez régulièrement la création de points de récupération dans les coffres-forts prévus.

Planification de votre migration

- Passez en revue les plans et politiques de sauvegarde existants.
- Identifiez les ressources qui prennent en charge AWS Backup la gestion complète et celles qui ne le sont pas.

- Ressources prenant en charge AWS Backup la gestion complète (par exemple, EFS, S3) : peuvent être sauvegardées directement dans un coffre-fort à espacement logique
- Ressources ne prenant pas en charge AWS Backup la gestion complète (par exemple EC2, EBS, FSx) : nécessitent une sauvegarde temporaire dans un coffre-fort de sauvegarde avant d'être copiées dans un coffre-fort à espacement logique
- Passez en revue votre volume et votre fréquence de sauvegarde actuels et assurez-vous que votre configuration est conforme aux limites de copies simultanées pour toutes les ressources ne permettant pas une AWS Backup gestion complète.
- Ignorez cette étape si vous effectuez déjà des copies vers un coffre-fort isolé de manière logique à la même fréquence que les sauvegardes de votre coffre-fort standard.
- Envisagez d'ajuster la fréquence des sauvegardes, si nécessaire, pour éviter la mise en file d'attente des tâches de copie.
- En cas de mise en file d'attente des tâches de copie, vous disposerez toujours d'un point de restauration utilisable dans votre coffre-fort de sauvegarde standard en attendant que la copie soit terminée dans votre coffre-fort logiquement espacé. Cependant, ce point de récupération ne fournira pas le niveau de protection qu'offre le coffre-fort Logically Airgapped.

Ressources soutenant le processus de migration AWS Backup de la gestion complète

Pour des ressources entièrement gérées, vous pouvez effectuer des sauvegardes directement dans votre coffre-fort isolé de manière logique sans avoir à effectuer d'opérations de copie.

Pour les sauvegardes basées sur des instantanés

Ce processus s'applique à tous les scénarios de capture instantanée, que votre coffre-fort de sauvegarde soit verrouillé ou non. Lors de la migration d'un plan de sauvegarde existant ou de l'utilisation d'un coffre-fort de sauvegarde existant (principal) et d'un coffre-fort logiquement espacé (copie) dans un nouveau plan de sauvegarde :

1. Conservez votre coffre-fort de sauvegarde existant ou ajoutez-le comme cible de sauvegarde (`TargetBackupVaultName`). Ce coffre-fort ne stockera aucune sauvegarde mais doit être fourni pour des raisons de rétrocompatibilité.
2. Mettez à jour votre plan de sauvegarde pour inclure le coffre-fort logiquement isolé (`TargetLogicallyAirGappedBackupVaultArn`), existant dans le même compte, en tant que cible principale.

3. Passez en revue toute action de copie existante vers un autre coffre-fort logiquement espacé pour déterminer si elle est toujours nécessaire. Vous pouvez également déplacer ce coffre en tant que cible principale à l'étape 2 s'il se trouve dans le même compte.

Pour les sauvegardes continues d'Amazon S3

Le coffre-fort isolé de manière logique en tant que cible de sauvegarde principale prend en charge la sauvegarde continue pour Amazon S3. Toutefois, vous ne pouvez conserver qu'un seul point de restauration continue actif par ressource dans un seul coffre. Si vous disposez d'un point de restauration continue Amazon S3 actif, vous devez le dissocier ou le supprimer avant d'en créer un nouveau dans un autre coffre-fort. L'ajout d'une cible de coffre-fort isolée de manière logique (provenant du même compte) à votre plan de sauvegarde, avec un point de restauration continue Amazon S3 actif existant, entraînera l'échec de la tâche de sauvegarde continue.

Pour migrer votre point de restauration continue Amazon S3 vers votre coffre-fort isolé de manière logique à partir d'un coffre-fort de sauvegarde déverrouillé :

1. Mettez à jour votre plan de sauvegarde pour ajouter une action de copie à votre coffre-fort logiquement isolé. Cela réduira le coût de génération de la sauvegarde initiale dans votre coffre-fort logiquement isolé. Ignorez cette étape si vous effectuez déjà une copie dans votre coffre-fort local logiquement espacé.
2. Vérifiez qu'au moins une copie instantanée est terminée correctement dans votre coffre-fort logiquement espacé avant de continuer.
3. Dissociez le point de restauration continue Amazon S3 existant. Appelez l'[DisassociateRecoveryPoint](#) API pour modifier le statut du point de récupération de AVAILABLE à STOPPÉ. Cette action préserve vos données de sauvegarde existantes tout en empêchant l'ajout de nouvelles données.
4. Mettez à jour le plan de sauvegarde pour ajouter un coffre-fort logiquement espacé (`TargetLogicallyAirGappedBackupVaultArn`) comme cible de sauvegarde.
5. Supprimez toutes les actions de copie précédentes du plan.
6. Lors de la prochaine exécution du plan de sauvegarde, un nouveau point de restauration continue sera créé dans votre coffre-fort logiquement isolé. Ce point de restauration sera incrémentiel, en fonction du cliché copié à l'étape 1.

Pour migrer votre point de restauration continue Amazon S3 vers votre coffre-fort isolé de manière logique à partir d'un coffre-fort de sauvegarde verrouillé :

1. Mettez à jour votre plan de sauvegarde pour ajouter une action de copie à votre coffre-fort logiquement isolé. Cela réduira le coût de génération de la sauvegarde initiale dans votre coffre-fort logiquement isolé. Ignorez cette étape si vous effectuez déjà une copie dans votre coffre-fort local logiquement espacé.
2. Vérifiez qu'au moins une copie instantanée est terminée correctement dans votre coffre-fort logiquement espacé avant de continuer. Assurez-vous que le cliché copié est conservé pendant une période suffisamment longue pour rester disponible jusqu'à ce que vous ayez terminé toutes les étapes.
3. Ajoutez le coffre logiquement espacé comme cible principale et supprimez toute action de copie.
 - a. Cette étape est nécessaire car les coffres-forts verrouillés ne prennent pas en charge la dissociation des points de restauration continue.
 - b. Votre point de restauration continue existant dans le coffre de sauvegarde verrouillé continuera à accumuler des données jusqu'à leur expiration conformément à leur cycle de vie.
 - c. Les nouvelles tâches de sauvegarde en continu échoueront car il ne peut exister qu'un seul point de restauration continue actif par ressource. Étant donné que ces tâches échouent, aucune action de copie ne sera exécutée.
4. Attendez que le point de restauration continue existant expire. Après expiration, un nouveau point de restauration continue sera créé dans le coffre hermétiquement fermé. Ce point de restauration sera incrémentiel en fonction de l'instantané copié à partir de l'étape 1, à condition que le cliché existe toujours dans votre coffre-fort isolé de manière logique.
5. Toutes les données accumulées dans votre coffre-fort standard seront perdues à leur expiration. Seules les données sauvegardées après la création du nouveau point de restauration dans le coffre logiquement aéré seront conservées.

Ressources ne prenant pas en charge le processus AWS Backup de migration de gestion complet

Les ressources qui ne sont pas entièrement gérées nécessitent une opération de copie vers le coffre-fort logiquement espacé. Le processus crée un point de récupération temporaire (facturable) dans votre coffre-fort de sauvegarde standard, qui est automatiquement copié dans votre coffre-fort isolé de manière logique, puis supprimé une fois la copie terminée. Lorsque vous mettez à jour votre plan de sauvegarde pour inclure une cible de coffre-fort logiquement isolée :

- Les tâches de sauvegarde créeront un point de restauration dans votre coffre de sauvegarde. Cela a un cycle de vie dicté par l'`DELETE_AFTER_COPY` événement.

- Une tâche de copie initie automatiquement le transfert du point de récupération vers votre coffre-fort isolé de manière logique.
- Une fois la copie terminée avec succès, le point de récupération temporaire de votre coffre-fort est supprimé.
- Si la copie échoue, le point de récupération temporaire est conservé pendant une durée maximale en fonction de la période de conservation que vous avez spécifiée, ce qui garantit que vous disposez d'un point de récupération utilisable.

Résolution des problèmes

La tâche de sauvegarde ou de copie échoue en raison d'une erreur d'incompatibilité du cycle de vie

Erreur pour les tâches de sauvegarde : `Backup job failed because the lifecycle is outside the valid range for backup vault.`

Erreur pour les tâches de copie : `Copy job failed. The retention specified in the job is not within the range specified for the target Backup Vault.`

Cause possible : les tâches de sauvegarde ou de copie échouent car la période de conservation est incompatible avec les paramètres de rétention minimaux ou maximaux du coffre-fort logiquement espacé.

Solution : mettez à jour votre plan de sauvegarde pour spécifier une période de conservation comprise entre les périodes de rétention minimale et maximale configurées pour votre coffre-fort isolé de manière logique.

Les tâches de sauvegarde continue échouent lorsque « la sauvegarde continue est déjà activée »

Erreur : `Bucket {bucket_name} already has continuous backup enabled for another vault Backup job failed.`

Cause possible : les tâches de sauvegarde en continu échouent car il existe déjà un point de restauration continue pour la ressource dans un autre coffre.

Solution : Chaque ressource ne peut avoir qu'un seul point de restauration continue. Si votre coffre-fort de sauvegarde est déverrouillé, dissociez le point de restauration continue existant à l'aide de la [disassociate-recovery-point](#) commande. Si votre coffre-fort de sauvegarde est verrouillé, attendez que le point de restauration continue existant expire conformément à son cycle de vie.

La tâche de sauvegarde se termine avec le message « Complété avec des problèmes » - Type de ressource non pris en charge

Message : Backup job completed successfully to the target backup vault. This resource type is not supported by logically air-gapped backup vault.

Cause possible : les tâches de sauvegarde pour les ressources non prises en charge et non entièrement gérées affichent le message « Terminé avec des problèmes » avec un message indiquant que la ressource n'est pas prise en charge.

Solution : les types de ressources qui ne sont pas pris en charge seront uniquement sauvegardés dans le coffre de sauvegarde. Si vous souhaitez conserver ces sauvegardes dans votre coffre-fort de sauvegarde, aucune action n'est requise. Si vous préférez ne pas mélanger des ressources non prises en charge à votre coffre-fort logiquement isolé, vous pouvez :

- Supprimez la ressource ou la cible du coffre-fort logiquement espacé de votre plan de sauvegarde pour ces ressources et continuez à sauvegarder uniquement dans votre coffre-fort de sauvegarde. Vous pouvez ensuite ajouter la ressource dans le cadre d'un autre plan.

La tâche de sauvegarde s'achève avec le message « Complété avec des problèmes » - Clé de chiffrement non prise en charge

Message : Backup job completed successfully to the target backup vault. This resource is encrypted with an AWS managed key and cannot be copied to a logically air-gapped backup vault.

Cause possible : les tâches de sauvegarde pour les ressources non prises en charge et non entièrement gérées affichent le message « Terminé avec des problèmes » avec un message indiquant que la ressource est cryptée à l'aide d'une clé AWS gérée.

Résolution : Les ressources non entièrement gérées chiffrées à l'aide de clés AWS gérées ne peuvent pas être copiées dans des coffres-forts séparés de manière logique. Si vous souhaitez conserver ces sauvegardes dans votre coffre-fort de sauvegarde, aucune action n'est requise. Si vous préférez ne pas mélanger des ressources non prises en charge à votre coffre-fort logiquement isolé, vous pouvez :

- Chiffrez à nouveau vos ressources avec une clé KMS gérée par le client, ou

- Supprimez la ressource ou la cible du coffre-fort logiquement espacé de votre plan de sauvegarde pour ces ressources et continuez à sauvegarder uniquement dans votre coffre-fort de sauvegarde. Vous pouvez ensuite ajouter la ressource dans le cadre d'un autre plan.

Les points de récupération restent en **EXPIRED** état

Cause possible : les points de restauration temporaires passent à EXPIRED l'état mais ne sont pas supprimés.

Résolution : AWS Backup il se peut que les autorisations nécessaires pour supprimer les points de récupération ne soient pas disponibles. Vérifiez que votre rôle de sauvegarde dispose des autorisations IAM nécessaires. Vous devrez peut-être supprimer manuellement les points expired de récupération.

Les tâches de copie sont mises en file d'attente ou échouent en raison d'une fréquence de sauvegarde élevée

Cause possible : les tâches de copie vers des coffres-forts à espacement logique sont mises en file d'attente ou échouent car les sauvegardes sont planifiées plus fréquemment que les copies ne peuvent être effectuées.

Solution : Réduisez la fréquence de vos sauvegardes ou ajustez votre calendrier de sauvegarde pour laisser plus de temps entre les sauvegardes. Consultez la [documentation sur AWS Backup les quotas](#) pour plus d'informations sur les limites de copies simultanées.

Approbation multipartite pour les coffres-forts à espacement logique

Vue d'ensemble de l'approbation multipartite dans un coffre-fort hermétique

AWS Backup vous offre la possibilité d'ajouter l'[approbation multipartite](#), une fonctionnalité depuis AWS Organizations, à vos coffres-forts logiquement espacés. L'approbation multipartite fournit une option supplémentaire pour protéger les opérations critiques par le biais d'un processus d'approbation distribué.

L'approbation multipartite est conçue pour aider à protéger les ressources critiques et à minimiser le délai de retour à une exploitation complète, par exemple en cas d'interruption causée par des acteurs malveillants ou des événements malveillants. Cette configuration peut vous aider à restaurer le contenu d'un coffre-fort logiquement isolé qui a peut-être été compromis.

Il n'y a aucun coût supplémentaire pour intégrer et utiliser des équipes d'approbation multipartites dotées de coffres-forts AWS Backup hermétiques (des frais de stockage et de transferts entre régions s'appliquent, comme indiqué sur la page de tarification).

En tant que AWS Backup client, vous pouvez utiliser l'approbation multipartite pour accorder la capacité d'approbation de certaines opérations à un groupe de personnes de confiance qui peuvent approuver de manière collaborative l'accès à un coffre-fort séparé à partir d'un compte de récupération créé séparément en cas d'activité malveillante présumée susceptible de compromettre l'utilisation du compte principal.

Les étapes suivantes décrivent le flux recommandé pour configurer une AWS organisation de reprise, configurer l'approbation multipartite, puis utiliser l'approbation multipartite avec vos coffres-forts logiquement séparés :

1. Un administrateur [crée une nouvelle organisation via Organizations](#) à utiliser pour les opérations de restauration.
2. Dans le compte de gestion de cette nouvelle organisation, l'administrateur crée et configure une instance IAM Identity Center (IDC) (pour activer une instance d'organisation, voir [Activer le centre d'identité IAM dans le guide de l'utilisateur de l'IAM Identity Center](#)). Consultez également la séquence de [création d'une source d'identité d'approbation multipartite](#) dans le Guide de l'utilisateur de l'approbation multipartite.
3. L'administrateur [créera ensuite une équipe d'approbation](#), le groupe principal de personnes de confiance qui seront les principaux utilisateurs de l'approbation multipartite.
4. L'administrateur a l'habitude de AWS RAM [partager une équipe d'approbation](#) avec chaque compte qui possède au moins un coffre-fort logiquement isolé (probablement votre compte principal). La RAM doit être configurée pour le compte propriétaire du coffre-fort et pour l'organisation secondaire.
5. L'administrateur de ces comptes [associe un coffre-fort logiquement isolé à une équipe d'approbation](#).
6. Un compte de récupération [demande l'accès](#) à un compte doté d'un coffre-fort logiquement isolé auquel est associée une équipe d'approbation multipartite (« équipe »). L'équipe associée au compte [approuve ou refuse la demande](#).
7. L'administrateur du compte propriétaire du coffre-fort logiquement isolé peut demander que [l'équipe d'approbation soit dissociée du](#) coffre-fort. La demande nécessite l'approbation actuelle de l'équipe.

8. Un administrateur peut [mettre à jour la composition de l'équipe d'approbation](#) si nécessaire conformément à ses pratiques de sécurité ou lorsque des personnes rejoignent ou quittent votre organisation.

Conditions préalables et meilleures pratiques pour utiliser l'approbation multipartite avec un coffre-fort hermétique

Avant de pouvoir utiliser efficacement et en toute sécurité l'approbation multipartite avec vos coffres-forts à espacement logique, il existe des conditions préalables et des meilleures pratiques recommandées.

Bonnes pratiques :

- Deux organisations (ou plus) par le biais AWS d'Organizations. Il doit s'agir de votre organisation principale dans laquelle vous possédez un ou plusieurs comptes dotés d'au moins un coffre-fort logiquement isolé. L'organisation secondaire doit être votre organisation de reprise. C'est dans cette organisation que votre équipe d'approbation multipartite sera gérée.

Conditions préalables

1. Vous avez [configuré l'approbation multipartite](#) et disposez d'au moins une équipe d'approbation.
2. Au moins un compte de votre organisation principale doit disposer d'un coffre-fort isolé logiquement (et du coffre-fort de sauvegarde d'origine).
3. Le compte de gestion de l'organisation principale est activé pour l'approbation multipartite.

Tip

AWS Backup vous recommande d'appliquer une politique de contrôle des services (SCP) à votre organisation principale et de la configurer avec les autorisations appropriées pour l'organisation et pour chaque équipe d'approbation. Consultez la section [Conditions d'approbation multipartite](#) pour un exemple de politique.

4. Votre équipe d'approbation multipartite de l'organisation secondaire (de restauration) est [partagée](#) à la fois AWS RAM avec vos comptes propriétaires du ou des coffres-forts séparés de manière logique et avec vos comptes de récupération.

Considérations et dépendances entre régions lors de l'utilisation de l'approbation multipartite

Lorsque vous activez l'approbation multipartite et votre instance IAM Identity Center dans différentes régions, l'approbation multipartite permet d'appeler IAM Identity Center dans toutes les régions. Cela signifie que les informations relatives aux utilisateurs et aux groupes sont transférées d'une région à l'autre. Approbation multipartite Les ressources de l'équipe ne peuvent être créées et stockées que dans l'est des Région AWS États-Unis (Virginie du Nord).

Les autres ressources Régions AWS faisant référence à des équipes d'approbation multipartites dépendront de l'est des Région AWS États-Unis (Virginie du Nord). En conséquence, l'approbation multipartite effectuera des appels interrégionaux si votre instance Identity Center and/or logiquement isolée ne se trouve pas dans l'est des États-Unis (Virginie du Nord).

Termes d'approbation multipartites, concepts et profils d'utilisateurs

L'approbation multipartite dans votre coffre-fort logiquement espacé est une intégration des AWS Organizations fonctionnalités Gestion des identités et des accès AWS (IAM) et AWS Backup(RAM) et AWS RAM (RAM). Gestion de compte AWS Grâce à la CLI, vous pouvez interagir avec chaque service pour envoyer les commandes appropriées. Vous pouvez également utiliser la console, mais vous devrez accéder à la console du service approprié pour effectuer des tâches spécifiques.

La manière dont vous interagissez avec l'approbation multipartite dépend de vos rôles et responsabilités au sein de vos organisations, ainsi que des autorisations dont vous disposez dans vos AWS Backup comptes.

Comme indiqué dans le [Guide de l'utilisateur de l'approbation multipartite](#), les membres de votre organisation qui utilisent l'approbation multipartite seront soit demandeurs, administrateurs, soit approbateurs. Des autorisations spécifiques s'appliquent à [chaque fonction](#). Conformément aux meilleures pratiques en matière de sécurité, un utilisateur ne doit remplir qu'une seule fonction.

Consoles, portails et sessions

AWS Backup les comptes dotés d'un ou de plusieurs coffres-forts séparés de manière logique peuvent faire l'objet d'une approbation multipartite.

Avant le processus d'approbation multipartite, un administrateur crée une organisation secondaire AWS Organizations à des fins de reprise (une organisation de reprise) si aucune organisation n'a été configurée auparavant.

L'administrateur utilise ensuite AWS Resource Access Manager (RAM) pour configurer le partage interorganisationnel entre l'organisation principale et l'organisation de reprise.

L'organisation principale héberge des comptes qui possèdent et utilisent un coffre-fort logiquement isolé dans lequel sont stockées les données protégées.

L'organisation de recouvrement héberge au moins un compte de recouvrement. Ce compte héberge un point d'accès qui peut servir de « porte dérobée » essentielle au coffre-fort partagé logiquement séparé. Ce point d'accès est appelé coffre de sauvegarde pour l'accès à la restauration. Ce coffre d'accès ne stocke pas de données ; il sert plutôt de point d'accès ou de montage qui reflète le contenu du coffre-fort source logiquement espacé, mais ne contient aucune donnée pouvant être modifiée ou supprimée. Par exemple, si un client suit le processus de restauration d'un point de restauration dans un coffre-fort de sauvegarde avec accès à la restauration, c'est le point de restauration situé dans le coffre-fort isolé de manière logique qui est restauré par le biais d'une restauration entre comptes via le compte de récupération.

Pour garantir une sécurité accrue, les clients utilisent ce compte de récupération pour effectuer des opérations protégées sur le compte principal, mais uniquement après que ces opérations ont été approuvées par l'[équipe d'approbation associée lors d'une session d'approbation](#). Une session est créée une AWS fois qu'une demande d'approbation a été envoyée, et cette session se termine lorsqu'un seuil de membres de l'équipe d'approbation approuve ou refuse la demande ou lorsque le temps de session autorisé est dépassé.

Une équipe est composée d'approbateurs (en fait, la partie de l'approbation multipartite réservée aux parties) qui reçoivent des notifications par e-mail concernant les demandes d'opérations protégées. Ces e-mails confirment qu'une session d'approbation a commencé pour la demande. L'approbation est accordée une fois que le seuil d'approbation minimum requis est atteint. Ce seuil peut être défini lors de la création de l'équipe d'approbation multipartite (« Équipe »).

Les équipes d'approbation multipartites sont gérées via le portail d'approbation multipartite des Organisations (« portail »), une application AWS gérée qui fournit aux identités un emplacement centralisé où les membres de l'équipe d'approbation peuvent recevoir et répondre aux invitations des équipes d'approbation et aux demandes d'opérations.

Tâches de l'administrateur

Plusieurs tâches impliquant AWS Backup une vue d'ensemble multipartite nécessitaient un utilisateur disposant d'autorisations d'administrateur et d'un accès au compte de gestion.

Création d'une équipe d'approbation

Un utilisateur de votre organisation disposant d'autorisations d'administrateur pour un AWS compte doit [configurer l'approbation multipartite](#) (étape 3 de l'[aperçu](#)).

Avant de procéder à cette étape, il est recommandé, à titre de bonne pratique, de configurer à la fois une organisation principale et une organisation secondaire (à des fins de restauration) AWS Organizations (étape 1 de la section [Vue d'ensemble](#)).

Consultez la section [Créer une équipe d'approbation](#) dans le guide de l'utilisateur de l'approbation multipartite pour créer votre équipe.

Pendant l'[aws mpa create-approval-team](#) opération, l'un des paramètres est `policies`. Voici une liste de ARNs (Amazon Resource Names) pour les politiques de ressources d'approbation multipartites qui définissent les autorisations qui protègent l'équipe.

La politique présentée dans l'exemple du Guide de l'utilisateur de l'approbation multipartite dans la procédure [Créer une équipe d'approbation](#) contient la politique `["arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault"]` avec plusieurs autorisations nécessaires.

Procédez comme suit pour renvoyer une liste des politiques disponibles en utilisant `aws mpa list-policies` :

1. Politiques relatives aux listes :

```
aws mpa list-policies --region us-east-1
```

2. Répertoriez toutes les versions des politiques :

```
aws mpa list-policy-versions --policy-arn arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault --region us-east-1
```

3. Obtenez des informations sur une politique :

```
aws mpa get-policy-version --policy-version-arn arn:aws:mpa::aws:policy/backup.amazonaws.com/CreateRestoreAccessVault/1 --region us-east-1
```

Développez ci-dessous pour voir la politique qui sera créée puis attachée à votre équipe d'approbation par cette opération :

Restaurer la politique du coffre d'accès

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VaultOwnerPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*",
      "Action": [
        "mpa:StartSession",
        "mpa:CancelSession"
      ],
      "Condition": {
        "StringEquals": {
          "mpa:RequestedOperation": "backup:RevokeRestoreAccessBackupVault",
          "mpa:ProtectedResourceAccount": "${aws:PrincipalAccount}"
        },
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
    }
  ]
}
```

Partagez une équipe d'approbation multipartite à l'aide de AWS RAM

Vous pouvez partager une équipe d'approbation multipartite avec d'autres AWS comptes en utilisant [AWS Resource Access Manager \(RAM\)](#), étape 4 de l'[aperçu](#).

Console

Partagez une équipe d'approbation multipartite à l'aide de AWS RAM

1. Connectez-vous à la [console AWS RAM](#).

2. Dans le volet de navigation, sélectionnez Resource shares.
3. Choisissez Créer une ressource.
4. Dans le champ Nom, entrez un nom descriptif pour votre partage de ressources.
5. Sous Type de ressource, sélectionnez Équipe d'approbation multipartite dans le menu déroulant.
6. Sous Ressources, sélectionnez l'équipe d'approbation que vous souhaitez partager.
7. Sous Principaux, spécifiez les AWS comptes avec lesquels vous souhaitez partager l'équipe d'approbation.
8. Pour partager avec des AWS comptes spécifiques, sélectionnez AWS des comptes et saisissez le compte IDs à 12 chiffres.
9. Pour partager avec une organisation ou une unité organisationnelle, sélectionnez Organisation ou unité organisationnelle et entrez l'ID approprié.
10. (Facultatif) Sous Balises, ajoutez les balises que vous souhaitez associer à ce partage de ressources.
11. Choisissez Créer une ressource.

L'état du partage des ressources s'affichera initialement sous la forme `PENDING`. Une fois que les comptes destinataires auront accepté l'invitation, le statut passera à `ACTIVE`.

CLI

Pour partager une équipe d'approbation multipartite AWS RAM via la CLI, utilisez les commandes suivantes :

Tout d'abord, identifiez l'ARN de l'équipe d'approbation que vous souhaitez partager :

```
aws mpa list-approval-teams --region us-east-1
```

Créez un partage de ressources à l'aide de la `create-resource-share` commande :

```
aws ram create-resource-share \  
--name "MPA-Team-Share" \  
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \  
--principals "ACCOUNT_ID_TO_SHARE_WITH" \  
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \  
--region us-east-1
```


Pour partager avec une organisation plutôt qu'avec des comptes spécifiques :

```
aws ram create-resource-share \
--name "MPA-Team-Share" \
--resource-arns "arn:aws:mpa:us-east-1:ACCOUNT_ID:approval-team/TEAM_ID" \
--permission-arns "arn:aws:ram::aws:permission/AWSRAMMPAApprovalTeamAccess" \
--allow-external-principals \
--region us-east-1
```

Vérifiez l'état de votre partage de ressources :

```
aws ram get-resource-shares \
--resource-owner SELF \
--region us-east-1
```

Le ou les comptes du destinataire devront accepter l'invitation au partage des ressources :

```
aws ram get-resource-share-invitations --region us-east-1
```

Exécutez dans le compte du destinataire pour accepter une invitation :

```
aws ram accept-resource-share-invitation \
--resource-share-invitation-arn "arn:aws:ram:REGION:ACCOUNT_ID:resource-share-
invitation/INVITATION_ID" \
--region us-east-1
```

Une fois l'invitation acceptée, l'équipe d'approbation multipartite sera disponible sur le compte du destinataire.

AWS propose des outils pour partager l'accès aux comptes, y compris l'accès par le biais [AWS Resource Access Manager](#) et l'[accès multipartite](#). Lorsque vous choisissez de partager un coffre-fort isolé de manière logique avec un autre compte, tenez compte des informations suivantes :

Fonctionnalité	AWS RAM partage basé	Accès basé sur l'approbation de plusieurs parties
Accès à des coffres-forts à espacement logique	Une fois le partage de RAM terminé, les coffres-forts sont accessibles.	Toute tentative effectuée par un autre compte doit être approuvée par un

Fonctionnalité	AWS RAM partage basé	Accès basé sur l'approbation de plusieurs parties
		certain nombre de membres de l'équipe d'approbation multipartite. La session d'approbation expire automatiquement 24 heures après le lancement de la demande.
Suppression de l'accès	Le compte propriétaire du coffre-fort logiquement espacé peut mettre fin au partage basé sur la RAM à tout moment.	L'accès à un coffre-fort ne peut être supprimé que sur demande adressée à l'équipe d'approbation multipartite.
Copier entre les comptes et and/or les régions	Cette option n'est pas prise en charge actuellement.	Les sauvegardes peuvent être copiées dans le même compte ou avec d'autres comptes de la même organisation que le compte de restauration.
Facturation des transferts entre régions		Les transferts entre régions sont facturés sur le même compte qui possède le coffre de sauvegarde de l'accès à la restauration.
Usage recommandé	Il est principalement utilisé pour la récupération des données perdues et pour les tests de restauration.	Il est principalement utilisé dans les situations où l'accès ou la sécurité du compte sont soupçonnés d'être compromis.
Régions	Disponible partout Régions AWS où des coffres-forts à espacement d'air logique sont pris en charge.	Disponible partout Régions AWS où des coffres-forts à espacement d'air logique sont pris en charge.

Fonctionnalité	AWS RAM partage basé	Accès basé sur l'approbation de plusieurs parties
Restaure	Tous les types de ressources pris en charge peuvent être restaurés à partir d'un compte partagé.	Tous les types de ressources pris en charge peuvent être restaurés à partir d'un compte partagé.
Configuration	Le partage peut avoir lieu dès que le AWS Backup compte configure le partage de RAM et que le compte destinataire accepte le partage.	Le partage nécessite que le compte de gestion crée d'abord une équipe, puis configure le partage de RAM. Ensuite, le compte de gestion opte pour l'approbation multipartite et affecte cette équipe à un coffre-fort isolé de manière logique.
Partage	Le partage s'effectue par le biais de la RAM au sein d'une même AWS organisation ou entre AWS organisations. L'accès est accordé selon le modèle « push », dans lequel le compte propriétaire du coffre-fort logiquement espacé accorde d'abord l'accès. Ensuite, l'autre compte accepte l'accès.	L'accès à un coffre-fort isolé de manière logique se fait par le biais des équipes d'approbation soutenues par les organisations au sein de la même AWS organisation ou de plusieurs organisations. L'accès est accordé selon le modèle « pull », selon lequel le compte destinataire demande d'abord l'accès, puis l'équipe d'approbation accepte ou refuse la demande.

Tâches du demandeur

Associez une équipe d'approbation multipartite à un coffre-fort hermétique

Demandeur : utilisateur ayant accès au compte propriétaire du coffre-fort logiquement isolé.

[Vous pouvez associer une équipe d'approbation multipartite à un coffre-fort isolé de manière logique afin de permettre l'approbation collaborative de l'accès au coffre-fort \(étape 5 de l'aperçu\).](#)

Console

Associez une équipe d'approbation multipartite à un coffre-fort hermétique

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à la section Backup vault dans le volet de navigation de gauche.
3. Sélectionnez le coffre-fort de sauvegarde isolé de manière logique que vous souhaitez associer à une équipe MPA.
4. Sur la page des détails du coffre-fort, sélectionnez Affecter une équipe d'approbation.
5. Dans le menu déroulant, sélectionnez l'équipe d'approbation que vous souhaitez associer au coffre
6. Facultatif Entrez un commentaire expliquant la raison de l'association.
7. Sélectionnez Envoyer la demande pour soumettre la demande d'association.

S'il s'agit de la première équipe d'approbation associée au coffre, elle sera associée au coffre. Si une équipe est déjà associée au coffre, voir [Mettre à jour une équipe d'approbation multipartite](#) pour connaître les étapes à suivre.

CLI

Utilisez la commande `CLlassociate-backup-vault-mpa-approval-team`, modifiée avec les paramètres suivants :

```
aws backup associate-backup-vault-mpa-approval-team \  
--backup-vault-name VAULT_NAME \  
--mpa-approval-team-arn MPA_TEAM_ARN \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

S'il s'agit de la première équipe d'approbation associée au coffre, elle sera associée au coffre. Si une équipe est déjà associée au coffre, voir [Mettre à jour une équipe d'approbation multipartite](#) pour connaître les étapes à suivre.

Demandez l'accès à un coffre-fort isolé de manière logique

Demandeur : utilisateur ayant accès au compte de récupération.

[Vous pouvez demander l'accès à un coffre-fort isolé de manière logique dans un autre compte \(étape 6 de l'aperçu\).](#)

Une fois qu'une équipe d'approbation a accédé à la demande, elle AWS Backup crée un coffre-fort de sauvegarde pour l'accès à la restauration dans le compte de restauration désigné afin que ce compte ait accès aux points de restauration du coffre-fort connecté logiquement séparé.

Console

Demandez l'accès à un coffre-fort isolé de manière logique

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à la section Backup vault dans le volet de navigation de gauche
3. Sélectionnez les coffres-forts accessibles via l'onglet MPA
4. Sélectionnez Demander l'accès au coffre-fort.
5. Entrez l'ARN du coffre-fort de sauvegarde source du coffre-fort à espacement logique auquel vous souhaitez accéder.
6. Entrez un nom facultatif pour le coffre de sauvegarde de l'accès à la restauration. Si vous n'entrez pas de nom, un nom AWS Backup sera attribué en fonction du nom du coffre-fort logiquement espacé.
7. Entrez un commentaire facultatif du demandeur expliquant le motif de la demande d'accès.
8. Sélectionnez Envoyer la demande pour soumettre la demande d'accès.

Les membres de l'équipe d'approbation associés au coffre source recevront une notification par e-mail pour approuver la demande.

Une fois la demande approuvée par le nombre requis (« seuil ») de membres de l'équipe, le coffre-fort de sauvegarde de l'accès à la restauration sera créé dans le compte de récupération.

CLI

Utilisez la commande `create-restore-access-backup-vault` de l'interface de ligne de commande :

```
aws backup create-restore-access-backup-vault \
--source-backup-vault-arn SOURCE_VAULT_ARN \
--backup-vault-name OPTIONAL_VAULT_NAME \
--requester-comment "OPTIONAL_COMMENT" \
--region REGION
```

Les membres de l'équipe d'approbation MPA associés au coffre source recevront une notification pour approuver la demande. Une fois la demande approuvée par le nombre requis (« seuil ») de membres de l'équipe, le coffre-fort de sauvegarde de l'accès à la restauration sera créé dans le compte de récupération.

Vous pouvez vérifier l'état du coffre en utilisant :

```
aws backup describe-backup-vault \
--backup-vault-name VAULT_NAME \
--region REGION
```

Dissociez l'équipe d'approbation multipartite du coffre-fort logiquement isolé

Demandeur : Administrateur du compte propriétaire du coffre-fort logiquement isolé.

[Vous pouvez dissocier une équipe d'approbation multipartite d'un coffre-fort isolé de manière logique \(étape 7 de l'aperçu\).](#)

Console

Dissocier l'équipe d'approbation du coffre-fort isolé de manière logique

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à la section Backup vault dans le volet de navigation de gauche.
3. Sélectionnez le coffre-fort de sauvegarde isolé de manière logique dont vous souhaitez dissocier l'équipe d'approbation.
4. Sur la page des détails du coffre-fort, sélectionnez Dissocier l'équipe d'approbation.
5. Entrez un commentaire facultatif du demandeur expliquant la raison de la dissociation.

6. Sélectionnez Envoyer la demande pour soumettre la demande de dissociation.

Les membres actuels de l'équipe d'approbation recevront une notification pour approuver la demande.

Une fois approuvée par le nombre requis de membres de l'équipe, l'équipe sera dissociée du coffre.

CLI

Utilisez la commande `disassociate-backup-vault-mpa-approval-team` de l'interface de ligne de commande :

```
aws backup disassociate-backup-vault-mpa-approval-team \  
--backup-vault-name VAULT_NAME \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Les membres actuels de l'équipe d'approbation de la MPA recevront une notification pour approuver la demande. Une fois approuvée par le nombre requis de membres de l'équipe, l'équipe sera dissociée du coffre.

Révoquer le coffre de sauvegarde de l'accès à la restauration

Demandeur : Administrateur du compte propriétaire du coffre-fort logiquement isolé.

Vous pouvez révoquer l'accès à un coffre-fort de sauvegarde avec accès à la restauration à partir du compte du coffre-fort source.

Console

Révoquer le coffre de sauvegarde de l'accès à la restauration

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à la section Backup vault dans le volet de navigation de gauche.
3. Sélectionnez le coffre-fort de sauvegarde isolé de manière logique dont vous souhaitez révoquer l'accès.
4. Sur la page de détails du coffre-fort, faites défiler la page vers le bas jusqu'à la section Accès via une approbation multipartite.

5. Recherchez le coffre-fort de sauvegarde de l'accès à la restauration que vous souhaitez révoquer, puis sélectionnez Demander la suppression de l'accès au coffre-fort.
6. Entrez un commentaire facultatif du demandeur expliquant le motif de la révocation.
7. Sélectionnez Envoyer la demande pour soumettre la demande de révocation.

Les membres de l'équipe d'approbation recevront une notification pour approuver la demande.

Une fois approuvé par le nombre requis de membres de l'équipe, le coffre de sauvegarde de l'accès à la restauration sera supprimé du compte de récupération

CLI

Tout d'abord, listez les coffres-forts de sauvegarde pour l'accès à la restauration associés à votre coffre-fort source :

```
aws backup list-restore-access-backup-vaults \  
--backup-vault-name SOURCE_VAULT_NAME \  
--region REGION
```

Ensuite, utilisez la commande CLI `revoke-restore-access-backup-vault` :

```
aws backup revoke-restore-access-backup-vault \  
--backup-vault-name SOURCE_VAULT_NAME \  
--restore-access-backup-vault-arn RESTORE_ACCESS_VAULT_ARN \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Les membres de l'équipe d'approbation recevront une notification pour approuver la demande. Une fois approuvé par le nombre requis de membres de l'équipe, le coffre de sauvegarde de l'accès à la restauration sera supprimé du compte de récupération.

Mettez à jour l'équipe d'approbation multipartite associée à un coffre-fort logiquement isolé

Demandeur : Administrateur du compte propriétaire du coffre-fort logiquement isolé.

[Vous pouvez mettre à jour l'équipe d'approbation multipartite associée à un coffre-fort isolé de manière logique \(étape 8 de la présentation\).](#)

Console

Mettre à jour l'équipe d'approbation associée à un coffre-fort isolé de manière logique

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à la section Backup vault dans le volet de navigation de gauche.
3. Sélectionnez le coffre-fort de sauvegarde isolé de manière logique pour lequel vous souhaitez informer l'équipe d'approbation.
4. Sur la page des détails du coffre-fort, sélectionnez Demander le changement d'équipe d'approbation.
5. Dans le menu déroulant, sélectionnez la nouvelle équipe d'approbation que vous souhaitez associer au coffre-fort.
6. Entrez un commentaire facultatif du demandeur expliquant la raison de la modification.
7. Sélectionnez Envoyer la demande pour soumettre la demande de modification.

Les membres actuels de l'équipe d'approbation recevront une notification par e-mail pour approuver la demande.

Une fois approuvée par le nombre requis de membres (seuil) de l'équipe MPA actuelle, la nouvelle équipe sera associée au coffre.

CLI

Utilisez la commande CLI `associate-backup-vault-mpa-approval-team` avec le nouvel ARN de l'équipe :

```
aws backup associate-backup-vault-mpa-approval-team \  
--backup-vault-name VAULT_NAME \  
--mpa-approval-team-arn NEW_MPA_TEAM_ARN \  
--requester-comment "OPTIONAL_COMMENT" \  
--region REGION
```

Les membres actuels de l'équipe d'approbation recevront une notification pour approuver la demande. Une fois approuvée par le nombre requis de membres (seuil) de l'équipe actuelle, la nouvelle équipe MPA sera associée au coffre.

Tâches d'approbateur

Un utilisateur membre d'une équipe d'approbation multipartite peut [approuver ou refuser les demandes](#) faisant partie d'une session. Les autres tâches incluent :

- [Répondre aux opérations demandées](#)
- [Afficher une équipe d'approbation](#)
- [Afficher l'historique des opérations](#)

Stratégies d'accès aux coffres

Avec AWS Backup, vous pouvez attribuer des politiques aux coffres-forts de sauvegarde et aux ressources qu'ils contiennent. L'attribution de politiques vous permet d'accorder l'accès aux utilisateurs afin qu'ils puissent créer des plans de sauvegarde et des sauvegardes à la demande, mais de limiter leur capacité à supprimer des points de récupération après leur création.

Pour plus d'informations sur l'utilisation de politiques permettant d'accorder ou de restreindre l'accès aux ressources, consultez [Stratégies basées sur l'identité et Stratégies basées sur une ressource](#) dans le Guide de l'utilisateur IAM. Vous pouvez également contrôler l'accès à l'aide de balises.

Vous pouvez utiliser les exemples de politiques suivants comme guide pour limiter l'accès aux ressources lorsque vous travaillez avec des AWS Backup coffres-forts. Contrairement aux autres politiques basées sur l'IAM, les politiques AWS Backup d'accès ne prennent pas en charge l'ajout d'un caractère générique dans la clé. Action

Pour obtenir la liste des Amazon Resource Names (ARNs) que vous pouvez utiliser pour identifier les points de récupération pour différents types de ressources, consultez la section relative [AWS Backup ressource ARNs](#) aux points de récupération spécifiques aux ressources. ARNs

Les politiques d'accès au coffre-fort contrôlent uniquement l'accès des utilisateurs à AWS Backup APIs. Certains types de sauvegarde, tels que les instantanés Amazon Elastic Block Store (Amazon EBS) et Amazon Relational Database Service (Amazon RDS), sont également accessibles à l'aide de ces services. APIs Vous pouvez créer des politiques d'accès distinctes dans IAM pour contrôler l'accès à ces types de sauvegarde APIs afin de contrôler totalement l'accès à ces types de sauvegarde.

Quelle que soit la politique d'accès du AWS Backup coffre, l'accès entre comptes pour toute action autre que `backup:CopyIntoBackupVault` sera rejeté, c'est-à-dire qu'il AWS Backup rejettera toute autre demande provenant d'un compte différent du compte de la ressource référencée.

Rubriques

- [Rejet de l'accès à un type de ressource dans un coffre-fort de sauvegarde](#)
- [Rejet de l'accès à un coffre-fort de sauvegarde](#)
- [Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde](#)

Rejet de l'accès à un type de ressource dans un coffre-fort de sauvegarde

Cette politique rejette l'accès aux opérations d'API spécifiées pour tous les instantanés Amazon EBS d'un coffre-fort de sauvegarde.

Rejet de l'accès à un coffre-fort de sauvegarde

Cette stratégie rejette l'accès aux opérations d'API spécifiées visant un coffre-fort de sauvegarde.

Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde

L'accès aux coffres-forts et la possibilité de supprimer des points de récupération qui y sont stockés sont déterminés par l'accès que vous accordez aux utilisateurs.

Suivez les étapes ci-après pour créer une stratégie d'accès basée sur les ressources sur un coffre-fort de sauvegarde qui empêche la suppression de toutes les sauvegardes dans le coffre-fort de sauvegarde.

Pour créer une stratégie d'accès basée sur les ressources pour un coffre-fort de sauvegarde

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation de gauche, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez un coffre-fort de sauvegarde dans la liste.
4. Dans la section Access policy (Stratégie d'accès), collez l'exemple JSON suivant. Cette stratégie empêche toute personne qui n'est pas le mandataire principal de supprimer un point de récupération dans le coffre-fort de sauvegarde cible.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "backup:DeleteRecoveryPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:userId": [
            "AIDA1234567890EXAMPLE",
            "ARO1234567890EXAMPLE:my-role-session",
            "ARO1234567890EXAMPLE:*",
            "112233445566"
          ]
        }
      }
    }
  ]
}
```

Pour autoriser les identités IAM de liste à l'aide de leur ARN, utilisez la clé de condition `aws:PrincipalArn` globale dans l'exemple suivant.

Pour plus d'informations sur l'obtention d'un ID unique pour une entité IAM, consultez [Obtention de l'identifiant unique](#) dans le Guide de l'utilisateur IAM.

Si vous souhaitez limiter cette possibilité à des types de ressources spécifiques, au lieu de `"Resource": "*"` , vous pouvez inclure explicitement les types de points de récupération à rejeter. Par exemple, pour les instantanés Amazon EBS, modifiez le type de ressource comme suit.

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. Choisissez Attach policy (Attacher la politique).

AWS Backup Verrou de coffre-fort

Note

AWS Backup Vault Lock a été évalué par Cohasset Associates pour une utilisation dans des environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour plus d'informations sur le lien entre AWS Backup Vault Lock et ces réglementations, consultez [l'évaluation de conformité de Cohasset Associates](#).

AWS Backup Vault Lock est une fonctionnalité optionnelle d'un coffre-fort de sauvegarde, qui peut être utile pour renforcer la sécurité et le contrôle de vos coffres-forts de sauvegarde. Lorsqu'un verrou est actif en mode conformité et que le délai de grâce est expiré, la configuration du coffre-fort ne peut pas être modifiée ou supprimée par le client, account/data le propriétaire ou AWS tant qu'elle contient des points de récupération. Chaque coffre-fort peut avoir un verrouillage de coffre-fort en place.

AWS Backup garantit que vos sauvegardes sont disponibles pour vous jusqu'à l'expiration de leur période de conservation. Si un utilisateur (y compris l'utilisateur root) tente de supprimer une sauvegarde ou de modifier les propriétés du cycle de vie dans un coffre verrouillé, AWS Backup il refusera l'opération.

- Les coffres-forts verrouillés en mode gouvernance peuvent être verrouillés par les utilisateurs disposant d'autorisations IAM suffisantes.
- Les coffres-forts verrouillés en mode conformité ne peuvent pas être supprimés une fois le délai de refroidissement (« délai de grâce ») expiré si des points de récupération se trouvent dans le coffre. Pendant le délai de grâce, vous pouvez toujours retirer le verrouillage de coffre-fort et modifier la configuration du verrouillage.

Modes de verrouillage du coffre-fort

Lorsque vous créez un verrouillage de coffre-fort, vous avez le choix entre deux modes : le mode Gouvernance ou le mode Conformité. Le mode Gouvernance est destiné à permettre à un coffre-fort d'être géré uniquement par des utilisateurs disposant de privilèges IAM suffisants. Le mode Gouvernance aide une organisation à répondre aux exigences de gouvernance, en garantissant que seul le personnel désigné peut apporter des modifications à un coffre-fort de sauvegarde. Le mode Conformité est destiné aux coffres-forts de sauvegarde dans lesquels le coffre-fort (et par extension, son contenu) ne devrait jamais être supprimé ou modifié avant la fin de la période de conservation

des données. Une fois qu'un coffre-fort en mode conformité est verrouillé, il est immuable, ce qui signifie que le verrou ne peut pas être retiré (le coffre-fort lui-même peut être supprimé s'il est vide et ne contient aucun point de récupération).

Un coffre-fort verrouillé en mode de gouvernance peut être géré ou supprimé par les utilisateurs disposant des autorisations IAM appropriées.

Un verrouillage de coffre-fort en mode Conformité ne peut être modifié ou supprimé par un utilisateur ou par AWS. Un verrou de coffre-fort en mode conformité dispose d'un délai de grâce que vous définissez avant qu'il ne soit verrouillé et que le contenu et le verrouillage du coffre-fort ne deviennent immuables.

Avantages de Vault Lock

AWS Backup Vault Lock offre plusieurs avantages, notamment :

- Configuration WORM (écriture unique, lecture multiple) pour toutes les sauvegardes que vous stockez et créez dans un coffre-fort de sauvegarde.
- Une couche de défense supplémentaire qui protège les sauvegardes (points de récupération) de vos coffres-forts de sauvegarde contre les suppressions involontaires ou malveillantes.
- Application de périodes de conservation, qui empêchent les suppressions anticipées par les utilisateurs privilégiés (y compris l'utilisateur Compte AWS root) et respectent les politiques et procédures de protection des données de votre organisation.

Verrouillage d'un coffre-fort de sauvegarde à l'aide de la console

Vous pouvez ajouter un verrou de coffre-fort à votre AWS Backup coffre-fort à l'aide de la console Backup.

Pour ajouter un verrouillage à votre coffre-fort de sauvegarde :

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Coffres-forts de sauvegarde. Cliquez sur le lien imbriqué sous les coffres-forts de sauvegarde appelés Verrouillages de coffre.
3. Sous Fonctionnement des verrouillages de coffre ou Verrouillages de coffre, cliquez sur + Créer un verrouillage de coffre.

4. Dans le volet Détails de verrouillage du coffre, choisissez le coffre-fort auquel vous souhaitez appliquer votre verrouillage.
5. Dans Mode de verrouillage de coffre, choisissez le mode dans lequel vous souhaitez que votre coffre-fort soit verrouillé. Pour plus d'informations sur le choix de vos modes, consultez [Modes de verrouillage du coffre-fort](#) plus haut sur cette page.
6. Pour la Période de rétention, choisissez les périodes de rétention minimale et maximale (les périodes de rétention sont facultatives). Les nouvelles tâches de sauvegarde et de copie créées dans le coffre-fort échoueront si elles ne sont pas conformes aux périodes de conservation que vous avez définies ; ces périodes ne s'appliqueront pas aux points de restauration déjà présents dans le coffre-fort.
7. Si vous avez choisi le mode Conformité, une section intitulée Date de début du verrouillage du coffre s'affiche. Si vous avez choisi le mode Gouvernance, rien ne s'affichera et cette étape peut être ignorée.

En mode Conformité, un verrouillage de coffre-fort dispose d'une période de réflexion entre sa création et le moment où le coffre-fort et son verrouillage deviennent immuables et inchangeables. Vous choisissez la durée de cette période (appelée délai de grâce), mais elle doit être d'au moins 3 jours (72 heures).

 Important

Une fois le délai de grâce expiré, le coffre-fort et son verrouillage sont immuables. Il ne peut être modifié ou supprimé par un utilisateur ou par AWS.

8. Lorsque vous êtes satisfait des choix de configuration, cliquez sur Création d'un verrouillage de coffre-fort.
9. Pour confirmer que vous souhaitez créer ce verrouillage dans le mode choisi, tapez `confirm` dans la zone de texte, puis cochez la case confirmant que la configuration est conforme à vos attentes.

Si les étapes ont été effectuées, une bannière « Succès » apparaîtra en haut de la console.

Verrouillage d'un coffre-fort de sauvegarde par programmation

Pour configurer AWS Backup Vault Lock, utilisez l'API [PutBackupVaultLockConfiguration](#). Les paramètres à inclure dépendent du mode de verrouillage du coffre-fort que vous souhaitez utiliser. Si vous souhaitez créer un verrouillage de coffre-fort en mode gouvernance, n'incluez pas

ChangeableForDays. Si ce paramètre est inclus, le verrouillage du coffre-fort sera créé en mode conformité.

Voici un exemple d'interface de ligne de commande pour la création d'un verrouillage de coffre-fort en mode conformité :

```
aws backup put-backup-vault-lock-configuration \  
  --backup-vault-name my_vault_to_lock \  
  --changeable-for-days 3 \  
  --min-retention-days 7 \  
  --max-retention-days 30
```

Voici un exemple d'interface de ligne de commande pour la création d'un verrouillage de coffre-fort en mode gouvernance :

```
aws backup put-backup-vault-lock-configuration \  
  --backup-vault-name my_vault_to_lock \  
  --min-retention-days 7 \  
  --max-retention-days 30
```

Vous pouvez configurer quatre options.

1. **BackupVaultName**

Nom du coffre-fort à verrouiller.

2. **ChangeableForDays** (à inclure uniquement pour le mode conformité)

Ce paramètre indique de AWS Backup créer le verrou du coffre-fort en mode de conformité. Omettez ce paramètre si vous avez l'intention de créer le verrouillage en mode gouvernance.

Cette valeur est exprimée en jours. Le nombre doit être entre 3 et 36 500 ; dans le cas contraire, une erreur sera renvoyée.

De la création de ce verrouillage de coffre-fort jusqu'à l'expiration de la date spécifiée, le verrouillage du coffre-fort peut être retiré du coffre-fort avec `DeleteBackupVaultLockConfiguration`. Pendant ce temps, vous pouvez également modifier la configuration avec `PutBackupVaultLockConfiguration`.

À compter de la date spécifiée déterminée par ce paramètre, le coffre-fort de sauvegarde sera immuable et ne pourra être ni modifié ni supprimé.

3. **MaxRetentionDays** (facultatif)

Cette valeur numérique est exprimée en jours. La période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération.

La durée de rétention maximale que vous choisissez doit être conforme aux politiques de rétention des données de votre organisation. Si votre organisation demande que les données soient conservées pendant un certain temps, cette valeur peut être définie sur cette période (en jours). Par exemple, les données financières ou bancaires peuvent devoir être conservées pendant 7 ans (environ 2 557 jours, selon les années bissextiles).

Si ce n'est pas spécifié, AWS Backup Vault Lock n'appliquera pas de période de conservation maximale. Si cela est spécifié, les tâches de sauvegarde et de copie vers ce coffre-fort dont les périodes de rétention du cycle de vie sont supérieures à la période de rétention maximale échoueront. Les points de récupération déjà enregistrés dans le coffre-fort avant la création de son verrouillage ne sont pas affectés. La période de rétention maximale la plus longue que vous puissiez spécifier est de 36 500 jours (environ 100 ans).

4. **MinRetentionDays**(facultatif ; obligatoire pour CloudFormation)

Cette valeur numérique est exprimée en jours. Il s'agit de la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Ce paramètre doit être défini en fonction de la durée requise par votre organisation pour conserver les données. Par exemple, si la réglementation ou la loi exigent que les données soient conservées pendant au moins sept ans, la valeur en jours serait d'environ 2 557, selon les années bissextiles.

Si ce n'est pas spécifié, AWS Backup Vault Lock n'appliquera pas de période de conservation minimale. Si cela est spécifié, les tâches de sauvegarde et de copie vers ce coffre-fort dont les périodes de rétention du cycle de vie sont inférieures à la période de rétention minimale échoueront. Les points de récupération déjà enregistrés dans le coffre-fort avant le verrouillage du AWS Backup coffre-fort ne sont pas affectés. La période de rétention minimale la plus courte que vous puissiez spécifier est d'un jour.

Vérifiez la configuration Vault Lock d'un AWS Backup coffre-fort de sauvegarde

Vous pouvez consulter les détails de AWS Backup Vault Lock sur un coffre-fort à tout moment en appelant [DescribeBackupVault](#) ou [ListBackupVaults](#) APIs.

Pour déterminer si vous avez appliqué un verrouillage de coffre-fort à un coffre-fort de sauvegarde, appelez `DescribeBackupVault` et vérifiez la propriété `Locked`. Si `"Locked": true`, comme dans l'exemple suivant, vous avez appliqué AWS Backup Vault Lock à votre coffre-fort de sauvegarde.

```
{
  "BackupVaultName": "my_vault_to_lock",
  "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
  "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
  "CreationDate": "2021-09-24T12:25:43.030000-07:00",
  "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
  "NumberOfRecoveryPoints": 1,
  "Locked": true,
  "MinRetentionDays": 7,
  "MaxRetentionDays": 30,
  "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

La sortie précédente confirme les options suivantes :

1. `Locked` est un booléen qui indique si vous avez appliqué AWS Backup Vault Lock à ce coffre-fort de sauvegarde. `True` signifie que AWS Backup Vault Lock entraîne l'échec des opérations de suppression ou de mise à jour des points de restauration stockés dans le coffre-fort (que vous soyez toujours dans le délai de grâce de refroidissement ou non).
2. `LockDate` est la date et l'heure UTC auxquelles votre délai de grâce de réflexion prend fin. Passé ce délai, vous ne pouvez plus ni supprimer ni modifier le verrouillage de ce coffre-fort. Utilisez n'importe quel convertisseur horaire accessible au public pour convertir cette chaîne en heure locale.

Si `"Locked": false`, comme dans l'exemple suivant, vous n'avez pas appliqué de verrouillage de coffre-fort (ou un verrouillage précédent a été supprimé).

```
{
  "BackupVaultName": "my_vault_to_lock",
  "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
  "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
```

```
"CreationDate": "2021-09-24T12:25:43.030000-07:00",  
"CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",  
"NumberOfRecoveryPoints": 3,  
"Locked": false  
}
```

Suppression du verrouillage de coffre-fort pendant le délai de grâce (mode Conformité)

Pour supprimer le verrouillage de votre coffre-fort pendant le délai de grâce (le temps qui suit le verrouillage du coffre-fort mais avant votreLockDate) à l'aide de la AWS Backup console,

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le menu de navigation de gauche, sous Mon compte, cliquez sur Coffres de sauvegarde, puis sur Backup Vault Lock.
3. Cliquez sur le verrouillage de coffre-fort que vous souhaitez supprimer, puis sur Gérer le verrouillage de coffre.
4. Cliquez sur Supprimer le verrouillage du coffre.
5. Une boîte d'avertissement apparaît, vous demandant de confirmer votre intention de supprimer le verrouillage de coffre-fort. Tapez `confirm` dans la zone de texte, puis cliquez sur Confirmer.

Si toutes les étapes ont été effectuées, une bannière « Succès » apparaîtra en haut de l'écran de la console.

Pour supprimer le verrouillage de votre coffre-fort pendant le délai de grâce à l'aide d'une commande d'interface de ligne de commande, utilisez [DeleteBackupVaultLockConfiguration](#) comme cet exemple d'interface de ligne de commande :

```
aws backup delete-backup-vault-lock-configuration \  
    --backup-vault-name my_vault_to_lock
```

Compte AWS fermeture avec coffre verrouillé

Lorsque vous fermez un site Compte AWS contenant un coffre-fort de sauvegarde AWS et que vous AWS Backup suspendez votre compte pendant 90 jours avec vos sauvegardes intactes. Si vous ne

ouvrez pas votre compte pendant ces 90 jours, le contenu de votre coffre-fort de sauvegarde est AWS supprimé, même si AWS Backup Vault Lock était en place.

Considérations supplémentaires en matière de sécurité

AWS Backup Vault Lock ajoute une couche de sécurité supplémentaire à votre défense approfondie de la protection des données. Le verrouillage du coffre-fort peut être combiné avec les autres fonctionnalités de sécurité suivantes :

- [Chiffrement de vos points de récupération](#)
- AWS Backup les [politiques d'accès au coffre-fort et au point de récupération](#), qui vous permettent d'accorder ou de refuser des autorisations au niveau du coffre-fort,
- [AWS Backup les meilleures pratiques en matière de sécurité](#), y compris sa bibliothèque de [politiques gérées par le client](#) qui vous permet d'accorder ou de refuser des autorisations de sauvegarde et de restauration par le service AWS pris en charge, et
- [AWS Backup Audit Manager](#), qui vous permet d'automatiser les contrôles de conformité de vos sauvegardes par rapport à [une liste de contrôles](#) que vous définissez.

Vous pouvez utiliser [Création de frameworks à l'aide de l' AWS Backup API](#) pour le contrôle [Les ressources sont incluses dans un plan de sauvegarde avec un AWS Backup Vault Lock](#) avec AWS Backup Audit Manager pour vous assurer que les ressources que vous souhaitez utiliser sont protégées par un verrouillage de coffre-fort.

- Les mécanismes qui rendent les ressources inactives peuvent avoir un impact sur la capacité à les restaurer. Bien qu'ils ne puissent toujours pas être supprimés dans un coffre verrouillé, ils peuvent être dans un état autre qu'actif. Par exemple, le paramètre Amazon Elastic Compute Cloud qui vous permet de [désactiver une AMI](#) peut bloquer temporairement la possibilité de restaurer les sauvegardes des EC2 instances. Cela concerne tous les points de EC2 restauration, même les sauvegardes touchées par le verrouillage d'un coffre-fort ou par un blocage légal.

Si une EC2 sauvegarde est désactivée, vous pouvez [réactiver une AMI désactivée](#). Une fois réactivé, il peut être restauré. Pour bloquer la fonctionnalité de désactivation de l'AMI, vous pouvez utiliser des politiques IAM pour ne pas l'autoriser `ec2:DisableImage`.

 Note

AWS Backup Vault Lock n'est pas la même fonctionnalité qu'[Amazon Glacier Vault Lock](#), qui n'est compatible qu'avec Amazon Glacier.

Création, maintenance et restauration de sauvegardes

Une sauvegarde, également appelée point de récupération, représente le contenu d'une ressource, comme par exemple un volume Amazon Elastic Block Store (Amazon EBS) ou une table Amazon DynamoDB, à un instant donné. Le point de restauration est un terme qui fait généralement référence aux différentes sauvegardes des AWS services, telles que les instantanés Amazon EBS et les sauvegardes DynamoDB. Les termes point de récupération et sauvegarde sont utilisés indifféremment.

AWS Backup enregistre les points de restauration dans des coffres-forts de sauvegarde, que vous pouvez organiser en fonction des besoins de votre entreprise. Par exemple, vous pouvez enregistrer un ensemble de ressources contenant des informations financières pour l'exercice 2020. Lorsque vous devez récupérer une ressource, vous pouvez utiliser la AWS Backup console ou le AWS Command Line Interface (AWS CLI) pour rechercher et récupérer la ressource dont vous avez besoin.

Chaque point de récupération présente un ID unique. L'ID unique est à la fin de l'Amazon Resource Name (ARN) du point de récupération. Pour des exemples de point de récupération ARNs et d'ID unicité, consultez le tableau dans [Ressources et opérations](#).

Important

Pour éviter des frais supplémentaires, configurez votre politique de rétention avec une durée de stockage à chaud d'au moins une semaine. Pour de plus amples informations, veuillez consulter [Comptage, coûts et facturation pour AWS Backup](#).

Les sections suivantes proposent une vue d'ensemble des tâches de gestion des sauvegardes élémentaires dans AWS Backup.

Rubriques

- [Création d'une sauvegarde à la demande à l'aide de AWS Backup](#)
- [Sauvegardes et point-in-time restauration continues \(PITR\)](#)
- [Backup créé par type de ressource](#)
- [Sauvegarde et copie de balises](#)
- [Suppression d'une sauvegarde](#)

- [Backup et modification des balises](#)
- [Recherche de sauvegardes](#)
- [Hiérarchisation des sauvegardes](#)
- [Restaurer une sauvegarde par type de ressource](#)
- [Tests de restauration](#)
- [Arrêter une tâche de sauvegarde](#)
- [Afficher les sauvegardes existantes](#)

Création d'une sauvegarde à la demande à l'aide de AWS Backup

Sur la AWS Backup console, la page Ressources protégées répertorie les ressources qui ont été sauvegardées au AWS Backup moins une fois. Si vous l'utilisez AWS Backup pour la première fois, aucune ressource (telle que les volumes Amazon EBS ou les bases de données Amazon RDS) n'est répertoriée sur cette page. C'est le cas même si une ressource a été affectée à un plan de sauvegarde, si ce plan de sauvegarde n'a pas exécuté de tâche de sauvegarde planifiée au moins une fois.

Remarque : une sauvegarde à la demande commence immédiatement à sauvegarder votre ressource. Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

Les sauvegardes à la demande ne peuvent pas être utilisées avec la point-in-time restauration (PITR), car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la sauvegarde, tandis que PITR utilise [des sauvegardes continues](#), qui enregistrent les modifications au fil du temps.

Considérations

- Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.
- Lorsque les sauvegardes expirent et sont marquées pour suppression dans le cadre de votre politique de cycle de vie, AWS Backup supprime les sauvegardes à un moment choisi au hasard au cours des 8 heures suivantes. Cette fenêtre permet de garantir des performances constantes.

- Pour les EC2 ressources Amazon, copie AWS Backup automatiquement les balises de ressources individuelles et de groupe existantes, en plus de toutes les balises que vous ajoutez au cours de cette étape.
- AWS Backup utilise EC2 les sauvegardes dont le comportement par défaut est « sans redémarrage ». AWS Backup prend actuellement en charge les ressources exécutées sur Amazon EC2, et certains types d'instances ne sont pas pris en charge. Pour de plus amples informations, veuillez consulter [Création de sauvegardes Windows VSS](#).

Pour créer une sauvegarde à la demande

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le tableau de bord, choisissez Créer une sauvegarde à la demande. Ou, dans le panneau de navigation, choisissez Ressources protégées, puis Créer une sauvegarde à la demande.
3. Pour la page Type de ressource, choisissez le type de ressource que vous souhaitez sauvegarder. Par exemple, choisissez DynamoDB pour les tables Amazon DynamoDB.
4. Choisissez le nom ou l'ID de la ressource à protéger. Par exemple, choisissez le nom de la table DynamoDB pour Amazon DynamoDB.
5. Assurez-vous que Create backup now (Créer une sauvegarde maintenant) est sélectionné.
6. Si le type de ressource prend en charge la transition vers le stockage à froid, le stockage à froid est présent. Pour plus d'informations, consultez la colonne Cycle de vie du stockage à froid dans le tableau [Disponibilité des fonctionnalités par ressource](#).

Pour spécifier à quel moment cette sauvegarde sera placée en stockage à froid, choisissez Déplacer les sauvegardes du stockage à chaud vers le stockage à froid, puis spécifiez la durée du stockage à chaud.

7. Pour Durée de conservation totale, spécifiez le nombre de jours. Si vous avez spécifié la durée d'entreposage au froid, la période de conservation est divisée entre le stockage à chaud et le stockage au froid.
8. Sélectionnez un Coffre de sauvegarde existant ou créez-en un. Si vous choisissez Créer un coffre de sauvegarde, une nouvelle page s'ouvre afin que vous puissiez créer un coffre. Une fois que vous avez terminé, vous revenez à la page Créer une sauvegarde à la demande.
9. Pour le rôle IAM, choisissez le rôle par défaut ou un rôle que vous avez créé.
10. Pour attribuer un tag à votre sauvegarde à la demande, développez le champ Tags ajoutés aux points de restauration, choisissez Ajouter un nouveau tag, puis entrez une clé de tag et une valeur de tag.

11. Les options de paramètres de sauvegarde avancés varient en fonction du type de ressource :
 - Pour les EC2ressources : pour prendre des instantanés cohérents avec les applications à l'aide du service Windows Volume Shadow Copy (VSS), choisissez Windows VSS.
 - Pour les ressources Amazon S3 : vous pouvez choisir d'exclure les listes de contrôle d'accès (ACLs) de votre sauvegarde en ne sélectionnant pas les listes de contrôle d'accès aux sauvegardes (ACLs).
12. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Cela ouvre la page Tâches, où vous pouvez voir la liste des tâches et consulter le statut des tâches.

Sauvegardes et point-in-time restauration continues (PITR)

Pour certaines ressources, AWS Backup prend en charge les sauvegardes et point-in-time restaurations continues (PITR) en plus des sauvegardes instantanées.

Avec les sauvegardes continues, vous pouvez restaurer les ressources AWS Backup prises en charge en les rétablissant à l'heure précise de votre choix, avec une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. Le PITR fonctionne en accédant à votre sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure à laquelle vous avez indiqué de procéder AWS Backup à la restauration.

Il est également possible d'effectuer des sauvegardes d'instantanés toutes les heures. Les sauvegardes d'instantanés peuvent être stockées pendant 100 ans au maximum. Les instantanés peuvent être copiés pour des sauvegardes complètes ou incrémentielles.

Étant donné que les sauvegardes continues et d'instantanés présentent des avantages différents, nous vous recommandons de protéger vos ressources à l'aide de règles de sauvegarde continues et instantanées.

Une sauvegarde à la demande commence immédiatement à sauvegarder vos ressources. Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

Vous ne pouvez pas utiliser de [sauvegardes à la demande](#) avec PITR, car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la

sauvegarde, tandis que PITR utilise des sauvegardes continues, qui enregistrent les modifications au fil du temps.

Vous pouvez opter pour des sauvegardes continues pour les ressources prises en charge lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API. Le plan de sauvegarde continue crée un point de restauration continue et met à jour ce point de restauration chaque fois que la tâche est exécutée.

Table des matières

- [Point-in-time considérations relatives au rétablissement](#)
- [Services pris en charge pour la sauvegarde continue et le PITR](#)
- [Résultat d'une sauvegarde continue](#)
- [Restauration d'une sauvegarde continue](#)
- [Arrêt ou suppression des sauvegardes continues](#)
- [Copie des sauvegardes continues](#)
- [Modification de votre période de rétention](#)
- [Suppression de la seule règle de sauvegarde continue d'un plan de sauvegarde](#)

Point-in-time considérations relatives au rétablissement

Tenez compte des considérations suivantes en matière de point-in-time rétablissement :

- Retour automatique aux instantanés : si AWS Backup n'est pas en mesure d'effectuer une sauvegarde continue, il essaie plutôt d'effectuer une sauvegarde par instantané.
- Aucune prise en charge des sauvegardes continues à la demande : AWS Backup ne prend pas en charge la sauvegarde continue à la demande, car la sauvegarde à la demande enregistre un moment précis, alors que la sauvegarde continue enregistre les modifications au fil du temps.
- Aucune prise en charge pour la transition vers le stockage à froid : les sauvegardes continues ne prennent pas en charge la transition vers le stockage à froid, car la transition vers le stockage à froid nécessite une période de transition minimale de 90 jours, tandis que les sauvegardes continues ont une période de rétention maximale de 35 jours.
- Restauration de l'activité récente : l'activité Amazon RDS autorise les restaurations jusqu'aux 5 dernières minutes d'activité ; Amazon S3 autorise les restaurations jusqu'aux 15 dernières minutes d'activité.

 Important

Une seule ressource ne peut faire l'objet que d'une seule sauvegarde continue. Développez ci-dessous pour plus de détails et les meilleures pratiques.

Sauvegardes continues superposées sur la même ressource

Chaque ressource (telle qu'un compartiment Amazon S3 ou une base de données Amazon RDS) ne peut faire l'objet que d'une seule sauvegarde continue (point de restauration) ; les sauvegardes continues supplémentaires sont redondantes. Lorsque plusieurs politiques, plans ou règles de sauvegarde demandent de AWS Backup créer plusieurs sauvegardes continues pour la même ressource, le processus suivant s'applique :

- Si plusieurs règles spécifient que plusieurs sauvegardes continues doivent se trouver dans un même coffre, suivez la règle AWS Backup ayant la plus longue période de conservation (cycle de vie) et ignore les règles supplémentaires.
- Si plusieurs règles spécifient que plusieurs sauvegardes continues doivent se trouver dans plusieurs coffres-forts, AWS Backup crée une sauvegarde continue conformément à la première règle traitée. Chaque règle suivante spécifiant une sauvegarde continue pour une ressource qui possède déjà une sauvegarde continue se traduira par une sauvegarde instantanée (périodique) à la place.

Lorsque des plans de sauvegarde continue dupliqués se produisent, les sauvegardes instantanées créées après le point de restauration continue peuvent afficher un état de `Completed with issues`. Les informations détaillées de ce point de récupération afficheront une erreur similaire à `“Enabling continuous backup failed, because of the following error: PITR already configured in backup plan: [ARN]”`. Cette erreur indique qu'au moins une sauvegarde continue est déjà configurée (pour un point de restauration différent de celui contenant l'erreur). Cette première sauvegarde continue (point de restauration) peut être utilisée pour une restauration instantanée (PITR) tant qu'elle a un statut de `COMPLETED`.

Pour éviter la création de snapshots involontaires présentant des problèmes (et des messages d'erreur), passez en revue la stratégie de sauvegarde de votre organisation. Si nécessaire, ajustez les plans et les politiques de sauvegarde qui créent plusieurs sauvegardes continues de la même ressource.

Une fois que vous avez effectué des ajustements qui se traduisent par une seule sauvegarde continue pour une ressource, les sauvegardes instantanées sont conservées conformément au cycle de vie spécifié du plan qui les a créées, puis elles sont transférées EXPIRED et supprimées. La sauvegarde continue et sa capacité point-in-time de restauration seront maintenues conformément à la règle qui l'a créée.

Services pris en charge pour la sauvegarde continue et le PITR

AWS Backup prend en charge les sauvegardes et point-in-time les restaurations continues pour les services et applications suivants :

Amazon S3

Pour activer la PITR pour les sauvegardes S3, les sauvegardes continues doivent faire partie du plan de sauvegarde.

Bien que la PITR puisse être active dans cette sauvegarde d'origine du compartiment source, les copies de destination entre régions ou entre comptes ne comporteront pas la PITR, et la restauration à partir de ces copies les rétablira la date à laquelle elles ont été créées (les copies seront des copies instantanées) au lieu d'être restaurées à un moment précis.

AWS Backup pour S3 repose sur la réception d'événements S3 via Amazon EventBridge. Si ce paramètre est désactivé dans les paramètres de notification des compartiments S3, les sauvegardes continues s'arrêteront pour ces compartiments, le paramètre étant désactivé. Pour plus d'informations, consultez la section [Utilisation EventBridge](#).

RDS

Programmes de sauvegarde : lorsqu'un AWS Backup plan crée à la fois des instantanés Amazon RDS et des sauvegardes continues, il AWS Backup planifie intelligemment vos fenêtres de sauvegarde afin de les coordonner avec la fenêtre de maintenance Amazon RDS afin d'éviter les conflits. Pour éviter davantage les conflits, la configuration manuelle de la fenêtre de sauvegarde automatique Amazon RDS n'est pas disponible. RDS prend des instantanés une fois par jour, même si un plan de sauvegarde prévoit une fréquence différente de celle d'une sauvegarde par jour.

Paramètres : une fois que vous avez appliqué une règle de sauvegarde AWS Backup continue à une instance Amazon RDS, vous ne pouvez pas créer ou modifier les paramètres de sauvegarde continue pour cette instance dans Amazon RDS ; les modifications doivent être effectuées via la AWS Backup console ou la CLI AWS Backup .

Transfert du contrôle de la sauvegarde continue d'une instance Amazon RDS vers Amazon RDS :

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Supprimez tous les plans de sauvegarde Amazon RDS avec une sauvegarde continue protégeant cette ressource.
4. Choisissez Coffres-forts de sauvegarde. Supprimez le point de récupération des sauvegardes continues de votre coffre-fort de sauvegarde. Vous pouvez également attendre la fin de leur période de conservation, ce qui entraînera AWS Backup la suppression automatique du point de récupération.

Une fois ces étapes terminées, le contrôle continu des sauvegardes de vos ressources AWS Backup sera transféré à Amazon RDS.

AWS CLI

Appelez l'opération de l'API `DisassociateRecoveryPoint`.

Pour en savoir plus, veuillez consulter la section [DisassociateRecoveryPoint](#).

Autorisations IAM requises pour les sauvegardes continues Amazon RDS

- À utiliser AWS Backup pour configurer des sauvegardes continues pour votre base de données Amazon RDS, vérifiez que l'autorisation d'API `rds:ModifyDBInstance` existe dans le rôle IAM défini par la configuration de votre plan de sauvegarde. Pour restaurer les sauvegardes continues Amazon RDS, vous devez ajouter l'autorisation `rds:RestoreDBInstanceToPointInTime` au rôle IAM que vous avez soumis pour la tâche de restauration. Vous pouvez utiliser le AWS Backup `default service role` pour effectuer des sauvegardes et des restaurations.
- Pour décrire la plage de temps disponible pour le point-in-time rétablissement, AWS Backup appelez `rds:DescribeDBInstanceAutomatedBackups`. Dans la AWS Backup console, vous devez disposer de l'autorisation d'`rds:DescribeDBInstanceAutomatedBackupsAPI` dans votre politique gérée Gestion des identités et des accès AWS (IAM). Vous pouvez utiliser les politiques gérées par `AWSBackupFullAccess` ou `AWSBackupOperatorAccess`. Les deux politiques disposent de toutes les autorisations requises. Pour plus d'informations, consultez [Stratégies gérées](#).

Périodes de conservation : lorsque vous modifiez votre période de rétention PITR, AWS Backup appellez [ModifyDBInstanceet appliquez cette modification](#), en commençant par la sauvegarde suivante, conformément à la règle de fréquence définie dans le plan de sauvegarde.

Copies des sauvegardes continues d'Amazon RDS :

- Les tâches de copie d'instantanés incrémentielles sont traitées plus rapidement que les tâches de copie d'instantanés complets. La conservation d'une copie précédente d'un instantané jusqu'à ce que la nouvelle tâche de copie soit terminée peut réduire la durée de la tâche de copie. Si vous choisissez de copier des instantanés à partir d'instances de base de données RDS, il est important de noter que la suppression initiale des copies précédentes entraînera la création de copies instantanées complètes (au lieu de copies incrémentielles). Pour plus d'informations sur l'optimisation des copies, consultez [Copie d'instantané incrémentielle](#) dans le Guide de l'utilisateur Amazon RDS.
- Création de copies des sauvegardes continues Amazon RDS : vous ne pouvez pas créer de copies des sauvegardes continues Amazon RDS car AWS Backup Amazon RDS n'autorise pas la copie des journaux de transactions. Il AWS Backup crée plutôt un instantané et le copie à la fréquence spécifiée dans le plan de sauvegarde.

Restaurations : vous pouvez effectuer une point-in-time restauration à l'aide d'Amazon RDS AWS Backup ou d'Amazon RDS. Pour les instructions relatives à AWS Backup la console, consultez [Restaurer une base de données Amazon RDS](#). Pour obtenir des instructions Amazon RDS, consultez [Restauration d'une instance de base de données à une date spécifiée](#) dans le Guide de l'utilisateur Amazon RDS.

 Tip

Une instance de base de données multi-AZ (zone de disponibilité) définie sur ne Always On doit pas avoir de rétention des sauvegardes définie sur zéro. En cas d'erreur, utilisez AWS CLI la commande `disassociate-recovery-point` au lieu de `delete-recovery-point`, puis remplacez le paramètre de rétention par 1 dans vos paramètres Amazon RDS.

Pour des informations générales sur le fonctionnement avec Amazon RDS, consultez le [Guide de l'utilisateur Amazon RDS](#).

Aurora

Pour activer la sauvegarde continue de vos ressources Aurora, consultez les étapes décrites dans la première section de cette page.

La procédure de restauration d'un cluster Aurora à un instant dans le passé est une [variante des étapes de restauration d'un instantané d'un cluster Aurora](#).

Lorsque vous effectuez une restauration à un instant dans le passé, la console affiche une section heure de restauration. Consultez Restauration d'une sauvegarde continue plus bas sur cette page dans [Utilisation des sauvegardes continues](#).

Instances SAP HANA sur Amazon EC2

Vous pouvez effectuer [des sauvegardes continues](#), qui peuvent être utilisées avec la point-in-time restauration (PITR) (notez que les sauvegardes à la demande préservent les ressources dans l'état dans lequel elles ont été prises, tandis que PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps).

Grâce aux sauvegardes continues, vous pouvez restaurer votre base de données SAP HANA sur une EC2 instance en la ramenant à l'heure précise de votre choix, dans un délai d'une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. La restauration PITR fonctionne en accédant à votre sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure indiquée AWS Backup pour la restauration.

Vous pouvez opter pour les sauvegardes continues lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API.

Pour activer les sauvegardes continues à l'aide de la console

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sous Règles de sauvegarde, choisissez Ajouter une règle de sauvegarde.
4. Dans la section Configuration de règle de backup, sélectionnez Activer les sauvegardes continues pour les ressources prises en charge.

Une fois que vous avez désactivé le [PITR \(point-in-timerestoration\)](#) pour les sauvegardes de base de données SAP HANA, les journaux continueront d'être envoyés AWS Backup jusqu'à expiration du point de restauration (statut égal à). EXPIRED) Vous pouvez passer à un autre emplacement de sauvegarde des journaux dans SAP HANA pour arrêter la transmission des journaux à AWS Backup.

Un point de restauration continue dont l'état est égal à STOPPED indique qu'un point de restauration continue a été interrompu ; en d'autres termes, les journaux transmis par SAP HANA à AWS Backup ce point et indiquant les modifications incrémentielles apportées à une base de données présentent une lacune. Les points de récupération qui se produisent pendant cet intervalle de temps ont un statut STOPPED..

Pour les problèmes que vous pouvez rencontrer lors des tâches de sauvegardes continues (points de récupération), consultez la section [Dépannage de la restauration SAP HANA](#) dans ce guide.

Résultat d'une sauvegarde continue

Vous pouvez utiliser la AWS Backup console pour trouver votre sauvegarde continue.

Pour rechercher une sauvegarde continue à l'aide de la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Coffres de sauvegarde, puis choisissez votre coffre-fort de sauvegarde dans la liste.
3. Dans la section Sauvegardes, dans la colonne Type de sauvegarde, triez les points de restauration En continu. Vous pouvez également trier par ID de point de récupération pour le préfixe En continu.

Restauration d'une sauvegarde continue

Pour restaurer une sauvegarde continue à l'aide de la AWS Backup console

- Pendant le processus de restauration PITR, la AWS Backup console affiche une section sur l'heure de restauration. Dans cette section, vous effectuez les opérations suivantes :
 - Choisir de restaurer à la Dernière heure de restauration.
 - Choisir Spécifier la date et l'heure pour entrer vos propres date et heure pendant votre période de rétention.

Pour restaurer une sauvegarde continue à l'aide de l' AWS Backup API

1. Pour Amazon S3, consultez [Utiliser l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration S3](#).
2. Pour Amazon RDS, consultez [Utiliser l' AWS Backup API, la CLI ou le SDK pour restaurer les points de récupération Amazon RDS](#).

Arrêt ou suppression des sauvegardes continues

Vous pouvez arrêter la création de sauvegardes continues ou supprimer des sauvegardes spécifiques (point-in-time-recovery ou points PITR).

Si vous souhaitez arrêter les sauvegardes continues, vous devez supprimer la règle de sauvegarde continue de votre plan de sauvegarde. Si vous souhaitez arrêter les sauvegardes continues pour une ou plusieurs ressources, mais pas pour toutes les ressources, créez un nouveau plan de sauvegarde avec la règle de sauvegarde continue pour les ressources que vous souhaitez toujours sauvegarder en continu. Si au contraire vous supprimez uniquement un point de récupération de sauvegarde continue de votre coffre-fort de sauvegarde, votre plan de sauvegarde continuera à exécuter la règle de sauvegarde continue, créant ainsi un nouveau point de récupération.

Cependant, même après avoir supprimé votre règle de sauvegarde continue, AWS Backup mémorise la période de conservation indiquée par votre règle de sauvegarde désormais supprimée. Il supprimera automatiquement votre point de récupération continue de votre coffre-fort de sauvegarde en fonction de la période de rétention que vous avez spécifiée.

Lorsque vous supprimez des points de récupération Amazon RDS, pensez à :

- Une instance de base de données multi-AZ (zone de disponibilité) définie sur `Always On` doit pas avoir de rétention des sauvegardes définie sur zéro. En cas d'erreur, utilisez AWS CLI la commande `disassociate-recovery-point` au lieu de `delete-recovery-point`, puis remplacez le paramètre de rétention par 1 dans vos paramètres Amazon RDS.
- Lorsqu'un point de point-in-time restauration (une sauvegarde créée par une sauvegarde continue) pour Amazon RDS est supprimé, le redémarrage de la base de données est déclenché et les journaux binaires sont désactivés. Pour plus de détails, consultez [Période de rétention des sauvegardes](#) dans le Guide de l'utilisateur Amazon RDS.

Lorsque vous supprimez des points de restauration Aurora, prenez en compte les points suivants :

Si cette option est sélectionnée pour un point de restauration Amazon Aurora, AWS Backup définit la période de rétention à 1 jour. Les sauvegardes Aurora ne peuvent pas être complètement supprimées tant que le cluster source n'a pas également été supprimé.

Copie des sauvegardes continues

Si une règle de sauvegarde continue spécifie également une copie entre comptes ou entre régions et AWS Backup prend en charge l'opération pour le type de ressource, AWS Backup prend un instantané de la ressource et copie l'instantané dans le coffre de destination. Pour en savoir plus sur la copie de vos points de récupération entre comptes et régions, consultez [Copie d'une sauvegarde](#).

Les sauvegardes continues créent des sauvegardes périodiques conformément à la fréquence définie dans la règle du plan de sauvegarde dans la and/or région du compte de destination.

AWS Backup ne prend pas en charge les copies à la demande de sauvegardes continues.

Modification de votre période de rétention

Vous pouvez l'utiliser AWS Backup pour augmenter ou diminuer la période de rétention de votre règle de sauvegarde continue existante. La période de rétention minimale est de 1 jour. La période de rétention maximale est de 35 jours. La modification de la période de conservation prendra effet lorsque la prochaine sauvegarde sera terminée après cette modification.

Période de conservation par service

Le comportement de rétention peut être spécifique au type de ressource sauvegardé dans le point de restauration.

Amazon S3

Lorsqu'une période de rétention d'un point de restauration continu Amazon S3 est modifiée (augmentée ou diminuée), le statut de ce point de récupération devient le même **STOPPED**. Un nouveau point de restauration continu avec les paramètres de rétention modifiés sera créé.

Amazon Aurora et Amazon RDS

Pour les points de restauration des ressources Aurora et Amazon RDS, un seul point de récupération est possible à la fois. Aucun nouveau point de restauration n'est créé lorsqu'une période de rétention est modifiée ; le point de restauration existant est plutôt AWS Backup mis à jour en fonction des spécifications de conservation du plan de sauvegarde.

Assurez-vous de définir la période de conservation de ces sauvegardes de manière à ce qu'elle soit supérieure à la fréquence des sauvegardes afin d'éviter que le point de restauration passe à EXPIRED l'état actuel.

 Tip

Une règle de fréquence de sauvegarde pour une sauvegarde continue n'est pas la même chose qu'un instantané de sauvegarde périodique. Chaque plan de sauvegarde, même s'il ne crée pas de capture instantanée, a une fréquence que vous définissez (horaire, quotidienne, hebdomadaire ou mensuelle, par exemple) à des fins de maintenance et de synchronisation.

Suppression de la seule règle de sauvegarde continue d'un plan de sauvegarde

Lorsque vous créez un plan de sauvegarde avec une règle de sauvegarde continue, puis que vous supprimez cette règle, AWS Backup mémorise la période de conservation de votre règle désormais supprimée. Il supprimera la sauvegarde continue de votre coffre-fort de sauvegarde à l'expiration de la période de rétention.

Backup créé par type de ressource

Avec AWS Backup, vous pouvez créer des sauvegardes automatiquement à l'aide de plans de sauvegarde ou manuellement en lançant une sauvegarde à la demande.

Création de sauvegardes automatiques

Lorsque les sauvegardes sont créées automatiquement par des plans de sauvegarde, elles sont configurées avec les paramètres de cycle de vie définis dans le plan de sauvegarde. Elles sont organisées dans le coffre-fort de sauvegarde spécifié dans le plan de sauvegarde. Elles sont également marquées avec les balises répertoriées dans le plan de sauvegarde. Pour plus d'informations sur les plans de sauvegarde, consultez [Plans de sauvegarde](#).

Création de sauvegardes à la demande

Lorsque vous créez une sauvegarde à la demande, vous pouvez configurer ces paramètres pour la sauvegarde en cours de création. Lorsqu'une sauvegarde est créée automatiquement ou

manuellement, une tâche de sauvegarde est lancée. Pour savoir comment créer une sauvegarde à la demande, consultez [Création d'une sauvegarde à la demande à l'aide de AWS Backup](#).

Remarque : une sauvegarde à la demande crée une tâche de sauvegarde ; l'état de la tâche de sauvegarde passera à `Running` dans un délai d'une heure (ou lorsque cela est spécifié). Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

[Les sauvegardes à la demande](#) ne peuvent pas être utilisées avec la [point-in-time restauration \(PITR\)](#), car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la sauvegarde, tandis que la sauvegarde PITR utilise [des sauvegardes continues](#) qui enregistrent les modifications au fil du temps.

Statuts des tâches de sauvegarde

Chaque tâche de sauvegarde a un ID unique. Par exemple, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Vous pouvez afficher l'état de votre tâche de sauvegarde sur la page Jobs (Tâches) de la console AWS Backup . Les statuts des tâches de sauvegarde incluent `CREATEDPENDING`, `RUNNING`, `ABORTING`, `ABORTED`, `COMPLETED`, `FAILEDEXPIRED`, et `PARTIAL`.

Sauvegardes incrémentielles

De nombreuses ressources prennent en charge la sauvegarde incrémentielle avec AWS Backup. Une liste complète est disponible dans la section de sauvegarde incrémentielle du tableau [Disponibilité des fonctionnalités par ressource](#).

Bien que chaque sauvegarde après la première (complète) soit incrémentielle (c'est-à-dire qu'elle ne capture que les modifications par rapport à la sauvegarde précédente), toutes les sauvegardes effectuées avec cette sauvegarde AWS Backup conservent les données de référence nécessaires pour permettre une restauration complète. Cela est vrai même si la sauvegarde d'origine (complète) a atteint la fin de son cycle de vie et a été supprimée.

Par exemple, si votre sauvegarde (complète) du premier jour a été supprimée en raison d'une politique de cycle de vie de 3 jours, vous pourrez toujours effectuer une restauration complète avec les sauvegardes des jours 2 et 3. AWS Backup conserve les données de référence nécessaires dès le premier jour pour ce faire.

Sauvegardes incrémentielles et régions

Les sauvegardes de ressources entièrement gérées par ne AWS Backup peuvent être incrémentielles que si le coffre-fort dans lequel la sauvegarde est créée contient également une sauvegarde antérieure (incrémentielle ou complète) ; les autres types de ressources (non entièrement gérés par AWS Backup) peuvent faire l'objet de sauvegardes incrémentielles tant qu'un coffre-fort de la même région possède une sauvegarde antérieure.

Accès aux ressources source

AWS Backup a besoin d'accéder à vos ressources sources pour les sauvegarder. Par exemple :

- Pour sauvegarder une EC2 instance Amazon, celle-ci peut être à l'`stopped` état `running` ou, mais pas à l'`terminated` état. Cela est dû au fait qu'une `stopped` instance `running` or peut communiquer avec AWS Backup, mais pas une `terminated` instance.
- Pour sauvegarder une machine virtuelle, son hyperviseur doit avoir le statut de passerelle de sauvegarde `ONLINE`. Pour plus d'informations, consultez [Compréhension du statut de l'hyperviseur](#).
- Pour sauvegarder une base de données Amazon RDS, Amazon Aurora ou un cluster Amazon DocumentDB, ces ressources doivent avoir le statut `AVAILABLE`.
- Pour sauvegarder un Amazon Elastic File System (Amazon EFS), celui-ci doit avoir le statut `AVAILABLE`.
- Pour sauvegarder un système de FSx fichiers Amazon, celui-ci doit avoir le statut `AVAILABLE`. Si le statut est `UPDATING`, la demande de sauvegarde est mise en file d'attente jusqu'à ce que le système de fichiers devienne `AVAILABLE`.

FSx for ONTAP ne prend pas en charge la sauvegarde de certains types de volumes, notamment les volumes DP (protection des données), les volumes LS (partage de charge), les volumes complets ou les volumes situés sur des systèmes de fichiers pleins. Pour plus d'informations, consultez [FSx ONTAP Working with backups](#).

AWS Backup conserve les sauvegardes créées précédemment conformément à votre politique de cycle de vie, quel que soit l'état de votre ressource source.

Rubriques

- [CloudFormation empiler des sauvegardes](#)
- [Sauvegardes SQL Amazon Aurora](#)

- [Sauvegarde DynamoDB avancée](#)
- [Amazon EBS et AWS Backup](#)
- [Sauvegardes Amazon Relational Database Service](#)
- [Sauvegardes Amazon Redshift](#)
- [Sauvegardes sans serveur Amazon Redshift](#)
- [Sauvegardes Amazon EKS](#)
- [Sauvegarde SAP HANA sur Amazon EC2](#)
- [Sauvegardes Amazon S3](#)
- [Sauvegardes Amazon Timestream](#)
- [Sauvegardes de machines virtuelles](#)
- [Création de sauvegardes Windows VSS](#)

CloudFormation empiler des sauvegardes

Une CloudFormation pile est composée de plusieurs ressources dynamiques et apatrides que vous pouvez sauvegarder en tant qu'unité unique. En d'autres termes, vous pouvez sauvegarder et restaurer une application contenant plusieurs ressources en sauvegardant une pile et en restaurant les ressources qu'elle contient. Toutes les ressources d'une pile sont définies par son modèle CloudFormation .

Lorsqu'une CloudFormation pile est sauvegardée, des points de récupération sont créés pour le CloudFormation modèle et pour chaque ressource supplémentaire prise AWS Backup en charge par la pile. Ces points de récupération sont regroupés au sein d'un point de récupération global appelé composite.

Ce point de récupération composite ne peut pas être restauré, mais les points de récupération imbriqués peuvent être restaurés. Vous pouvez restaurer une ou toutes les sauvegardes imbriquées au sein d'une sauvegarde composite à l'aide de la console ou de l' AWS CLI.

CloudFormation terminologie de la pile d'applications

- Point de récupération composite : point de récupération utilisé pour regrouper les points de récupération imbriqués, ainsi que d'autres métadonnées.
- Point de restauration imbriqué : point de récupération d'une ressource faisant partie d'une CloudFormation pile et sauvegardée dans le cadre du point de récupération composite. Chaque point de récupération imbriqué appartient à la pile d'un point de récupération composite.

- Tâche composite : tâche de sauvegarde, de copie ou de restauration pour une CloudFormation pile qui peut déclencher d'autres tâches de sauvegarde pour des ressources individuelles de la pile.
- Tâche imbriquée : tâche de sauvegarde, de copie ou de restauration d'une ressource au sein d'une CloudFormation pile.

CloudFormation empiler les tâches de sauvegarde

Le processus de création d'une sauvegarde est appelé tâche de sauvegarde. Une tâche de sauvegarde de CloudFormation pile possède un [statut](#). Lorsqu'une tâche de sauvegarde est terminée, elle a le statut `Completed`. Cela signifie qu'un [CloudFormation point de récupération](#) (une sauvegarde) a été créée.

CloudFormation les piles peuvent être sauvegardées à l'aide de la console ou sauvegardées par programme. Pour sauvegarder n'importe quelle ressource, y compris une CloudFormation pile, voir [Création d'une sauvegarde](#) ailleurs dans ce guide AWS Backup du développeur.

CloudFormation les piles peuvent être sauvegardées à l'aide de la commande `StartBackupJob` API. Notez que la documentation et la console font référence à des points de récupération composites et imbriqués ; le langage de l'API utilise la terminologie « points de récupération parent/enfant » dans la même relation contextuelle.

CloudFormation les piles contenant toutes les AWS ressources sont indiquées par votre [CloudFormation modèle](#). Notez que votre modèle peut contenir des ressources qui ne sont pas encore prises en charge par AWS Backup. Si votre modèle contient une combinaison de ressources AWS prises en charge et de ressources non prises en charge, AWS Backup vous sauvegarderez toujours le modèle dans une pile composite, mais Backup créera uniquement des points de restauration pour les services pris en charge par Backup. Tous les types de ressources contenus dans le CloudFormation modèle seront inclus dans une sauvegarde, même si vous n'avez pas opté pour un service en particulier (en faisant passer un service sur « Activé » dans les paramètres de la console).

CloudFormation point de récupération

Statut du point de récupération

Lorsque la tâche de sauvegarde d'une pile est terminée (le statut de la tâche est `Completed`), une sauvegarde de la pile est créée. Cette sauvegarde est également connue sous le nom de point de récupération composite. Un point de récupération composite peut avoir l'un des statuts suivants :

Completed, Failed ou Partial. Notez qu'une tâche de sauvegarde possède un statut et qu'un point de récupération (également appelé sauvegarde) possède également un statut distinct.

Une tâche de sauvegarde terminée signifie que l'ensemble de votre pile et les ressources qu'elle contient sont protégées par AWS Backup. Un statut d'échec indique que la tâche de sauvegarde a échoué ; vous devez créer à nouveau la sauvegarde une fois le problème à l'origine de l'échec résolu.

Un statut Partial signifie que toutes les ressources de la pile n'ont pas été sauvegardées. Cela peut se produire si le CloudFormation modèle contient des ressources qui ne sont pas actuellement prises en charge par AWS Backup, ou si une ou plusieurs tâches de sauvegarde appartenant aux ressources de la pile (ressources imbriquées) ont un statut autre que Completed. Vous pouvez créer manuellement une sauvegarde à la demande pour exécuter à nouveau toutes les ressources dont le statut n'est pas Completed. Si vous vous attendiez à ce que la pile ait le statut Completed mais qu'il est plutôt Partial, vérifiez laquelle des conditions ci-dessus pourrait être vraie pour votre pile.

Chaque ressource imbriquée au sein du point de récupération composite possède son propre point de récupération individuel, chacun ayant son propre statut (Completed ou Failed). Les points de récupération imbriqués dont le statut est Completed peuvent être restaurés.

Gestion des points de récupération

Les points de récupération composite (sauvegardes) peuvent être copiés ; les points de récupération imbriqués peuvent être copiés, supprimés, dissociés ou restaurés. Un point de récupération composite contenant des sauvegardes imbriquées ne peut pas être supprimé. Une fois que les points de récupération imbriqués au sein d'un point de récupération composite ont été supprimés ou dissociés, vous pouvez supprimer manuellement le point de récupération composite ou le laisser subsister jusqu'à ce que le cycle de vie du plan de sauvegarde le supprime.

Suppression d'un point de récupération

Vous pouvez supprimer un point de récupération à l'aide de la AWS Backup console ou du AWS CLI.

Pour supprimer des points de récupération à l'aide de la AWS Backup console,

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez CloudFormation pour afficher uniquement vos CloudFormation piles.

3. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cocher la case située à gauche de chaque point de récupération pour l'inclure dans votre sélection de points de récupération que vous souhaitez supprimer.
4. Cliquez sur le bouton Supprimer.

Lorsque vous utilisez la console pour supprimer un ou plusieurs points de récupération composite, un message d'avertissement apparaît. Cette boîte d'avertissement vous demande de confirmer votre intention de supprimer les points de récupération composite, y compris les points de récupération imbriqués dans les piles composites.

Pour supprimer des points de récupération à l'aide de l'API, utilisez la commande `DeleteRecoveryPoint`.

Lorsque vous utilisez l'API avec le, AWS Command Line Interface vous devez supprimer tous les points de récupération imbriqués avant de supprimer un point composite. Si vous envoyez une demande d'API pour supprimer une sauvegarde de pile composite (point de récupération) qui contient encore des points de récupération imbriqués, la demande renvoie une erreur.

Dissociation d'un point de récupération imbriqué d'un point de récupération composite

Vous pouvez dissocier un point de récupération imbriqué d'un point de récupération composite (par exemple, vous souhaitez conserver le point de récupération imbriqué mais supprimer le point de récupération composite). Les deux points de récupération resteront, mais ils ne seront plus connectés ; en d'autres termes, les actions effectuées sur le point de récupération composite ne s'appliqueront plus au point de récupération imbriqué une fois celui-ci dissocié.

Vous pouvez dissocier le point de récupération à l'aide de la console ou appeler l'API `DisassociateRecoveryPointFromParent`. [Notez que les appels d'API utilisent le terme « parent » pour désigner les points de récupération composite.]

Copie d'un point de récupération

Vous pouvez copier un point de récupération composite ou un point de récupération imbriqué si la ressource prend en charge la copie [entre comptes et entre régions](#).

Pour copier des points de restauration à l'aide de la AWS Backup console :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez `CloudFormation` pour afficher uniquement vos CloudFormation piles.
3. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cliquer sur le bouton circulaire situé à gauche de n'importe quel point de récupération pour le copier.
4. Une fois sélectionné, cliquez sur le bouton Copier dans le coin supérieur droit du volet.

Lorsque vous copiez un point de récupération composite, les points de récupération imbriqués qui ne prennent pas en charge la fonctionnalité de copie ne se retrouveront pas dans la pile copiée. Le point de récupération composite aura le statut `Partial`.

Questions fréquentes (FAQ)

1. « Qu'est-ce qui est inclus dans la sauvegarde de l'application ? »

Dans le cadre de chaque sauvegarde d'une application définie à l'aide CloudFormation, le modèle, la valeur traitée de chaque paramètre du modèle et les ressources imbriquées prises en charge par AWS Backup sont sauvegardés. Une ressource imbriquée est sauvegardée de la même manière qu'une ressource individuelle ne faisant pas partie d'une CloudFormation pile est sauvegardée. Notez que les valeurs des paramètres marqués comme no-echo ne seront pas sauvegardées.

2. « Puis-je sauvegarder ma CloudFormation pile contenant des piles imbriquées ? »

Oui. Vos CloudFormation piles contenant des piles imbriquées peuvent se trouver dans votre sauvegarde.

3. « Un statut `Partial` signifie-t-il que la création de ma sauvegarde a échoué ? »

Non. Un statut partiel indique que certains points de récupération ont été sauvegardés, tandis que d'autres ne l'ont pas été. Trois conditions permettent de vérifier si vous attendiez un résultat de sauvegarde `Completed` :

- a. Votre CloudFormation pile contient-elle des ressources qui ne sont actuellement pas prises en charge par ? AWS Backup Pour obtenir la liste des ressources prises en charge, consultez

la section [AWS Ressources prises en charge et applications tierces](#) dans notre guide du développeur.

- b. Une ou plusieurs tâches de sauvegarde appartenant aux ressources de la pile n'ont pas abouti et la tâche doit être à nouveau exécutée.
- c. Un point de récupération imbriqué a été supprimé ou dissocié d'un point de récupération composite.

4. « Comment exclure des ressources de ma CloudFormation pile de sauvegarde ? »

Lorsque vous sauvegardez votre CloudFormation pile, vous pouvez exclure des ressources de la sauvegarde. Dans la console, lors des processus de [création d'un plan de sauvegarde](#) et de [mise à jour d'un plan de sauvegarde](#), il existe une étape d'[attribution de ressources](#). Dans cette étape, il existe une section Sélection des ressources. Si vous choisissez d'inclure des types de ressources spécifiques et que vous les avez incluses en CloudFormation tant que ressource à sauvegarder, vous pouvez exclure une ressource spécifique des types IDs de ressources sélectionnés. Vous pouvez également utiliser des balises pour exclure des ressources de la pile.

Avec l'interface de ligne de commande, vous pouvez utiliser

- `NotResources` dans votre plan de sauvegarde pour exclure une ressource spécifique de vos CloudFormation piles.
- `StringNotLike` pour exclure des éléments via des balises.

5. « Quels types de sauvegardes sont pris en charge pour les ressources imbriquées ? »

Les sauvegardes de ressources imbriquées peuvent être complètes ou incrémentielles, selon le type de sauvegarde pris en charge AWS Backup pour ces ressources. Pour plus d'informations, consultez [Fonctionnement des sauvegardes incrémentielles](#). Notez toutefois que le PITR (point-in-time restauration) [n'est pas pris en charge](#) pour les ressources imbriquées Amazon S3 et Amazon RDS.

6. « Les ensembles de modifications qui font partie de la CloudFormation pile sont-ils sauvegardés ? »

Non Les ensembles de modifications ne sont pas sauvegardés dans le cadre de la sauvegarde par CloudFormation pile.

7. « Quel est l'impact de l'état de la CloudFormation pile sur la sauvegarde ? »

L'état de la CloudFormation pile peut avoir un impact sur la sauvegarde. Une pile avec les statuts suivants peut être sauvegardée : COMPLETE, CREATE_COMPLETE, ROLLBACK_COMPLETE, UPDATE_COMPLETE, UPDATE_ROLLBACK_COMPLETE, IMPORT_COMPLETE ou IMPORT_ROLLBACK_COMPLETE.

Si le téléchargement d'un nouveau modèle échoue et que la pile passe au statut ROLLBACK_COMPLETE, le nouveau modèle sera sauvegardé, mais les sauvegardes des ressources imbriquées seront basées sur les ressources annulées.

8. « En quoi les cycles de vie des piles d'applications diffèrent-ils des autres cycles de vie des points de récupération ? »

Les cycles de vie des points de récupération imbriqués sont déterminés par le plan de sauvegarde auquel ils appartiennent. Le point de récupération composite est déterminé par le cycle de vie le plus long de tous les points de récupération imbriqués. Lorsque le dernier point de récupération imbriqué restant dans un point de récupération composite est supprimé ou dissocié, le point de récupération composite est également supprimé.

9. « Comment sont CloudFormation copiées les balises d'un point de récupération ? »

Oui. Ces balises seront copiées sur chaque point de récupération imbriqué correspondant.

- 10.« Existe-t-il un ordre pour supprimer les points de restauration composite et imbriqués (sauvegardes) ? »

Oui. Certaines sauvegardes doivent être supprimées avant que d'autres puissent être supprimées. Les sauvegardes composite contenant des points de récupération imbriqués ne peuvent pas être supprimées tant que tous les points de récupération composite n'ont pas été supprimés. Une fois qu'un point de récupération composite ne contient plus de points de récupération imbriqués, vous pouvez le supprimer manuellement. Dans le cas contraire, il sera supprimé conformément au cycle de vie de son plan de sauvegarde.

Restauration d'applications au sein d'une pile

Consultez [Comment restaurer des sauvegardes de pile d'applications](#) pour en savoir plus sur la restauration de points de récupération imbriqués.

Sauvegardes SQL Amazon Aurora

Vous pouvez l'utiliser AWS Backup pour créer des sauvegardes de vos clusters Amazon Aurora DSQL à région unique ou multirégionale. Les sauvegardes du cluster SQL Amazon Aurora sont toujours des sauvegardes complètes.

La création de sauvegarde pour les clusters SQL Amazon Aurora utilise le processus de création de sauvegarde standard. Pour plus d'informations, consultez les ressources suivantes :

- [Création d'une sauvegarde à la demande à l'aide de AWS Backup](#)
- [Création d'un plan de sauvegarde](#)

AWS Backup Pour créer des sauvegardes de vos clusters Amazon Aurora DSQL, vous devez activer la protection d'Aurora DSQL. Pour de plus amples informations, veuillez consulter [Inscription au service](#).

Lorsque vous sauvegardez un cluster multirégional, tenez compte des points suivants :

- Une sauvegarde de cluster multirégional nécessite une sauvegarde distincte pour chaque région du cluster ; une sauvegarde dans une région ne crée pas de point de récupération pour toutes les régions d'un cluster multirégional.
- Il est AWS Backup recommandé de créer un point de récupération dans une région et de le copier dans une autre région associée. Pour une [restauration multirégionale](#), vous avez besoin d'un point de récupération dans une région prise en charge et d'une copie de ce point de récupération dans une autre région au sein du même triplet régional.

Les triplets pris en charge suivants sont disponibles. Lorsqu'il y a plus de régions, choisissez-en trois dans le même groupe.

- USA Est (Virginie du Nord) ; USA Est (Ohio) ; USA Ouest (Californie du Nord)
- Europe (Irlande) ; Europe (Londres) ; Europe (Paris) ; Europe (Francfort)
- Asie-Pacifique (Tokyo) ; Asie-Pacifique (Séoul) ; Asie-Pacifique (Osaka)

AWS Backup recommande d'ajouter la règle de copie de sauvegarde au plan de sauvegarde. Si vous n'ajoutez pas la règle de copie au plan de sauvegarde, vous devez copier manuellement la sauvegarde dans la région requise dans laquelle effectuer la restauration, ce qui augmentera les délais de votre objectif de temps de restauration (RTO).

Pour plus d'informations sur la restauration d'un point de restauration Aurora DSQL (sauvegarde), consultez [Restauration Amazon Aurora DSQL](#).

Sauvegarde DynamoDB avancée

AWS Backup prend en charge des fonctionnalités avancées supplémentaires pour répondre à vos besoins en matière de protection des données Amazon DynamoDB.

Les clients qui ont commencé à utiliser DynamoDB AWS Backup après novembre 2021 ont activé par défaut les fonctionnalités avancées de sauvegarde DynamoDB. Plus précisément, les fonctionnalités avancées de sauvegarde DynamoDB sont activées par défaut pour les clients qui n'ont pas créé de coffre-fort de sauvegarde avant le 21 novembre 2021.

Il est recommandé aux AWS Backup clients existants d'activer les fonctionnalités avancées de DynamoDB. Il n'y a aucune différence dans le prix du stockage de sauvegarde à chaud une fois que vous avez activé les fonctionnalités avancées. Vous pouvez potentiellement économiser de l'argent en transférant les sauvegardes vers un stockage à froid et optimiser vos coûts en utilisant des balises de répartition des coûts. Vous pouvez également commencer à tirer parti des fonctionnalités AWS Backup de copie et de sécurité entre régions et entre comptes.

Rubriques

- [Avantages de la sauvegarde DDB avancée](#)
- [Considérations relatives à la sauvegarde DynamoDB avancée](#)
- [Activation de la sauvegarde DynamoDB avancée à l'aide de la console](#)
- [Activation de la sauvegarde DynamoDB avancée par programmation](#)
- [Modification d'une sauvegarde DynamoDB avancée](#)
- [Restauration d'une sauvegarde DynamoDB avancée](#)
- [Suppression d'une sauvegarde DynamoDB avancée](#)
- [Autres avantages de la gestion complète d' AWS Backup lorsque vous activez la sauvegarde DynamoDB avancée](#)

Avantages de la sauvegarde DDB avancée

Après avoir activé AWS Backup les fonctionnalités avancées dans votre Région AWS, vous débloquez les fonctionnalités suivantes pour toutes les nouvelles sauvegardes de tables DynamoDB que vous créez :

- Réduction des coûts et optimisation :
 - [Hiérarchisation des sauvegardes vers le stockage à froid](#) pour réduire les coûts de stockage
 - [Balisage de répartition des coûts à utiliser avec Cost Explorer](#)
- Options de copie supplémentaires :
 - [Copie entre régions](#)
 - [Copie entre comptes](#)
- Sécurité:
 - Les sauvegardes héritent des balises de leurs tables DynamoDB source, ce qui vous permet de les utiliser pour définir des autorisations [et des politiques de contrôle des services](#) (). SCPs

Considérations relatives à la sauvegarde DynamoDB avancée

S'inscrire

Les sauvegardes, y compris celles des ressources DDB avancées, peuvent être créées par un plan de sauvegarde, une sauvegarde à la demande ou via une politique de sauvegarde. Les sauvegardes créées par un plan ou à la demande seront automatiquement activées dans votre compte pour autoriser les sauvegardes des ressources DDB avancées.

[Si votre tâche de sauvegarde est créée par une politique de sauvegarde, vous devez activer manuellement les sauvegardes DynamoDB avancées, soit via la console Backup, soit via la CLI.](#)

Politiques et rôles personnalisés

Si vous utilisez un rôle ou une politique personnalisé au lieu AWS Backup du rôle de service par défaut, vous devez ajouter ou utiliser les politiques d'autorisation suivantes (ou ajouter leurs autorisations équivalentes) à votre rôle personnalisé :

- `AWSBackupServiceRolePolicyForBackup` pour effectuer une sauvegarde DynamoDB avancée.
- `AWSBackupServiceRolePolicyForRestores` pour restaurer des sauvegardes DynamoDB avancées.

Pour en savoir plus sur les politiques AWS gérées et consulter des exemples de politiques gérées par le client, consultez. [Politiques gérées pour AWS Backup](#)

Activation de la sauvegarde DynamoDB avancée à l'aide de la console

Vous pouvez activer les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB à l'aide de la console DynamoDB AWS Backup ou de DynamoDB.

Pour activer les fonctionnalités avancées de sauvegarde DynamoDB depuis la console, procédez comme suit : AWS Backup

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le menu de navigation de gauche, choisissez Paramètres.
3. Dans la section Services pris en charge, vérifiez que DynamoDB est Activé.

Si ce n'est pas le cas, choisissez Activation et activez DynamoDB en tant que service pris en charge par AWS Backup .

4. Dans la section Fonctionnalités avancées pour les sauvegardes DynamoDB, choisissez Activer.
5. Choisissez Activer les fonctions.

Pour savoir comment activer les fonctionnalités AWS Backup avancées à l'aide de la console DynamoDB, [consultez la section AWS Backup Activation](#) des fonctionnalités dans le guide de l'utilisateur d'Amazon DynamoDB.

Activation de la sauvegarde DynamoDB avancée par programmation

Vous pouvez également activer les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB à l'aide de la AWS Command Line Interface (CLI). Vous activez les sauvegardes DynamoDB avancées lorsque vous définissez les deux valeurs suivantes sur `true` :

Pour activer par programmation les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB, procédez comme suit :

1. Vérifiez si vous avez déjà activé les fonctionnalités AWS Backup avancées de DynamoDB à l'aide de la commande suivante :

```
$ aws backup describe-region-settings
```

Si `"DynamoDB":true` sous les options `"ResourceTypeManagementPreference"` et `"ResourceTypeOptInPreference"`, vous avez déjà activé la sauvegarde DynamoDB avancée.

Si, comme dans le résultat suivant, vous possédez au moins une instance de "DynamoDB":false, vous n'avez pas encore activé la sauvegarde DynamoDB avancée. Passez à l'étape suivante.

```
{
  "ResourceTypeManagementPreference":{
    "DynamoDB":false,
    "EFS":true
  }
  "ResourceTypeOptInPreference":{
    "Aurora":true,
    "DocumentDB":false,
    "DynamoDB":false,
    "EBS":true,
    "EC2":true,
    "EFS":true,
    "FSx":true,
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. Utilisez l'opération [UpdateRegionSettings](#) suivante pour définir "ResourceTypeManagementPreference" et "ResourceTypeOptInPreference" sur "DynamoDB":true :

```
aws backup update-region-settings \
    --resource-type-opt-in-preference DynamoDB=true \
    --resource-type-management-preference DynamoDB=true
```

Modification d'une sauvegarde DynamoDB avancée

Lorsque vous créez une sauvegarde DynamoDB après avoir activé les fonctionnalités avancées, vous pouvez l'utiliser AWS Backup pour :

- Copier une sauvegarde dans plusieurs régions
- Copier une sauvegarde dans plusieurs comptes
- Modifier le moment AWS Backup où une sauvegarde passe en stockage à froid

- Balisage de la sauvegarde

Pour utiliser ces fonctionnalités avancées sur une sauvegarde existante, consultez [Modification d'une sauvegarde](#).

Si vous désactivez ultérieurement les fonctionnalités AWS Backup avancées de DynamoDB, vous pouvez continuer à effectuer ces opérations sur les sauvegardes DynamoDB que vous avez créées pendant la période pendant laquelle vous avez activé les fonctionnalités avancées.

Restauration d'une sauvegarde DynamoDB avancée

Vous pouvez restaurer les sauvegardes DynamoDB effectuées AWS Backup avec les fonctionnalités avancées activées de la même manière que vous restaurez les sauvegardes DynamoDB effectuées avant l'activation des fonctionnalités avancées. AWS Backup Vous pouvez effectuer une restauration à l'aide de l'un ou de l'autre AWS Backup ou de DynamoDB.

Vous pouvez définir le mode de chiffrement de votre table récemment restaurée à l'aide des options suivantes :

- Lorsque vous effectuez une restauration dans la même région que votre table d'origine, vous pouvez éventuellement spécifier une clé de chiffrement pour la table restaurée. Si vous ne spécifiez pas de clé de chiffrement, la table restaurée AWS Backup sera automatiquement chiffrée à l'aide de la même clé que celle utilisée pour chiffrer la table d'origine.
- Lorsque vous effectuez une restauration dans une région différente de celle de votre table d'origine, vous devez spécifier une clé de chiffrement.

Pour rétablir l'utilisation AWS Backup, voir [Restaurer une table Amazon DynamoDB](#).

Pour effectuer une restauration à l'aide de DynamoDB, consultez [Restauration d'une table DynamoDB à partir d'une sauvegarde](#) dans le Guide de l'utilisateur Amazon DynamoDB.

Suppression d'une sauvegarde DynamoDB avancée

Vous ne pouvez pas supprimer les sauvegardes créées à l'aide de ces fonctionnalités avancées dans DynamoDB. Vous devez utiliser AWS Backup pour supprimer des sauvegardes afin de maintenir la cohérence globale dans l'ensemble de votre environnement AWS .

Pour supprimer une sauvegarde DynamoDB, consultez [Suppression d'une sauvegarde](#).

Autres avantages de la gestion complète d' AWS Backup lorsque vous activez la sauvegarde DynamoDB avancée

Lorsque vous activez les fonctionnalités AWS Backup avancées de DynamoDB, vous déléguez la gestion complète de vos sauvegardes DynamoDB à AWS Backup. Cela vous donne les avantages supplémentaires suivants :

Chiffrement

AWS Backup chiffre automatiquement les sauvegardes avec la clé KMS de votre AWS Backup coffre-fort de destination. Auparavant, elles étaient chiffrées à l'aide de la même méthode de chiffrement que votre table DynamoDB source. Cela augmente le nombre de défenses que vous pouvez utiliser pour protéger vos données. Pour plus d'informations, consultez [Chiffrement pour les sauvegardes dans AWS Backup](#).

Amazon Resource Name (ARN)

L'espace de noms de service de chaque ARN de sauvegarde est `awsbackup`. Auparavant, l'espace de noms du service était `dynamodb`. Autrement dit, le début de chaque ARN passera de `arn:aws:dynamodb` à `arn:aws:backup`. Voir AWS Backup dans [ARNs la](#) référence d'autorisation de service.

Grâce à cette modification, vous ou votre administrateur de sauvegarde pouvez créer des stratégies d'accès pour les sauvegardes à l'aide de l'espace de noms de service `awsbackup` qui s'appliquent désormais aux sauvegardes DynamoDB créées après l'activation des fonctionnalités avancées. En utilisant l'espace de noms du service `awsbackup`, vous pouvez également appliquer des politiques aux autres sauvegardes effectuées par AWS Backup. Pour plus d'informations, consultez [Contrôle d'accès](#).

Emplacement des frais sur le relevé de facturation

Les frais relatifs aux sauvegardes (y compris le stockage, les transferts de données, les restaurations et les suppressions anticipées) figurent dans la section « Sauvegarde » de votre AWS facture. Auparavant, les frais apparaissaient sous « DynamoDB » sur votre facture.

Cette modification garantit que vous pouvez utiliser la AWS Backup facturation pour surveiller de manière centralisée vos coûts de sauvegarde. Pour plus d'informations, consultez [Comptage, coûts et facturation pour AWS Backup](#).

Amazon EBS et AWS Backup

Le processus de sauvegarde des ressources Amazon EBS est similaire aux étapes utilisées pour sauvegarder d'autres types de ressources :

- [Création d'une sauvegarde à la demande](#)
- [Création d'une sauvegarde planifiée](#)

Des informations spécifiques aux ressources sont indiquées dans les sections suivantes.

Niveau d'archive Amazon EBS pour le stockage à froid

EBS est l'une des ressources qui prend en charge la transition des sauvegardes vers le stockage à froid. Pour de plus amples informations, veuillez consulter [Cycle de vie et niveaux de stockage](#).

Sauvegardes multi-volumes en cas de panne sur Amazon EBS

Par défaut, AWS Backup crée des sauvegardes cohérentes en cas de crash des volumes Amazon EBS attachés à une instance Amazon. EC2 La cohérence en cas de crash signifie que les instantanés de chaque volume Amazon EBS attaché à la même EC2 instance Amazon sont pris exactement au même moment. Vous n'avez plus besoin d'arrêter vos instances ou de coordonner plusieurs volumes Amazon EBS pour garantir l'état de votre application en cas de panne.

Les instantanés multivolumes compatibles avec les crashes étant une AWS Backup fonctionnalité par défaut, vous n'avez rien de différent à faire pour utiliser cette fonctionnalité.

Le rôle utilisé pour créer un point de restauration d'un instantané EBS est associé à ce cliché. Ce même rôle doit être utilisé pour supprimer les points de restauration qu'il a créés ou pour transférer ses points de restauration vers un niveau d'archivage.

Amazon EBS Snapshot Lock et AWS Backup

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une EC2 AMI AWS Backup Amazon gérée auxquels Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut EXPIRED. Ces points de récupération peuvent être [supprimés manuellement](#) si vous choisissez de supprimer d'abord le verrouillage d'instantané Amazon EBS.

Restauration des ressources Amazon EBS

Pour restaurer vos volumes Amazon EBS, suivez les étapes décrites dans [Restauration d'un volume Amazon EBS](#).

Sauvegardes Amazon Relational Database Service

Amazon RDS et AWS Backup

Lorsque vous envisagez les options de sauvegarde de vos instances et clusters Amazon RDS, il est important de préciser le type de sauvegarde que vous souhaitez créer et utiliser. Plusieurs AWS ressources, dont Amazon RDS, proposent leurs propres solutions de sauvegarde natives.

Amazon RDS offre la possibilité d'effectuer des [sauvegardes automatisées et des sauvegardes manuelles](#). Dans la terminologie d'Amazon RDS, tous les points de restauration créés par AWS Backup, y compris ceux d'un plan de sauvegarde, sont considérés comme des sauvegardes manuelles.

Lorsque vous [créez une sauvegarde](#) (point de restauration) d'une instance Amazon RDS, AWS Backup vérifie si vous avez déjà utilisé Amazon RDS pour créer une sauvegarde automatique. AWS Backup Si une sauvegarde automatique existe, AWS Backup crée une copie instantanée incrémentielle (copy-db-snapshotopération). S'il n'existe aucune sauvegarde, AWS Backup crée un instantané de l'instance que vous indiquez, au lieu d'une copie (create-db-snapshotopération).

Le premier instantané créé par AWS Backup, créé par l'une ou l'autre opération, produira un instantané complet. Toutes les copies suivantes seront des sauvegardes incrémentielles, à condition que la sauvegarde complète existe.

Important

Lorsqu'un plan de AWS Backup sauvegarde est planifié pour créer plusieurs instantanés quotidiens d'une instance Amazon RDS, et lorsque l'une de ces fenêtres de démarrage de [AWS Backup sauvegarde coïncide avec la fenêtre de sauvegarde](#) Amazon RDS, [le lignage des données des sauvegardes peut être](#) bifurqué vers des sauvegardes non identiques, créant ainsi des sauvegardes imprévues et contradictoires. Pour éviter cela, assurez-vous que votre plan AWS Backup de sauvegarde ou votre fenêtre Amazon RDS ne coïncident pas avec leur époque.

Considérations

RDS Custom for SQL Server et RDS Custom for Oracle ne sont actuellement pas pris en charge par AWS Backup.

AWS Backup ne prend pas en charge la sauvegarde et la restauration de RDS sur les Outposts.

Sauvegardes continues et restauration ponctuelle d'Amazon RDS

Les sauvegardes continues impliquent AWS Backup de créer une sauvegarde complète de votre ressource Amazon RDS, puis de capturer toutes les modifications via un journal des transactions. Vous pouvez obtenir une meilleure granularité en revenant au moment où vous souhaitez effectuer la restauration au lieu de choisir un instantané précédent pris à intervalles de temps fixes.

Consultez les [sauvegardes continues et les services pris en charge par le PITR](#) et [la gestion des paramètres de sauvegarde continue](#) pour plus d'informations.

Sauvegardes à plusieurs zones de disponibilité Amazon RDS

AWS Backup sauvegarde et prend en charge les options de déploiement Amazon RDS pour MySQL et pour PostgreSQL Multi-AZ (zone de disponibilité) avec une instance de base de données principale et deux instances de base de données de secours lisibles.

Les sauvegardes à plusieurs zones de disponibilité sont disponibles dans les régions suivantes : région Asie-Pacifique (Sydney), région Asie-Pacifique (Tokyo), région Europe (Irlande), région USA Est (Ohio), région USA Ouest (Oregon), région Europe (Stockholm), région Asie-Pacifique (Singapour), région USA Est (Virginie du Nord) et région Europe (Francfort).

L'option de déploiement multi-AZ optimise les transactions d'écriture et est idéale lorsque vos charges de travail nécessitent une capacité de lecture supplémentaire, une latence des transactions d'écriture plus faible, une meilleure résilience face à l'instabilité du réseau (qui a un impact sur la cohérence de la latence des transactions d'écriture), ainsi qu'une disponibilité et une durabilité élevées.

Pour créer un cluster multi-AZ, vous pouvez choisir MySQL ou PostgreSQL comme type de moteur.

Dans la AWS Backup console, il existe trois options de déploiement :

- Cluster de base de données multi-AZ : crée un cluster de bases de données avec une instance de base de données principale et deux instances de base de données de secours lisibles, chaque instance de base de données se trouvant dans une zone de disponibilité différente. Assure une

haute disponibilité, une redondance des données et augmente la capacité des charges de travail prêtes à être installées sur les serveurs.

- Instance de base de données multi-AZ : crée une instance de base de données primaire avec une instance de base de données de secours dans une zone de disponibilité différente. Cela garantit une haute disponibilité et une redondance des données, mais l'instance de base de données de secours ne prend pas en charge les connexions pour les charges de travail de lecture.
- Instance de base de données unique : crée une instance de base de données unique sans instance de base de données de secours.

Comportement de sauvegarde avec les instances et les clusters

- [Point-in-TimeRecovery](#) (PITR) peut prendre en charge les instances, mais pas les clusters.
- La copie d'un instantané de cluster de bases de données multi-AZ n'est pas prise en charge.
- Le nom de ressource Amazon (ARN) d'un point de récupération RDS dépend de l'utilisation d'une instance ou d'un cluster :

Un ARN d'instance RDS : `arn:aws:rds:region:account:db:name`

Un cluster à plusieurs zones de disponibilité RDS :

`arn:aws:rds:region:account:cluster:name`

Pour plus d'informations, consultez [Déploiements de clusters de base de données Multi-AZ](#) dans le Guide de l'utilisateur Amazon RDS.

Pour plus d'informations sur [Création d'un instantané de cluster de bases de données multi-AZ](#), consultez le Guide de l'utilisateur Amazon RDS.

Sauvegardes Amazon Redshift

Amazon Redshift est un entrepôt des données cloud évolutif et entièrement géré qui vous permet d'obtenir plus rapidement des informations grâce à des analyses rapides, simples et sécurisées. Vous pouvez l'utiliser AWS Backup pour protéger vos entrepôts de données grâce à des sauvegardes immuables, à des politiques d'accès distinctes et à une gouvernance organisationnelle centralisée des tâches de sauvegarde et de restauration.

Un entrepôt de données Amazon Redshift est un ensemble de ressources informatiques appelées nœuds, qui sont organisées en un groupe appelé cluster. AWS Backup peut sauvegarder ces clusters.

Pour en savoir plus sur [Amazon Redshift](#), consultez le [Guide de démarrage Amazon Redshift](#), le [Manuel du développeur de base de données Amazon Redshift](#) et le [Guide de la gestion du cluster Amazon Redshift](#).

Sauvegarde des clusters Amazon Redshift provisionnés

Vous pouvez protéger vos clusters Amazon Redshift à l'aide de la AWS Backup console ou par programmation à l'aide d'une API ou d'une CLI. Ces clusters peuvent être sauvegardés selon une planification régulière dans le cadre d'un plan de sauvegarde, ou ils peuvent être sauvegardés selon les besoins via une sauvegarde à la demande.

Vous pouvez restaurer une seule table (également appelée restauration au niveau des éléments) ou un cluster entier. Notez que les tables ne peuvent pas être sauvegardées seules ; les tables sont sauvegardées dans le cadre d'un cluster lors de la sauvegarde du cluster.

L'utilisation vous AWS Backup permet de visualiser vos ressources de manière centralisée ; toutefois, si Amazon Redshift est la seule ressource que vous utilisez, vous pouvez continuer à utiliser le planificateur de snapshots automatique dans Amazon Redshift. Notez que vous ne pouvez pas continuer à gérer les paramètres manuels des instantanés à l'aide d'Amazon Redshift si vous choisissez de les gérer via. AWS Backup

Vous pouvez sauvegarder des clusters Amazon Redshift via la AWS Backup console ou à l'aide du. AWS CLI

Il existe deux manières d'utiliser la AWS Backup console pour sauvegarder un cluster Amazon Redshift : à la demande ou dans le cadre d'un plan de sauvegarde.

Création de sauvegardes Amazon Redshift à la demande

Consultez la page [Création d'une sauvegarde à la demande](#) pour plus d'informations.

Pour créer un instantané manuel, laissez la case Sauvegarde continue décochée lorsque vous créez un plan de sauvegarde incluant les ressources Amazon Redshift.

Création de sauvegardes Amazon Redshift planifiées dans un plan de sauvegarde

Vos sauvegardes planifiées peuvent inclure des clusters Amazon Redshift s'il s'agit d'une ressource protégée. Pour choisir de protéger les clusters Amazon Redshift, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.

2. Dans le volet de navigation, choisissez Ressources protégées.
3. Activez Amazon Redshift.
4. Consultez [Attribution de ressources à la console](#) pour inclure des clusters Amazon Redshift dans un plan existant ou nouveau.

Sous Gérer les plans de backup, vous pouvez choisir de [créer un plan de sauvegarde](#) et d'inclure des clusters Amazon Redshift ou vous pouvez [mettre à jour un plan existant](#) pour inclure des clusters Amazon Redshift. Lorsque vous ajoutez le type de ressource Amazon Redshift, vous pouvez choisir d'ajouter tous les clusters Amazon Redshift ou de cocher les cases à côté des clusters que vous souhaitez inclure dans votre plan de sauvegarde.

Sauvegarde par programmation

Vous pouvez également définir votre plan de sauvegarde dans un document JSON et le fournir à l'aide de la console AWS Backup ou de l' AWS CLI. Voir [Création de plans de sauvegarde à l'aide d'un document JSON et de la AWS Backup CLI](#) pour savoir comment créer un plan de sauvegarde par programmation.

Vous pouvez effectuer les opérations suivantes avec l'API :

- Arrêter une tâche de sauvegarde.
- Décrire une tâche de sauvegarde
- Obtenir les métadonnées du point de récupération

Note

BackupSizeInBytes les métadonnées sont prises en charge pour les types de ressources suivants : volumes Amazon EBS, systèmes de fichiers Amazon EFS, bases de données Amazon RDS, tables DynamoDB, EC2 instances Amazon, systèmes de fichiers Amazon et FSx compartiments Amazon S3. Ce champ indique la taille de la sauvegarde en octets et est disponible via l'DescribeRecoveryPointAPI et la AWS Backup console. Pour les types de ressources non pris en charge, ce champ ne sera pas renseigné.

- Répertorier les points de récupération par ressource
- Répertorier les balises pour le point de récupération

Affichage des sauvegardes de cluster Amazon Redshift

Pour afficher et modifier les sauvegardes de vos tables Amazon Redshift dans la console, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Choisissez Coffres-forts de sauvegarde. Cliquez ensuite sur le nom du coffre-fort de sauvegarde qui contient vos clusters Amazon Redshift.
3. Le coffre-fort de sauvegarde affichera un résumé et une liste des sauvegardes. Vous pouvez cliquer sur le lien dans la colonne ID de récupération.
4. Pour supprimer un ou plusieurs points de récupération, cochez la ou les cases que vous souhaitez supprimer. Sous le bouton Actions, vous pouvez sélectionner Supprimer.

Restauration d'un cluster Amazon Redshift

Pour plus d'informations, consultez [Restauration d'un cluster Amazon Redshift](#).

Sauvegardes sans serveur Amazon Redshift

Aperçu

AWS Backup propose une gestion complète des sauvegardes de vos espaces de noms Amazon Redshift Serverless. Vous pouvez ainsi planifier et restaurer des instantanés manuels Redshift Serverless via AWS Backup la console ou via la CLI.

La protection des données Redshift Serverless AWS Backup propose plusieurs options pour sauvegarder et restaurer vos entrepôts de données. Vous pouvez créer un instantané planifié ou à la demande de votre espace de noms. Vous pouvez ensuite choisir de restaurer toutes les bases de données de cet instantané dans un cluster provisionné par Amazon Redshift ou dans un espace de noms sans serveur. Vous pouvez également restaurer une seule table.

Redshift Serverless propose des instantanés automatisés et manuels. Actuellement, il AWS Backup peut être utilisé pour gérer les instantanés manuels, mais pas les instantanés automatisés.

Options de sauvegarde pour Redshift Serverless

Vous pouvez utiliser la AWS Backup console ou la CLI pour créer des sauvegardes à la demande ou dans le cadre d'un plan de sauvegarde.

Créez une sauvegarde à la demande

Vous pouvez créer des sauvegardes à la demande des espaces de noms Redshift Serverless en suivant les étapes suivantes :

Console

1. Ouvrez la [AWS Backup console](#).
2. Dans le tableau de bord, choisissez Créer une sauvegarde à la demande.
3. Choisissez Redshift Serverless dans le menu déroulant des types de ressources.
4. Sélectionnez l'espace de noms que vous souhaitez sauvegarder.
5. Assurez-vous que l'option Créer une sauvegarde maintenant est sélectionnée.
6. Spécifiez la période de conservation de la sauvegarde.
7. Sélectionnez un coffre-fort de sauvegarde existant ou créez-en un.
8. Sélectionnez le rôle IAM à utiliser pour la sauvegarde.
9. Ajoutez éventuellement des balises à la sauvegarde. Pour attribuer un tag à votre sauvegarde à la demande, développez le champ Tags ajoutés aux points de restauration, choisissez Ajouter un nouveau tag, puis entrez une clé de tag et une valeur de tag.
10. Sélectionnez Créer une sauvegarde à la demande pour commencer le travail de sauvegarde.
11. Une fois la tâche lancée, la console affiche l'écran Tâches où vous pouvez voir la liste de vos tâches de sauvegarde et leur statut.

AWS CLI

Utilisez la commande `start-backup-job`.

Paramètres requis

- `BackupVaultName`
- `IamRoleArn`
- `ResourceArn`

Paramètres facultatifs

- `CompleteWindowMinutes`

- IdempotencyToken
- Lifecycle
- StartWindowMinutes

Exemple Exemple

L'exemple suivant crée une sauvegarde à la demande d'un espace de noms Redshift Serverless.

```
aws backup start-backup-job \  
  --backup-vault-name sample-vault \  
  --iam-role-arn arn:aws:iam::account:role/service-role/  
AWSBackupDefaultServiceRole \  
  --resource-arn arn:aws:redshift-serverless:region:account:namespace/namespace-  
name-UUID
```

Créez des sauvegardes Redshift sans serveur planifiées dans un plan de sauvegarde

Vous pouvez créer un nouveau plan de sauvegarde pour leurs espaces de noms Redshift Serverless via la console ou via la CLI, AWS Backup ou vous pouvez ajouter Redshift Serverless à un plan de sauvegarde existant.

Vos sauvegardes planifiées peuvent inclure des espaces de noms Redshift Serverless s'il s'agit d'une ressource protégée. Pour choisir de protéger Redshift Serverless dans la AWS Backup console, procédez comme suit :

Console

Pour choisir de protéger Redshift Serverless dans la AWS Backup console, procédez comme suit :

1. Ouvrez la [AWS Backup console](#).
2. Dans le volet de navigation, choisissez Ressources protégées.
3. Activez Amazon Redshift Serverless.
4. Consultez [Sélectionnez AWS les services à sauvegarder](#) la section pour inclure les espaces de noms Redshift Serverless dans un plan existant ou nouveau. Lorsque vous ajoutez le type de ressource Redshift Serverless, vous pouvez choisir d'ajouter tous les espaces de noms Amazon Redshift ou de cocher les cases à côté des espaces de noms que vous souhaitez sauvegarder.

Dans la section **Manage Backup plans**, vous pouvez :

- [Créez un plan de sauvegarde](#) et incluez Redshift Serverless ;
- [Mettez à jour](#) un plan de sauvegarde existant pour inclure Redshift Serverless.

AWS CLI

Voir [Créez des plans de sauvegarde à l'aide du AWS CLI](#) pour les conseils d'utilisation `create-backup-plan`.

Si vous souhaitez modifier un plan existant pour inclure vos ressources sans serveur, utilisez la commande `update-backup-plan`.

L'ARN (Amazon Resource Name) pour les ressources sans serveur à inclure dans "BackupSelection" : {« Resources » a le format suivant :

```
arn:aws:redshift-serverless:Region:account:snapshot/a12bc34d-567e-890f-123g-h4ijk56l78m9
```

Consultez [Restauration sans serveur Amazon Redshift](#) pour plus d'informations sur la restauration des données d'un instantané vers un espace de noms sans serveur.

Sauvegardes Amazon EKS

Un cluster Amazon Elastic Kubernetes Service (Amazon EKS) est composé de plusieurs ressources que vous pouvez sauvegarder en une seule unité. Lorsque vous sauvegardez un cluster Amazon EKS, vous AWS Backup créez un point de restauration composite qui inclut à la fois des sauvegardes d'état du cluster EKS et des sauvegardes de volumes persistants.

Lorsqu'un cluster Amazon EKS est sauvegardé, des points de restauration sont créés pour l'état du cluster Amazon EKS et les volumes persistants pris en charge par AWS Backup. Ces points de récupération sont regroupés au sein d'un point de récupération global appelé composite.

Une sauvegarde Amazon EKS comporte deux composants distincts :

- État du cluster Amazon EKS : il s'agit d'une sauvegarde de l'état du cluster Amazon EKS. Consultez la terminologie de sauvegarde Amazon EKS ci-dessous pour savoir ce qui est inclus.

- Stockage persistant : il s'agit d'une sauvegarde du stockage persistant (Amazon EBS, Amazon S3, Amazon Elastic File System) attaché au cluster Amazon EKS via Persistent Volume Claims et [pris en charge par le pilote EKS Add Ons CSI](#).

Terminologie de sauvegarde Amazon EKS

Les termes suivants sont utilisés dans la documentation de sauvegarde Amazon EKS. Pour la terminologie spécifique à Amazon EKS, reportez-vous à la [documentation Amazon EKS](#).

Terminologie EKS Backup

- Point de restauration composite : point de récupération utilisé pour regrouper des points de restauration imbriqués pour une sauvegarde de cluster Amazon EKS.
- Point de restauration imbriqué : point de récupération d'une ressource faisant partie d'un cluster Amazon EKS et sauvegardée dans le cadre du point de récupération composite.
- État du cluster EKS — Les manifestes Kubernetes (fichiers YAML ou JSON) qui définissent l'état souhaité des ressources Kubernetes dans votre cluster. Cela inclut les ressources et les déploiements Kubernetes tels que : les secrets, les cartes de configuration, les ensembles d'états, les classes de stockage DaemonSets, les cartes de stockage, les ensembles de répliques, les revendications de volume persistantes, les définitions de ressources personnalisées, les rôles et les liaisons de rôles.
- Child Recovery Point de configuration du cluster Amazon EKS : contient l'état du cluster Amazon EKS.
- Persistent Volume Child Recovery Points : contient des sauvegardes de volumes persistants pour les types de stockage pris en charge (EBS, S3, EFS) [pris en charge par le pilote EKS Add Ons CSI](#).

Structure de sauvegarde Amazon EKS

Les sauvegardes Amazon EKS incluent les composants suivants :

- État du cluster Amazon EKS
- Stockage persistant : sauvegardes des types de stockage pris en charge, notamment Amazon EBS, Amazon EFS et Amazon S3

Amazon EKS Backups n'inclura pas les composants suivants :

- Images de conteneurs provenant de référentiels externes (ECR, Docker)
- Composants de l'infrastructure du cluster EKS (sous-réseaux VPCs, par exemple)
- Ressources EKS générées automatiquement, telles que les nœuds, les pods générés automatiquement, les événements, les baux et les tâches.

Configuration de la sauvegarde EKS et prérequis (« Avant la sauvegarde »)

- Paramètres du cluster EKS :
 - [Le mode d'autorisation](#) du cluster EKS est défini sur API ou API_AND_CONFIG_MAP pour créer des [entrées AWS Backup d'accès permettant d'accéder](#) au cluster EKS.
- Autorisations :
 - AWS Backup la politique gérée [AWSBackupServiceRolePolicyForBackup](#) contient les autorisations requises pour sauvegarder votre cluster Amazon EKS et votre stockage persistant EBS et EFS
 - Si votre cluster EKS contient un compartiment S3, vous devez vous assurer que les politiques et conditions préalables suivantes pour votre compartiment S3 sont ajoutées et activées, comme indiqué dans la documentation :
 - [AWSBackupServiceRolePolicyForSauvegarde S3](#)
 - [Conditions préalables pour les sauvegardes S3](#)
- Chiffrement :
 - Les points de récupération pour enfants Amazon EKS seront chiffrés avec le jeu de clés Amazon KMS du Backup Vault cible
 - Les points de restauration du stockage persistant seront chiffrés conformément au support actuel pour chaque classe de stockage : instantanés EBS, sauvegardes S3, sauvegardes EFS. [Voir Chiffrement des sauvegardes dans AWS Backup](#)

Création d'une sauvegarde Amazon EKS

Le processus de création d'une sauvegarde est appelé tâche de sauvegarde. Une tâche de sauvegarde de cluster Amazon EKS possède un statut. Lorsqu'une tâche de sauvegarde est terminée, elle a le statut Terminé. Cela signifie qu'un point de restauration (une sauvegarde) a été créé.

Création d'une sauvegarde Amazon EKS à la demande

Console

Pour créer une sauvegarde à la demande de votre cluster Amazon EKS :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Sous Type de ressource, sélectionnez Amazon EKS.
4. Cochez la case à côté du cluster Amazon EKS que vous souhaitez sauvegarder.
5. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).
6. Configurez vos paramètres de sauvegarde, notamment la fenêtre de sauvegarde, la transition vers le stockage à froid et la période de conservation.
7. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).

AWS CLI

Pour créer une sauvegarde à la demande de votre cluster Amazon EKS à l'aide de AWS CLI :

Utilisez la commande start-backup-job :

```
aws backup start-backup-job \
                                --backup-vault-name my-backup-vault \
                                --resource-arn arn:aws:eks:us-
west-2:123456789012:cluster/my-cluster \
                                --iam-role-arn arn:aws:iam::123456789012:role/
service-role \
                                --region us-west-2
```

Spécifiez éventuellement des paramètres supplémentaires tels que les paramètres du cycle de vie :

```
aws backup start-backup-job \
                                --backup-vault-name my-backup-vault \
                                --resource-arn arn:aws:eks:us-
west-2:123456789012:cluster/my-cluster \
                                --iam-role-arn arn:aws:iam::123456789012:role/
service-role \
```



```
--lifecycle  
MoveToColdStorageAfterDays=30,DeleteAfterDays=365 \  
--region us-west-2
```

Surveillez l'état de la tâche de sauvegarde :

```
aws backup describe-backup-job \  
--backup-job-id backup-job-id \  
--region us-west-2
```

Format ARN de sauvegarde Amazon EKS

Point de restauration composite arn ::backup : *partition* ::recovery-point:composite:eks/ - *region accountId cluster-name timestamp*

Child Recovery Point arn ::backup : *partition* ::recovery-point:eks/ - *region accountId cluster-name timestamp*

Points de récupération Amazon EKS

Statut du point de récupération

Lorsque la tâche de sauvegarde d'un cluster Amazon EKS est terminée (le statut de la tâche est `Completed`), une sauvegarde du cluster est créée. Cette sauvegarde est également connue sous le nom de point de récupération composite. Un point de récupération composite peut avoir l'un des statuts suivants : `Completed`, `Failed` ou `Partial`.

Chaque sauvegarde Amazon EKS crée une tâche de sauvegarde parent pour le point de restauration composite et des tâches de sauvegarde enfant pour chaque point de restauration enfant (configuration du cluster et volumes persistants).

- Une tâche de sauvegarde terminée signifie que l'ensemble de votre cluster Amazon EKS et les ressources qu'il contient sont protégés par AWS Backup.
- Un statut d'échec indique que la tâche de sauvegarde a échoué ; vous devez créer à nouveau la sauvegarde une fois le problème à l'origine de l'échec résolu.
- Un `Partial` statut signifie que toutes les ressources du cluster n'ont pas été sauvegardées. Cela peut se produire si une ou plusieurs tâches de sauvegarde appartenant aux ressources du cluster (ressources imbriquées) ont un statut autre que `Completed`. Vous pouvez créer manuellement

une sauvegarde à la demande pour exécuter à nouveau toutes les ressources dont le statut n'est pas `Completed`.

Chaque ressource imbriquée au sein du point de récupération composite possède son propre point de récupération individuel, chacun ayant son propre statut (`Completed` ou `Failed`). Les points de récupération imbriqués dont le statut est `Completed` peuvent être restaurés.

AWS Backup prend en charge les transitions du cycle de vie vers le stockage à froid pour les points de restauration de volumes persistants. Vous pouvez vous abonner aux notifications pour recevoir des alertes sur l'état des tâches de sauvegarde.

Gestion des points de récupération

Les points de restauration composites (sauvegardes) peuvent être copiés ; les points de restauration secondaires des volumes persistants peuvent être copiés, supprimés, dissociés ou restaurés. Le point de récupération enfant de l'état du cluster Amazon EKS ne peut pas être copié, supprimé ou dissocié car il entretient une relation 1:1 avec son point de récupération composite parent.

Un point de récupération composite contenant des sauvegardes imbriquées ne peut pas être supprimé. Une fois que les points de récupération imbriqués au sein d'un point de récupération composite ont été supprimés ou dissociés, vous pouvez supprimer manuellement le point de récupération composite ou le laisser subsister jusqu'à ce que le cycle de vie du plan de sauvegarde le supprime.

Suppression d'un point de récupération

Vous pouvez supprimer un point de récupération à l'aide de la console ou du AWS CLI.

Pour supprimer des points de récupération à l'aide de la console :

Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup/>.

1. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez EKS pour afficher uniquement vos clusters Amazon EKS.
2. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cocher la case située à gauche de chaque point de récupération pour l'inclure dans votre sélection de points de récupération que vous souhaitez supprimer.

3. Cliquez sur le bouton Supprimer.

Lorsque vous utilisez la console pour supprimer un ou plusieurs points de récupération composite, un message d'avertissement apparaît. Cette boîte d'avertissement vous demande de confirmer votre intention de supprimer les points de récupération composite, y compris les points de récupération imbriqués dans les piles composites.

Pour supprimer des points de récupération à l'aide de l'API, utilisez la `DeleteRecoveryPoint` commande.

Lorsque vous utilisez l'API avec le, AWS Command Line Interface vous devez supprimer tous les points de récupération imbriqués avant de supprimer un point composite.

Dissociation d'un point de récupération imbriqué d'un point de récupération composite

Vous pouvez dissocier un point de récupération imbriqué d'un point de récupération composite (par exemple, vous souhaitez conserver le point de récupération imbriqué mais supprimer le point de récupération composite). Les deux points de récupération resteront, mais ils ne seront plus connectés ; en d'autres termes, les actions effectuées sur le point de récupération composite ne s'appliqueront plus au point de récupération imbriqué une fois celui-ci dissocié. Le point de récupération enfant de l'état du cluster Amazon EKS ne peut pas être dissocié car il entretient une relation 1:1 avec son point de récupération composite parent.

Vous pouvez dissocier le point de récupération à l'aide de la console ou appeler l'API `DisassociateRecoveryPointFromParent`.

Copie d'un point de récupération

Vous pouvez copier un point de récupération composite ou un point de récupération imbriqué si la ressource prend en charge la copie [entre comptes et entre régions](#).

Pour copier des points de restauration à l'aide de la AWS Backup console :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez EKS pour afficher uniquement vos clusters Amazon EKS.
3. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour

développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cliquer sur le bouton circulaire situé à gauche de n'importe quel point de récupération pour le copier.

4. Une fois sélectionné, cliquez sur le bouton Copier dans le coin supérieur droit du volet.

Les sauvegardes Amazon EKS prennent en charge tous les types de copies :

- Même région/même compte
- Compte croisé
- Entre régions
- Régions d'adhésion

Limitations

- Les volumes persistants utilisant un pilote CSI via une migration CSI, les plug-ins de stockage intégrés à l'arborescence ou les contrôleurs ACK ne sont pas pris en charge.
- Les compartiments Amazon S3 associés à des préfixes spécifiques associés au pilote CSI MountPoints ne peuvent pas être sauvegardés. Seuls les buckets Amazon S3 en tant que cibles sont pris en charge, pas de préfixes spécifiques
- Les sauvegardes de bucket Amazon S3 dans le cadre d'une sauvegarde de cluster EKS ne prendront en charge que les sauvegardes instantanées.
- Le pilote Amazon FSx via CSI n'est pas pris en charge via EKS Backups
- Soumis à des [quotas de sauvegarde et de restauration](#)

Questions fréquentes (FAQ)

1. « Qu'est-ce qui est inclus dans la sauvegarde Amazon EKS ? »

Dans le cadre de chaque sauvegarde d'un cluster Amazon EKS, l'état du cluster Amazon EKS et les volumes persistants pris en charge par AWS Backup celui-ci sont sauvegardés. L'état du cluster Amazon EKS inclut des informations telles que le nom du cluster, le rôle IAM, la configuration Amazon VPC, les paramètres réseau, la journalisation, le chiffrement, les extensions, les entrées d'accès, les groupes de nœuds gérés, les profils Fargate, les associations d'identité des pods et les fichiers manifestes Kubernetes.

2. « Un statut *Partial* signifie-t-il que la création de ma sauvegarde a échoué ? »

Non. Un statut partiel indique que certains points de récupération ont été sauvegardés, tandis que d'autres ne l'ont pas été. Il existe deux conditions pour vérifier si vous attendiez un résultat `Completed` de sauvegarde :

- a. Une ou plusieurs tâches de sauvegarde appartenant aux ressources du cluster n'ont pas abouti et la tâche doit être réexécutée.
 - b. Un point de récupération imbriqué a été supprimé ou dissocié d'un point de récupération composite.
3. « Dois-je installer un agent ou un module complémentaire Amazon EKS sur mon cluster Amazon EKS avant la sauvegarde ? »

Non AWS Backup ne nécessite l'installation d'aucun agent ou module complémentaire sur votre cluster Amazon EKS. La seule condition préalable est de définir le [mode d'autorisation](#) de votre cluster EKS sur `API` ou `API_AND_CONFIG_MAP` pour créer des [entrées d'accès AWS Backup pour accéder](#) au cluster EKS.

4. « Les sauvegardes Amazon EKS incluent-elles des composants d'infrastructure Amazon EKS ou des images Amazon ECR ? »

Non Les sauvegardes Amazon EKS se concentrent sur l'état du cluster EKS et les charges de travail des applications, et non sur les composants d'infrastructure sous-jacents ou les images de conteneur.

5. « Puis-je transformer mon point de restauration composite EKS en chambre froide ? »

Vous pouvez passer à la chambre froide pour les points de récupération pour enfants sous-jacents qui prennent en charge les niveaux de stockage frigorifique. Consultez la [matrice de disponibilité des AWS Backup fonctionnalités](#) pour obtenir la liste complète des services d'assistance.

6. « Mes sauvegardes EKS sont-elles incrémentielles ? »

AWS Backup effectuera des sauvegardes incrémentielles de chaque point de restauration enfant lorsqu'il est pris en charge aujourd'hui, y compris les volumes EBS, les systèmes de fichiers EFS et les compartiments S3. Le point de restauration secondaire de l'état du cluster EKS sera une sauvegarde complète. Consultez la [matrice AWS Backup de disponibilité des fonctionnalités](#).

7. « Puis-je créer un index et effectuer des recherches dans mes sauvegardes EKS ? »

Non, mais vous pouvez créer des index à la demande et rechercher des volumes persistants dans lesquels le type de stockage sous-jacent prend en charge cette fonctionnalité. AWS Backup Consultez la [matrice AWS Backup de disponibilité des fonctionnalités](#).

Sauvegarde SAP HANA sur Amazon EC2

Note

[Services pris en charge par Région AWS](#) contient les régions actuellement prises en charge dans lesquelles les sauvegardes de base de données SAP HANA sur les EC2 instances Amazon sont disponibles.

AWS Backup prend en charge les sauvegardes et les restaurations des bases de données SAP HANA sur les EC2 instances Amazon.

Rubriques

- [Vue d'ensemble des bases de données SAP HANA avec AWS Backup](#)
- [Conditions préalables à la sauvegarde des bases de données SAP HANA via AWS Backup](#)
- [Opérations de sauvegarde SAP HANA dans la console AWS Backup](#)
- [Afficher les sauvegardes de base de données SAP HANA](#)
- [Utilisation AWS CLI pour les bases de données SAP HANA avec AWS Backup](#)
- [Résolution des problèmes de sauvegarde des bases de données SAP HANA](#)
- [Glossaire des termes de SAP HANA lors de l'utilisation AWS Backup](#)
- [AWS Backup support des bases de données SAP HANA sur les EC2 instances \(notes de version\)](#)

Vue d'ensemble des bases de données SAP HANA avec AWS Backup

Outre la possibilité de créer des sauvegardes et de restaurer des bases de données, AWS Backup l'intégration avec Amazon EC2 Systems Manager for SAP permet aux clients d'identifier et de baliser les bases de données SAP HANA.

AWS Backup est intégré à AWS Backint Agent pour effectuer des sauvegardes et des restaurations SAP HANA. Pour plus d'informations, consultez [AWS Backint](#).

Conditions préalables à la sauvegarde des bases de données SAP HANA via AWS Backup

Plusieurs conditions préalables doivent être remplies avant que les activités de sauvegarde et de restauration puissent être effectuées. Notez que vous aurez besoin d'un accès administratif à votre

base de données SAP HANA et d'autorisations pour créer de nouveaux rôles et politiques IAM dans votre AWS compte afin d'effectuer ces étapes.

Complétez [ces prérequis sur Amazon EC2 Systems Manager](#).

1. [Configurer les autorisations requises pour l' EC2 instance Amazon exécutant la base de données SAP HANA](#)
2. [Enregistrez vos informations d'identification dans AWS Secrets Manager](#)
3. [Installez AWS Backup et AWS Systems Manager pour les agents SAP](#)
4. [Vérifier l'agent SSM](#)
5. [Vérifier les paramètres](#)
6. [Enregistrer la base de données SAP HANA](#)

Il est recommandé d'enregistrer chaque instance HANA une seule fois. Plusieurs inscriptions peuvent en entraîner plusieurs ARNs pour la même base de données. Le maintien d'un ARN et d'un enregistrement uniques simplifie la création et la maintenance des plans de sauvegarde et peut également contribuer à réduire la duplication imprévue des sauvegardes.

Opérations de sauvegarde SAP HANA dans la console AWS Backup

Une fois les prérequis et le SSM pour les configurations SAP terminés, vous pouvez sauvegarder et restaurer votre SAP HANA sur des bases de données. EC2

Activation de la protection des ressources SAP HANA

AWS Backup Pour protéger vos bases de données SAP HANA, SAP HANA doit être activé comme l'une des ressources protégées. Pour l'activer :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Activation du service, sélectionnez Configurer les ressources.
4. Inscrivez-vous à SAP HANA sur Amazon EC2. .
5. Cliquez sur Confirmer.

L'opt-in au service pour SAP HANA sur Amazon EC2 sera désormais activé.

Création d'une sauvegarde planifiée des bases de données SAP HANA

Vous pouvez [modifier un plan de sauvegarde existant](#) et y ajouter des ressources SAP HANA, ou vous pouvez [créer un nouveau plan de sauvegarde](#) uniquement pour les ressources SAP HANA.

Si vous choisissez de créer un nouveau plan de sauvegarde, trois options s'offrent à vous :

1. Option 1 : démarrer avec un modèle

1. Choisissez un modèle de plan de sauvegarde.
2. Spécifiez un nom de plan de sauvegarde.
3. Cliquez sur Créer un plan.

2. Option 2 : élaborer un nouveau plan

1. Spécifiez un nom de plan de sauvegarde.
2. (Facultatif) Spécifiez les balises à ajouter au plan de sauvegarde.
3. Spécifiez la configuration des règles de sauvegarde.
 - a. Spécifiez un nom de règle de sauvegarde.
 - b. Sélectionnez un coffre-fort de sauvegarde existant ou créez-en un. C'est ici que vos sauvegardes sont stockées.
 - c. Spécifiez une fréquence de sauvegarde.
 - d. Spécifiez une fenêtre de sauvegarde.

Notez que la transition vers le stockage à froid n'est actuellement pas prise en charge.

- e. Spécifiez la période de rétention.

La copie vers la destination n'est actuellement pas prise en charge

- f. (Facultatif) Spécifiez les balises à ajouter aux points de récupération.

4. Cliquez sur Créer un plan.

3. Option 3 : définir un plan à l'aide de JSON

1. Spécifiez le JSON de votre plan de sauvegarde en modifiant l'expression JSON d'un plan de sauvegarde existant ou en créant une nouvelle expression.
2. Spécifiez un nom de plan de sauvegarde.
3. Cliquez sur Valider l'expression JSON.

Une fois le plan de sauvegarde créé, vous pouvez attribuer des ressources au plan de sauvegarde à l'étape suivante.

Quel que soit le plan que vous utilisez, assurez-vous d'[attribuer les ressources](#). Vous pouvez choisir les bases de données SAP HANA à attribuer, y compris les bases de données système et locataire. Vous avez également la possibilité d'exclure une ressource spécifique IDs.

Créez une sauvegarde à la demande des bases de données SAP HANA

Vous pouvez [créer une sauvegarde à la demande complète](#) qui s'exécute immédiatement après sa création. Notez que les sauvegardes à la demande des bases de données SAP HANA sur les EC2 instances Amazon sont des sauvegardes complètes ; les sauvegardes incrémentielles ne sont pas prises en charge.

Votre sauvegarde à la demande est à présent créée. Elle commencera à sauvegarder les ressources que vous avez spécifiées. La console vous redirigera vers la page des Tâches de sauvegarde, où vous pouvez voir la progression des tâches. Notez l'ID de la tâche de sauvegarde indiqué dans la bannière bleue en haut de votre écran, car vous en aurez besoin pour trouver facilement le statut de votre tâche de sauvegarde. Lorsque la sauvegarde est terminée, le statut passe à Completed. Les sauvegardes peuvent prendre plusieurs heures.

Actualisez la Liste des tâches de sauvegarde pour voir le changement de statut. Vous pouvez également rechercher et cliquer sur votre ID de tâche de backup pour afficher le statut détaillé de la tâche.

Sauvegardes continues des bases de données SAP HANA

Vous pouvez effectuer [des sauvegardes continues](#), qui peuvent être utilisées avec la point-in-time restauration (PITR) (notez que les sauvegardes à la demande préservent les ressources dans l'état dans lequel elles ont été prises, tandis que PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps).

Grâce aux sauvegardes continues, vous pouvez restaurer votre base de données SAP HANA sur une EC2 instance en la ramenant à l'heure précise de votre choix, dans un délai d'une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. La restauration PITR fonctionne en accédant à votre

sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure indiquée AWS Backup pour la restauration.

Vous pouvez opter pour les sauvegardes continues lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API.

Pour activer les sauvegardes continues à l'aide de la console

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sous Règles de sauvegarde, choisissez Ajouter une règle de sauvegarde.
4. Dans la section Configuration de règle de backup, sélectionnez Activer les sauvegardes continues pour les ressources prises en charge.

Une fois que vous avez désactivé le [PITR \(point-in-timerestoration\)](#) pour les sauvegardes de base de données SAP HANA, les journaux continueront d'être envoyés AWS Backup jusqu'à expiration du point de restauration (statut égal à). EXPIRED) Vous pouvez passer à un autre emplacement de sauvegarde des journaux dans SAP HANA pour arrêter la transmission des journaux à AWS Backup.

Un point de restauration continue dont l'état est égal à STOPPED indique qu'un point de restauration continue a été interrompu ; en d'autres termes, les journaux transmis par SAP HANA à AWS Backup ce point et indiquant les modifications incrémentielles apportées à une base de données présentent une lacune. Les points de récupération qui se produisent pendant cet intervalle de temps ont un statut STOPPED..

Pour les problèmes que vous pouvez rencontrer lors des tâches de sauvegardes continues (points de récupération), consultez la section [Dépannage de la restauration SAP HANA](#) dans ce guide.

Afficher les sauvegardes de base de données SAP HANA

Affichage du statut de vos tâches de sauvegarde et de récupération :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Choisissez des tâches de sauvegarde, des tâches de restauration ou des tâches de copie pour voir la liste de vos tâches.
4. Recherchez et cliquez sur votre ID de tâche pour afficher les statuts détaillés de la tâche.

Affichage de tous les points de récupération dans un coffre :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Recherchez et cliquez sur un coffre-fort de sauvegarde pour afficher tous les points de récupération qu'il contient.

Affichage des détails des ressources protégées :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Vous pouvez également filtrer par type de ressource pour afficher toutes les sauvegardes de ce type de ressource.

Utilisation AWS CLI pour les bases de données SAP HANA avec AWS Backup

Chaque action dans la console Backup est associée à un appel d'API correspondant.

Pour configurer AWS Backup et gérer ses ressources par programmation, utilisez l'appel d'API [StartBackupJob](#) pour sauvegarder une base de données SAP HANA sur une instance. EC2

Utilisez `start-backup-job` comme commande de l'interface de ligne de commande.

Résolution des problèmes de sauvegarde des bases de données SAP HANA

Si vous rencontrez des erreurs au cours de votre flux de travail, consultez les exemples d'erreurs suivants et les solutions suggérées :

Prérequis pour Python

- Erreur : erreur Zypper liée à la version de Python depuis SSM pour SAP et nécessitant AWS Backup Python 3.6, mais SUSE 12 prend en charge Python 3.4 SP5 par défaut.

Résolution : installez plusieurs versions de Python SUSE12 SP5 en procédant comme suit :

1. Exécutez une commande `update-alternatives` pour créer un lien symbolique pour Python 3 dans «/3 ». `usr/local/bin/` instead of directly using `'/usr/bin/python` Cette commande définira Python 3.4 comme version par défaut. La commande est la suivante :

```
# sudo update-alternatives --install /usr/local/bin/python3 python3 /usr/bin/python3.4 5
```

2. Ajoutez Python 3.6 à la configuration alternative en exécutant la commande suivante : `# sudo update-alternatives --install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
3. Modifiez la configuration alternative en Python 3.6 en exécutant la commande suivante : `# sudo update-alternatives --config python3`

Le résultat suivant doit être affiché :

```
There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
  Selection Path Priority Status
*  0 /usr/bin/python3.4 5 auto mode
  1 /usr/bin/python3.4 5 manual mode
  2 /usr/bin/python3.6 2 manual mode
Press enter to keep the current choice[*], or type selection number:
```

4. Entrez le numéro correspondant à Python 3.6.
5. Vérifiez la version de Python et confirmez que Python 3.6 est utilisé.
6. (Facultatif, mais recommandé) Vérifiez que les commandes Zypper fonctionnent comme prévu.

Amazon EC2 Systems Manager pour la découverte et l'enregistrement de SAP

- Erreur : SSM pour SAP n'a pas réussi à découvrir la charge de travail en raison du blocage de l'accès au point de terminaison public pour AWS Secrets Manager et SSM.

Solution : testez si les points de terminaison sont accessibles depuis votre base de données SAP HANA. S'ils ne peuvent pas être atteints, vous pouvez créer des points de terminaison Amazon VPC AWS Secrets Manager et SSM pour SAP.

1. Testez l'accès à Secrets Manager depuis EC2 l'hôte Amazon pour HANA DB en exécutant la commande suivante : `aws secretsmanager get-secret-value --secret-id hanaeccsbx_hbx_database_awsbkp`. Si la commande ne renvoie aucune valeur, le pare-feu bloque l'accès au point de terminaison du service Secrets Manager. Le journal s'arrêtera à l'étape « Récupération des secrets depuis Secrets Manager ».
2. Testez la connectivité au SSM pour le point de terminaison SAP en exécutant la commande `aws ssm-sap list-registration`. Si la commande ne renvoie aucune valeur, le pare-feu bloque l'accès au point de terminaison SSM pour SAP.

Exemple d'erreur : Connection was closed before we received a valid response from endpoint URL: "https://ssm-sap.us-west-2.amazonaws.com/register-application".

Deux options s'offrent à vous si les points de terminaison ne sont pas accessibles.

- Ouvrez des ports de pare-feu pour permettre à Secrets Manager et à SSM pour SAP d'accéder au point de terminaison de service public ; ou
- Créez des points de terminaison VPC pour Secrets Manager et SSM pour SAP, puis :
 - Assurez-vous qu'Amazon VPC est activé pour DNSSupport et. DNSHostname
 - Assurez-vous que votre point de terminaison VPC a activé l'option Autoriser le nom DNS privé.
 - Si le SSM pour SAP Discovery s'est terminé avec succès, le journal indiquera que l'hôte a été découvert.
- Erreur : AWS Backup et la connexion Backint échoue en raison d'un accès bloqué aux points de terminaison publics du AWS Backup service. aws-backint-agent.log peut afficher des erreurs similaires à celles-ci : time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id" ou level=fatal msg="Error performing backup missing backup data plane Id. En outre, la AWS Backup console peut afficher Fatal Error: An internal error occurred.

Résolution : Ouvrez les ports du pare-feu pour autoriser l'accès aux points de terminaison de service public (HTTPS). Une fois cette option utilisée, le DNS résoudra les demandes adressées aux AWS services via des adresses IP publiques.

- Erreur : L'enregistrement de SSM pour SAP échoue car le mot de passe HANA contient des caractères spéciaux. Les exemples d'erreurs peuvent inclure Error connecting to database HBX/HBX when validating its credentials. ou Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated. après avoir testé une connexion à l'aide de hdbsql for systemdb et tenantdb qui a été testée à partir d'une EC2 instance Amazon de la base de données HANA.

Dans la AWS Backup console de la page Tâches, les détails de la tâche de sauvegarde peuvent indiquer un état FAILED d'erreur Miscellaneous: b' * 10: authentication failed SQLSTATE: 28000\n'.

Résolution : Assurez-vous que votre mot de passe ne contient pas de caractères spéciaux, tels que \$.

- Erreur : **b'* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...**

Résolution : L'installation de l' AWS BackInt agent pour SAP HANA ne s'est peut-être pas terminée correctement. Réessayez le processus pour déployer le [AWS Backint Agent et l'agent Amazon EC2 Systems Manager](#) sur votre serveur d'applications SAP.

- Erreur : la console ne correspond pas aux fichiers journaux après l'enregistrement.

Le journal de découverte indique l'échec de l'enregistrement lors de la tentative de connexion à HANA DB en raison de la présence de caractères spéciaux dans le mot de passe, bien que la console SSM for SAP Application Manager for SAP indique que l'enregistrement a bien été effectué. Il ne confirme pas que l'enregistrement a bien été effectué. Si la console indique un enregistrement réussi, mais pas les journaux, les sauvegardes échoueront.

Confirmez le statut de l'enregistrement :

1. Connectez-vous à la console [SSM](#)
2. Sélectionnez Exécuter la commande dans le menu de navigation de gauche.
3. Dans le champ de texte Historique des commandes, entrez `Instance ID:Equal:`, avec la valeur égale à l'instance que vous avez utilisée pour l'enregistrement. Cela filtrera l'historique des commandes.
4. Utilisez la colonne `command id` pour rechercher les commandes dont le statut est défini `Failed`. Recherchez ensuite le nom du document de `AWSSystemsManagerSAP-Discovery`.
5. Dans l'AWS CLI, exécutez la commande `aws ssm-sap register-application status`. Si la valeur renvoyée s'affiche `Error`, l'enregistrement a échoué.

Solution : Assurez-vous que votre mot de passe HANA ne comporte pas de caractères spéciaux (tels que « \$ »).

Création d'une sauvegarde d'une base de données SAP HANA

- Erreur : AWS Backup la console affiche le message « Erreur fatale » lorsqu'une sauvegarde à la demande pour SystemDB ou TenantDB est créée. Cela se produit car le point de terminaison public n'est pas accessible. Cela est dû à un pare-feu côté client qui bloque l'accès à ce point de terminaison.

`aws-backint-agent.log` peut afficher des erreurs telles que `level=error msg="Storage configuration validation failed: missing backup data plane Id"` ou `level=fatal msg="Error performing backup missing backup data plane Id."`

Solution : Ouvrez l'accès par pare-feu au point de terminaison public.

- Erreur : `Database cannot be backed up while it is stopped.`

Résolution : assurez-vous que la base de données à sauvegarder est active. Les données et journaux de base de données ne peuvent être sauvegardés que tant que la base de données est en ligne.

- Erreur : `Getting backup metadata failed. Check the SSM document execution for more details.`

Résolution : assurez-vous que la base de données à sauvegarder est active. Les données et journaux de base de données ne peuvent être sauvegardés que tant que la base de données est en ligne.

Surveillance des journaux de sauvegarde

- Erreur : `Encountered an issue with log backups, please check SAP HANA for details.`

Solution : Vérifiez SAP HANA pour vous assurer que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.

- Erreur : `One or more log backup attempts failed for recovery point.`

Résolution : vérifiez SAP HANA pour plus de détails. Assurez-vous que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.

- Erreur : `Unable to determine the status of log backups for recovery point.`

Résolution : vérifiez SAP HANA pour plus de détails. Assurez-vous que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.

- Erreur : `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

Résolution : attendez que la tâche de restauration soit terminée. Les sauvegardes du journal devraient reprendre.

Glossaire des termes de SAP HANA lors de l'utilisation AWS Backup

Types de sauvegarde des données : SAP HANA prend en charge deux types de sauvegardes de données : les sauvegardes complètes et les sauvegardes INC (incrémentielles). AWS Backup optimise le type utilisé lors de chaque opération de sauvegarde.

Sauvegardes de catalogue : SAP HANA gère son propre manifeste appelé catalogue. AWS Backup interagit avec ce catalogue. Chaque nouvelle sauvegarde créera une entrée dans le catalogue.

Sauvegarde continue des journaux (journaux des transactions) : pour les fonctions de récupération ponctuelle (PITR), SAP HANA suit toutes les transactions depuis la dernière sauvegarde.

Copie système : tâche de restauration dans laquelle la base de données cible de restauration est différente de la base de données source à partir de laquelle le point de récupération a été créé.

Restauration destructive : une restauration destructive est un type de tâche de restauration au cours de laquelle une base de données restaurée supprime ou remplace la base de données source ou existante.

FULL : une sauvegarde d'une base de données complète.

INC : une sauvegarde incrémentielle est une sauvegarde de toutes les modifications apportées à une base de données SAP HANA depuis la sauvegarde précédente.

AWS Backup support des bases de données SAP HANA sur les EC2 instances (notes de version)

Certaines fonctionnalités ne sont pas prises en charge pour le moment :

- Les sauvegardes continues (qui utilisent des journaux de transactions) ne peuvent pas être copiées vers d'autres régions ou comptes. Les sauvegardes instantanées peuvent être copiées vers des régions et des comptes pris en charge à partir de sauvegardes complètes.
- Backup Audit Manager et les rapports ne sont actuellement pas pris en charge.
- [Services pris en charge par Région AWS](#) contient les régions actuellement prises en charge pour les sauvegardes de base de données SAP HANA sur les EC2 instances Amazon.

Sauvegardes Amazon S3

Aperçu

AWS Backup prend en charge la sauvegarde et la restauration centralisées des applications stockant des données dans S3 uniquement ou parallèlement à d'autres AWS services de base de données, de stockage et de calcul. De nombreuses [fonctionnalités sont disponibles pour les sauvegardes S3](#), notamment Backup Audit Manager.

Vous pouvez utiliser une politique de sauvegarde unique AWS Backup pour automatiser de manière centralisée la création de sauvegardes des données de vos applications. AWS Backup organise automatiquement les sauvegardes entre différents AWS services et applications tierces dans un emplacement crypté centralisé (appelé [coffre de sauvegarde](#)) afin que vous puissiez gérer les sauvegardes de l'ensemble de votre application via une expérience centralisée. Pour S3, vous pouvez créer des sauvegardes continues, restaurer les données de votre application stockées dans S3 et restaurer les sauvegardes point-in-time en un seul clic.

Hiérarchisation des sauvegardes

Amazon S3 est la seule ressource qui prend en charge la hiérarchisation des sauvegardes vers un niveau de stockage chaud moins coûteux. Pour plus d'informations, consultez la section [Hiérarchisation des sauvegardes](#).

Conditions préalables pour les sauvegardes S3

Autorisations et politiques relatives à la sauvegarde et à la restauration Amazon S3

Pour sauvegarder, copier et restaurer des ressources S3, vous devez disposer des politiques appropriées à votre rôle. Pour ajouter ces politiques, accédez à [Politiques gérées par AWS](#). Ajoutez [AWSBackupServiceRolePolicyForS3Backup](#) et [AWSBackupServiceRolePolicyForS3Restore](#) aux rôles que vous souhaitez utiliser pour sauvegarder et restaurer des compartiments S3.

Si vous ne disposez pas des autorisations suffisantes, demandez au responsable du compte administratif (admin) de votre organisation d'ajouter les politiques aux rôles prévus.

Pour plus d'informations, consultez [Politiques gérées et politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Sauvegardes et gestion des versions

Vous devez [activer la gestion des versions S3 sur votre compartiment S3](#) pour pouvoir l'utiliser AWS Backup pour Amazon S3.

Nous vous recommandons de [définir une période d'expiration du cycle de vie](#) pour vos versions S3.

Tous les objets (y compris toutes les versions) présents dans le compartiment au début de la sauvegarde seront stockés dans le point de restauration (sauvegarde terminée). Il peut s'agir de la version actuelle de chaque objet, des anciennes versions, des marqueurs de suppression et des objets en attente d'actions du cycle de vie.

Le coût de stockage sera calculé pour tous les objets de la sauvegarde, y compris les objets dont la suppression est prévue (objets qui expireront). Vous pouvez utiliser une CLI ou des scripts pour supprimer l'inclusion d'objets dont l'expiration est prévue.

Pour en savoir plus sur la configuration des politiques de cycle de vie S3, suivez les instructions [sur cette page](#).

Considérations relatives aux sauvegardes Amazon S3

Les points suivants doivent être pris en compte lors de la sauvegarde des ressources S3 :

- Support ciblé des métadonnées d'objets : AWS Backup prend en charge les métadonnées suivantes : balises, listes de contrôle d'accès (ACLs), métadonnées définies par l'utilisateur, date de création d'origine et ID de version. Vous pouvez également restaurer toutes les données et métadonnées sauvegardées, à l'exception de la date de création d'origine, de l'ID de version, de la classe de stockage et des balises électroniques.
- Lorsque vous restaurez un objet S3, AWS Backup applique une valeur de somme de contrôle, même si l'objet d'origine n'a pas utilisé la fonction de somme de contrôle.
- Le nom d'une clé d'objet S3 peut être composé de la plupart des chaînes encodables en UTF-8. Les caractères Unicode suivants sont acceptés : #x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF .

Les noms de clés d'objet qui incluent des caractères ne figurant pas dans cette liste peuvent être exclus des sauvegardes.

- Transition vers le stockage à froid : utilisez la politique de gestion AWS Backup du cycle de vie pour définir le calendrier d'expiration des sauvegardes. La transition vers le stockage à froid des sauvegardes S3 n'est pas prise en charge.

- Pour les sauvegardes périodiques, AWS Backup faites de votre mieux pour suivre toutes les modifications apportées aux métadonnées de votre objet. Toutefois, si vous mettez à jour une balise ou une liste ACL plusieurs fois en une minute, AWS Backup peut ne pas capturer tous les états intermédiaires.
- AWS Backup ne prend pas en charge les sauvegardes d' [SSE-C-encrypted](#) objets. AWS Backup ne prend pas non plus en charge les sauvegardes des configurations de compartiments, y compris les politiques, les paramètres, les noms ou les points d'accès des compartiments.
- AWS Backup ne prend pas en charge les sauvegardes de S3 sur AWS Outposts.
- CloudTrail journalisation — Si vous enregistrez des événements de lecture de données, CloudTrail les journaux doivent être envoyés dans un autre compartiment cible. Si vous enregistrez CloudTrail les journaux dans le compartiment qu'ils enregistrent, une boucle infinie se produit, ce qui peut entraîner des frais inattendus.

Pour plus d'informations, veuillez consulter la rubrique [Événements de données](#) dans le Guide de l'utilisateur CloudTrail .

- Journalisation des accès au serveur : si vous activez la journalisation des accès au serveur, les journaux doivent être envoyés dans un autre compartiment cible. Si vous enregistrez ces journaux dans le compartiment qu'ils enregistrent, il y a une boucle infinie. Pour plus d'informations, consultez [Activer la journalisation des accès au serveur Amazon S3](#).

Types et quantités de seaux pris en charge

AWS Backup prend en charge la sauvegarde et la restauration de compartiments S3 à usage général. Les compartiments de répertoire ne sont pas pris en charge pour le moment.

La limite supérieure de la quantité d'une ressource (appelée quota), telle qu'un bucket, autorisée dans un AWS compte dépend du service. Les [quotas Amazon S3](#) sont différents des [AWS Backup quotas](#).

Dans chaque AWS compte, vous pouvez créer des sauvegardes pour un maximum de 100 compartiments par défaut. Vous pouvez demander une augmentation du quota jusqu'à 1 000 compartiments.

Les comptes contenant plus de 1 000 compartiments sont soumis à des limites de quota ; lorsque les demandes dépassent le quota, des tâches peuvent échouer. Il est recommandé de limiter un compte à 1 000 compartiments.

Classes de stockage S3 prises en charge

AWS Backup vous permet de sauvegarder vos données S3 stockées dans les [classes de stockage S3](#) suivantes :

- S3 Standard
- Standard S3 - Accès peu fréquent (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Hiérarchisation intelligente (S3 INT)

Les sauvegardes d'un objet de la classe de stockage [S3 Intelligent-Tiering \(INT\)](#) accèdent à ces objets. Cet accès déclenche S3 Intelligent-Tiering pour déplacer automatiquement ces objets vers Frequent Access.

Les sauvegardes qui accèdent aux niveaux d'accès peu fréquents, y compris les classes S3 Standard - Infrequent Access (IA) et S3 One Zone-IA, sont soumises aux frais de stockage S3 liés à l'accès fréquent (s'applique aux niveaux d'accès peu fréquent ou d'accès instantané aux archives).

Les classes de stockage archivées S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive ne sont pas prises en charge.

Pour plus d'informations sur la tarification du stockage pour Amazon S3, consultez la section [Tarification d'Amazon S3](#).

Types de sauvegarde S3

Avec AWS Backup, vous pouvez créer les types de sauvegardes suivants de vos compartiments S3, notamment des données d'objets, des balises, des listes de contrôle d'accès (ACLs) et des métadonnées définies par l'utilisateur :

- Les sauvegardes continues vous permettent de procéder à des restaurations à n'importe quel moment au cours des 35 derniers jours. Les sauvegardes continues d'un compartiment S3 ne doivent être configurées que dans le cadre d'un seul plan de sauvegarde.

Consultez [Récupération ponctuelle](#) pour obtenir une liste des services pris en charge et des instructions sur la manière d'utiliser AWS Backup pour effectuer des sauvegardes continues.

- Les sauvegardes périodiques utilisent des instantanés de vos données pour vous permettre de conserver les données pendant la durée spécifiée, jusqu'à 99 ans. Vous pouvez planifier des sauvegardes périodiques à des fréquences telles que 1 heure, 12 heures, 1 jour, 1 semaine ou 1 mois. AWS Backup effectue des sauvegardes périodiques pendant la fenêtre de sauvegarde que vous définissez dans votre [plan de sauvegarde](#).

Consultez [la section Création d'un plan de sauvegarde](#) pour comprendre comment AWS Backup appliquer votre plan de sauvegarde à vos ressources.

Des copies entre comptes et entre régions sont disponibles pour les sauvegardes S3, mais les copies de sauvegardes continues ne disposent pas de fonctionnalités de point-in-time restauration.

Les sauvegardes continues et périodiques des compartiments S3 doivent toutes deux résider dans le même coffre-fort de sauvegarde.

AWS Backup pour S3 repose sur la réception d'événements S3 via Amazon EventBridge. Si ce paramètre est désactivé dans les paramètres de notification des compartiments S3, les sauvegardes continues s'arrêteront pour ces compartiments, le paramètre étant désactivé. Pour plus d'informations, consultez la section [Utilisation EventBridge](#).

Pour les deux types de sauvegarde, la première sauvegarde est complète, tandis que les sauvegardes suivantes sont incrémentielles au niveau de l'objet.

Comparaison des types de sauvegarde S3

Votre stratégie de sauvegarde des ressources S3 peut impliquer uniquement des sauvegardes continues, des sauvegardes périodiques (instantanés) ou une combinaison des deux. Les informations ci-dessous peuvent vous aider à choisir ce qui convient le mieux à votre organisation :

Sauvegardes continues uniquement :

- Une fois la première sauvegarde complète de vos données existantes terminée, les modifications apportées aux données de votre compartiment S3 sont suivies au fur et à mesure qu'elles se produisent.
- Les modifications suivies vous permettent d'utiliser le PITR (point-in-time restauration) pendant la période de conservation de la sauvegarde continue. Pour exécuter une tâche de restauration, vous choisissez l'instant dans le passé auquel vous souhaitez effectuer la restauration.
- La période de rétention de chaque sauvegarde continue est de 35 jours au maximum.

- Pour les plans de sauvegarde que vous créez via la CLI, les paramètres de sauvegarde avancés pour Amazon S3 (qui incluent la possibilité d'inclure des balises et de les inclure ACLs dans la sauvegarde) sont activés par défaut. Vous pouvez les exclure dans les options de sauvegarde. Voir un [Paramètres de sauvegarde avancés d'Amazon S3](#) exemple de syntaxe.

Sauvegardes périodiques (instantanés) uniquement, planifiées ou à la demande :

- AWS Backup analyse l'intégralité du compartiment S3, récupère l'ACL et les balises de chaque objet, et lance une requête Head pour chaque objet figurant dans le cliché précédent mais introuvable dans le cliché en cours de création.
- La sauvegarde est point-in-time cohérente.
- La date et l'heure de sauvegarde enregistrées correspondent à l'heure à laquelle la traversée du compartiment est AWS Backup terminée, et non à l'heure à laquelle une tâche de sauvegarde a été créée.
- La première sauvegarde d'un compartiment est une sauvegarde complète. Chaque sauvegarde suivante est incrémentielle et représente l'évolution des données depuis le dernier instantané.
- L'instantané créé par la sauvegarde périodique peut avoir une période de rétention allant jusqu'à 99 ans.

Sauvegardes continues associées à periodic/snapshot des sauvegardes :

- Une fois la première sauvegarde complète de vos données existantes (chaque compartiment) terminée, les modifications apportées à votre compartiment sont suivies au fur et à mesure qu'elles se produisent.
- Vous pouvez effectuer une point-in-time restauration à partir d'un point de restauration continu.
- Les instantanés sont point-in-time cohérents.
- Les instantanés sont pris directement depuis le point de récupération continue, ce qui élimine le besoin d'analyser à nouveau un compartiment pour accélérer les processus.
- Les instantanés et les points de récupération continue partagent la même lignée de données ; le stockage des données entre les points de récupération d'instantanés et continue n'est pas dupliqué.
- Lorsque les paramètres de sauvegarde avancés d'Amazon S3, tels que l'inclusion de balises et ACLs le contenu d'une sauvegarde, sont modifiés pour un continuous point AWS Backup de récupération, ce point de récupération est arrêté et en crée un nouveau avec les paramètres mis à jour.

Lorsqu'une tâche de sauvegarde continue est en cours d'exécution pour un compartiment S3, vous pouvez toujours lancer des tâches de sauvegarde périodiques (instantanées). Toutefois, le comportement suivant s'applique :

- Les tâches de sauvegarde instantanée utiliseront les mêmes options de sauvegarde (ACLs et les mêmes paramètres de balises d'objet) que la sauvegarde continue existante.
- Si vous spécifiez pour une tâche de capture d'écran des options de sauvegarde différentes de celles utilisées pour la sauvegarde continue, la tâche de capture d'écran utilisera toujours les paramètres de la sauvegarde continue et se terminera avec le statut « Terminée avec problèmes ».

Lorsque cela se produit, le message d'état suivant s'affiche : "Periodic/snapshot backup for bucket <bucket name> has different backup options than the continuous backup. When using continuous backups along with snapshot backups for the same bucket, the snapshot will use the same settings for backing up ACLs and Object tags as the continuous backup."

Le tableau suivant indique dans quels cas une analyse complète est requise lors de la modification BackupOptions de points de restauration continue existants :

Comportement du scan complet en cas BackupOptions de modification

Précédent BackupOptions	Nouveau BackupOptions	Analyse complète
sauvegarde ACLs et backupObjectTags activation	sauvegarde ACLs et backupObjectTags désactivation	Non
sauvegarde ACLs et backupObjectTags activation	sauvegarde ACLs activée ; backupObjectTags désactivée	Non
sauvegarde ACLs et backupObjectTags activation	sauvegarde ACLs désactivée ; backupObjectTags activée	Non
sauvegarde ACLs et backupObjectTags désactivation	sauvegarde ACLs et backupObjectTags activation	Oui
sauvegarde ACLs activée ; backupObjectTags désactivée	sauvegarde ACLs et backupObjectTags activation	Oui

Précédent BackupOptions	Nouveau BackupOptions	Analyse complète
sauvegarde ACLs désactivée ; backupObjectTags activée	sauvegarde ACLs et backupObjectTags activation	Oui

Fenêtres de fin de sauvegarde S3

Le tableau ci-dessous présente des exemples de compartiments de différentes tailles pour vous aider à estimer le temps d'exécution de la sauvegarde complète initiale d'un compartiment S3. Les durées de sauvegarde varient en fonction de la taille, du contenu, de la configuration et des paramètres de chaque compartiment.

Taille de compartiment	Nombre d'objets	Durée estimée pour terminer la sauvegarde initiale
425 Go (gigaoctets)	135 millions	31 heures
800 To (téraoctets)	670 millions	38 heures
6 Po (pétaoctets)	5 milliards	100 heures
370 To (téraoctets)	7,5 milliards	180 heures

Bonnes pratiques et considérations financières pour les sauvegardes S3

Meilleures pratiques en matière de seaux de grande taille

Pour les compartiments contenant plus de 300 millions d'objets :

- Pour les compartiments contenant plus de 300 millions d'objets, le taux de sauvegarde peut atteindre 17 000 objets par seconde lors de la sauvegarde complète initiale du compartiment (les sauvegardes incrémentielles auront une vitesse différente) ; les compartiments contenant moins de 300 millions d'objets sont sauvegardés à un rythme proche de 1 000 objets par seconde.
- Des sauvegardes continues sont recommandées.
- Si le cycle de vie des sauvegardes est prévu pour plus de 35 jours, vous pouvez également activer les sauvegardes d'instantanés pour le compartiment dans le même coffre-fort dans lequel vos sauvegardes continues sont stockées.

Optimisation de la stratégie de sauvegarde

- Pour les comptes qui effectuent des sauvegardes au moins une fois par jour ou plus fréquemment, il est possible de réaliser des économies en utilisant des sauvegardes continues si les données contenues dans les sauvegardes subissent des modifications minimales entre chaque sauvegarde.
- Les compartiments plus volumineux qui ne changent pas fréquemment peuvent tirer parti des sauvegardes continues, car cela peut se traduire par une réduction des coûts lorsque les analyses de l'ensemble du compartiment ainsi que plusieurs demandes par objet n'ont pas besoin d'être exécutées sur des objets préexistants (objets inchangés par rapport à la sauvegarde précédente).
- Les compartiments contenant plus de 100 millions d'objets et dont le taux de suppression est faible par rapport à la taille globale de la sauvegarde peuvent réaliser des économies grâce à un plan de sauvegarde qui inclut à la fois une sauvegarde continue avec une période de rétention de 2 jours et des instantanés d'une rétention plus longue.
- La durée des sauvegardes périodiques (instantanés) coïncide avec le début du processus de sauvegarde lorsqu'une analyse des compartiments n'est pas nécessaire. Les analyses ne sont pas nécessaires dans un compartiment contenant à la fois une sauvegarde continue et des instantanés, car dans ces cas, les instantanés sont pris à partir d'un point de récupération continue.

Cycle de vie des objets et marqueurs de suppression

- Les politiques de cycle de vie S3 comportent une fonctionnalité optionnelle appelée Supprimer les marqueurs de suppression d'objet arrivés à expiration. Lorsque cette fonctionnalité est supprimée, les marqueurs de suppression, parfois par millions, expirent sans plan de nettoyage. Lorsque des compartiments dépourvus de cette fonctionnalité sont sauvegardés, deux problèmes ont un impact sur le temps et les coûts :
 - Les marqueurs de suppression sont sauvegardés, tout comme les objets. Le temps de sauvegarde et le temps de restauration peuvent être attribués en fonction du rapport entre les objets et les marqueurs de suppression.
 - Chaque objet ou marqueur sauvegardé est soumis à des frais minimum. Chaque marqueur de suppression est facturé de la même manière qu'un objet de 128 Ko.

Considérations relatives aux coûts des classes de stockage

- Pour chaque objet d'un seul S3-GIR (Amazon S3 Glacier Instant Retrieval), il AWS Backup effectue plusieurs appels, ce qui entraîne des frais de récupération lors de l'exécution d'une sauvegarde.

Des coûts de récupération similaires s'appliquent aux compartiments contenant des objets des classes de stockage S3-IA et S3 One Zone-IA.

AWS optimisation des coûts de service

- L'utilisation des fonctionnalités d' AWS KMS Amazon CloudWatch et d'Amazon dans GuardDuty le cadre de votre stratégie de sauvegarde peut entraîner des coûts supplémentaires au-delà du stockage des données du compartiment S3. CloudTrail Consultez les sections suivantes pour en savoir plus sur ces fonctionnalités :
- [Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3](#) dans le Guide de l'utilisateur Amazon S3.
- Vous pouvez réduire les CloudTrail coûts en excluant les AWS KMS événements et en désactivant les événements de données S3 :
 - Exclure AWS KMS des événements : dans le guide de CloudTrail l'utilisateur, [la création d'un parcours dans la console \(sélecteurs d'événements de base\)](#) permet d'exclure AWS KMS des événements afin de les exclure de votre suivi (le paramètre par défaut inclut tous les événements KMS) :
 - L'option de journalisation ou d'exclusion des événements KMS n'est disponible que si vous journalisez les événements de gestion sur votre journal de suivi. Si vous choisissez de ne pas journaliser les événements de gestion, les événements KMS ne sont pas journalisés, et vous ne pouvez pas modifier les paramètres de journalisation des événements KMS.
 - AWS KMS des actions telles que EncryptDecrypt, et génèrent GenerateDataKey généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les actions KMS pertinentes de faible volume, telles que Disable, Delete et ScheduleKey (qui comptent généralement moins de 0,5 % du volume des événements KMS) sont journalisées en tant qu'événements Écrire.
 - Pour exclure les événements de volume important tels que Encrypt, Decrypt et GenerateDataKey, tout en continuant de journaliser les événements pertinents tels que Disable, Delete et ScheduleKey, choisissez de journaliser les événements de gestion Écrire et effacez la case à cocher pour Exclure les événements AWS KMS .
 - Désactiver les événements de données S3 : par défaut, les journaux de suivi et les stockages de données d'événement ne journalisent pas les événements de données. Désactivez les événements de données S3 avant votre sauvegarde initiale afin de réduire les coûts.

- Pour réduire les CloudWatch coûts, vous pouvez arrêter d'envoyer CloudTrail des événements aux CloudWatch journaux lorsque vous mettez à jour un journal pour désactiver les paramètres CloudWatch des journaux.
- [Estimation GuardDuty du coût d'utilisation](#) dans le guide de GuardDuty l'utilisateur Amazon.

Messages de sauvegarde S3

Lorsqu'une tâche de sauvegarde se termine ou échoue, le message suivant peut s'afficher. Le tableau suivant peut vous aider à déterminer la cause possible du message d'état.

Scénario	Statut de la tâche	Message	Exemple
Tous les objets n'ont pas pu être sauvegardés pour un instantané ou une sauvegarde continue initiale	FAILED	« Aucun objet n'a été sauvegardé depuis le compartiment source <i>BucketName</i> . Pour être informé de ces défaillances, activez les notifications d'événements SNS. »	Le rôle Backup n'est pas autorisé à obtenir l'ACL de version de l'objet. Par conséquent, aucun des objets n'est sauvegardé.
Tous les objets n'ont pas pu être sauvegardés pour une sauvegarde continue ultérieure.	COMPLETED	« Aucun objet n'a été sauvegardé depuis le compartiment source <i>BucketName</i> . Pour être informé de ces défaillances, activez les notifications d'événements SNS. »	

Paramètres de sauvegarde avancés d'Amazon S3

AWS Backup fournit des paramètres avancés pour contrôler les métadonnées incluses dans vos sauvegardes Amazon S3. Vous pouvez éventuellement exclure les listes de contrôle d'accès (ACLs)

et les balises d'objets, ce qui peut être utile si vos objets sont configurés sans balises ACLs d'objet. En d'autres termes, si vous n'utilisez pas de balises ACLs ou d'objets pour vos ressources S3, il peut être avantageux de les exclure de vos sauvegardes.

Configuration de la sauvegarde des balises ACLs et des balises d'objet

Vous pouvez configurer les options de sauvegarde des ACL et des balises d'objet via la AWS Backup console ou via le AWS CLI.

Console

Configurer les options d'ACL et de balise à l'aide de la console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup/>.
2. Dans le volet de navigation, choisissez Backup plans, puis Create backup plan.
3. Dans les paramètres de votre plan de sauvegarde, développez les paramètres de sauvegarde avancés.
4. Pour les ressources Amazon S3, configurez les options suivantes :
 - Sauvegarder ACLs : cochez la case pour les inclure ACLs ou ne la cochez pas pour les exclure.

Backup up object tags : cochez la case pour inclure les tags d'objet dans votre sauvegarde.

5. Terminez la configuration du plan de sauvegarde et choisissez Créer un plan.

AWS CLI

Vous pouvez inclure ou exclure de manière sélective des listes de contrôle d'accès (ACLs) et des balises d'objets de vos sauvegardes Amazon S3 à l'aide des options de sauvegarde suivantes :

Backup ACLs

Contrôle si ACLs les objets sont inclus dans la sauvegarde. Définissez sur `disabled` pour exclure ACLs. Par défaut : `enabled`

BackupObjectTags

Contrôle si les balises d'objet sont incluses dans la sauvegarde. Définissez sur `disabled` pour exclure les balises. Par défaut : `enabled`

Configurez les options d'ACL et de balise à l'aide du AWS CLI

Pour configurer les options de sauvegarde des ACL et des balises d'objet à l'aide de AWS CLI, utilisez la `update-backup-plan` commande avec des paramètres de sauvegarde avancés :

```
aws backup update-backup-plan \
  --backup-plan-id "your-backup-plan-id" \
  --backup-plan '{
    "BackupPlanName": "MyS3BackupPlan",
    "Rules": [{
      "RuleName": "MyS3BackupRule",
      "TargetBackupVaultName": "MyBackupVault",
      "ScheduleExpression": "cron(0 2 ? * * *)",
      "Lifecycle": {
        "DeleteAfterDays": 30
      },
      "RecoveryPointTags": {},
      "CopyActions": [],
      "EnableContinuousBackup": false
    }],
    "AdvancedBackupSettings": [{
      "ResourceType": "S3",
      "BackupOptions": {
        "BackupACLs": "disabled",
        "BackupObjectTags": "disabled"
      }
    }
  ]
}'
```

Les `BackupOptions` paramètres contrôlent l'inclusion des métadonnées :

- `"BackupACLs": "disabled"`- Exclut ACLs des sauvegardes
- `"BackupObjectTags": "disabled"`- Exclut les balises d'objet des sauvegardes
- `"BackupACLs": "enabled"`- Inclus ACLs dans les sauvegardes (par défaut)
- `"BackupObjectTags": "enabled"`- Inclut des balises d'objet dans les sauvegardes (par défaut)

Sauvegardes Amazon Timestream

Amazon Timestream est une base de données de séries temporelles évolutive qui permet de stocker et d'analyser plusieurs milliards de points de données de séries temporelles par jour. Timestream est optimisé pour économiser du temps et des coûts en conservant les données récentes en mémoire et en stockant les données historiques dans un niveau de stockage optimisé en termes de coûts conformément à vos politiques.

Une base de données Timestream contient des tables. Ces tables contiennent des enregistrements et chaque enregistrement est un point de données unique dans une série temporelle. Une série chronologique est une séquence d'enregistrements enregistrés sur un intervalle de temps, tel que le cours d'une action, le niveau d'utilisation de la mémoire d'une EC2 instance Amazon ou un relevé de température. AWS Backup peut sauvegarder et restaurer de manière centralisée les tables Timestream. Vous pouvez copier ces sauvegardes de tables sur d'autres comptes et sur plusieurs autres comptes Régions AWS au sein de la même organisation.

Timestream ne propose pas actuellement de services de sauvegarde et de restauration natifs. Le fait de AWS Backup créer des copies sécurisées de vos tables Timestream peut donc ajouter une couche supplémentaire de sécurité et de résilience à vos ressources.

Sauvegarde des tables Timestream

Vous pouvez sauvegarder les tables Timestream via la AWS Backup console ou à l'aide du. AWS CLI

Il existe deux manières d'utiliser la AWS Backup console pour sauvegarder une table Timestream : à la demande ou dans le cadre d'un plan de sauvegarde.

Création de sauvegardes Timestream à la demande

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. À l'aide du volet de navigation, choisissez Ressources protégées, puis Créer une sauvegarde à la demande.
3. Sur la page Créer une sauvegarde à la demande, choisissez Amazon Timestream.
4. Choisissez le Type de ressource Timestream, puis le nom de la table que vous souhaitez sauvegarder.
5. Dans la fenêtre Sauvegarde, assurez-vous que Créer le backup maintenant est sélectionné. Une sauvegarde est immédiatement lancée et votre cluster s'affiche plus tôt sur la page Ressources protégées.

6. Dans le menu déroulant Transition vers le stockage à froid, vous pouvez définir vos paramètres de transition.
7. Dans Période de rétention, vous pouvez choisir la durée de rétention de votre sauvegarde.
8. Choisissez un coffre-fort de sauvegarde existant ou créez-en un. Si vous choisissez Créer un coffre de sauvegarde, une nouvelle page s'ouvre afin que vous puissiez créer un coffre. Une fois que vous avez terminé, vous revenez à la page Créer une sauvegarde à la demande.
9. Sous Rôle IAM, choisissez Rôle par défaut (si le rôle AWS Backup par défaut n'est pas présent dans votre compte, il sera créé pour vous avec les autorisations appropriées).
10. (Facultatif) Des balises peuvent être ajoutées à votre point de récupération. Si vous souhaitez affecter une ou plusieurs balises à votre sauvegarde à la demande, entrez une clé et une valeur facultative, puis choisissez Add tag (Ajouter une balise).
11. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Vous accédez ainsi à la page Jobs (Tâches), où vous pouvez consulter une liste des tâches.
12. Choisissez l'ID de tâche de backup du cluster pour voir les détails de cette tâche. Il affichera un statut Completed, In Progress ou Failed. Vous pouvez cliquer sur le bouton Actualiser pour mettre à jour le statut.

Création de sauvegardes Timestream planifiées dans un plan de sauvegarde

Vos sauvegardes planifiées peuvent inclure des tables Timestream s'il s'agit d'une ressource protégée. Pour activer la protection des tables Amazon Timestream :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées.
3. Activez Amazon Timestream.
4. Consultez [Attribution de ressources à la console](#) pour inclure des tables Timestream dans un plan existant ou nouveau.

Sous Gérer les plans de backup, vous pouvez choisir de [créer un plan de sauvegarde](#) et d'inclure des tables Timestream, ou vous pouvez [mettre à jour un plan existant](#) pour inclure des tables Timestream. Lorsque vous ajoutez le type de ressource Timestream, vous pouvez choisir d'ajouter Toutes les tables Timestream ou de cocher les cases à côté des tables que vous souhaitez ajouter sous Sélectionner des types de ressources spécifiques.

La première sauvegarde des tables Timestream sera une sauvegarde complète. Les sauvegardes suivantes seront des sauvegardes incrémentielles.

Après avoir créé ou modifié votre plan de sauvegarde, accédez à Plans de sauvegarde dans le volet de navigation de gauche. Le plan de sauvegarde que vous avez spécifié doit afficher vos clusters sous Attributions de ressources.

Sauvegarde par programmation

Vous pouvez utiliser le nom d'opération `start-backup-job`. Incluez les paramètres suivants :

```
aws backup start-backup-job \  
--backup-vault-name backup-vault-name \  
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \  
--iam-role-arn arn:aws:iam::account:role/role-name \  
--region Région AWS \  
--endpoint-url URL
```

Affichage des sauvegardes des tables Timestream

Pour afficher et modifier les sauvegardes de vos tables Timestream dans la console, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Choisissez Coffres-forts de sauvegarde. Cliquez ensuite sur le nom du coffre-fort de sauvegarde qui contient vos tables Timestream.
3. Le coffre-fort de sauvegarde affichera un résumé et une liste des sauvegardes.
 - a. Vous pouvez cliquer sur le lien dans la colonne ID du point de récupération, ou
 - b. Vous pouvez cocher la case située à gauche de l'ID du point de récupération et cliquer sur Actions pour supprimer les points de récupération dont vous n'avez plus besoin.

Restauration d'une table Timestream

Découvrez comment [restaurer une table Timestream](#).

Sauvegardes de machines virtuelles

AWS Backup prend en charge la protection des données centralisée et automatisée pour les machines VMware virtuelles sur site (VMs) ainsi que VMs dans le VMware Cloud™ (VMC) activé AWS et le VMware Cloud™ (VMC) activé. AWS Outposts Vous pouvez effectuer des sauvegardes depuis vos machines virtuelles sur site et VMC vers. AWS Backup Vous pouvez ensuite effectuer une restauration sur site VMs, VMs dans la VMC ou dans la VMC activée. AWS Backup AWS Outposts

AWS Backup vous fournit également des fonctionnalités AWS natives de gestion des sauvegardes de machines virtuelles entièrement gérées, telles que la découverte des machines virtuelles, la planification des sauvegardes, la gestion de la rétention, un niveau de stockage peu coûteux, la copie entre régions et entre comptes, la prise en charge de AWS Backup Vault Lock et d' AWS Backup Audit Manager, un chiffrement indépendant des données sources et des politiques d'accès aux sauvegardes. Pour obtenir une liste complète des fonctionnalités et des détails, consultez le tableau [Disponibilité des fonctionnalités par ressource](#).

Vous pouvez l'utiliser AWS Backup pour protéger vos machines virtuelles sur [VMware Cloud™ on AWS Outposts](#). AWS Backup stocke les sauvegardes de vos machines virtuelles dans le site Région AWS auquel votre VMware Cloud™ on AWS Outposts est connecté. Vous pouvez l'utiliser AWS Backup pour protéger votre VMware Cloud™ AWS Backup VMs lorsque vous utilisez VMware Cloud™ AWS Outposts pour répondre à vos besoins en matière de faible latence et de traitement local des données de vos applications. En fonction de vos exigences en matière de résidence des données, vous pouvez AWS Backup choisir de stocker des sauvegardes des données de votre application dans le parent Région AWS auquel vous AWS Outposts êtes connecté.

Soutenu VMs

AWS Backup peut sauvegarder et restaurer des machines virtuelles gérées par un VMware vCenter.

Actuellement pris en charge :

- vSphere 8, 7.0 et 6.7
- Tailles de disque virtuel multiples de 1 KiB
- Banques de données NFS, VMFS et VSAN sur site et dans VMC sur AWS
- Modes de transport SCSI Hot-Add et NBDSSL (Network Block Device Secure Sockets Layer) pour copier des données de la source vers des applications sur site VMs AWS VMware
- Mode Hot-Add pour protéger VMs sur VMware Cloud on AWS

Non pris en charge actuellement :

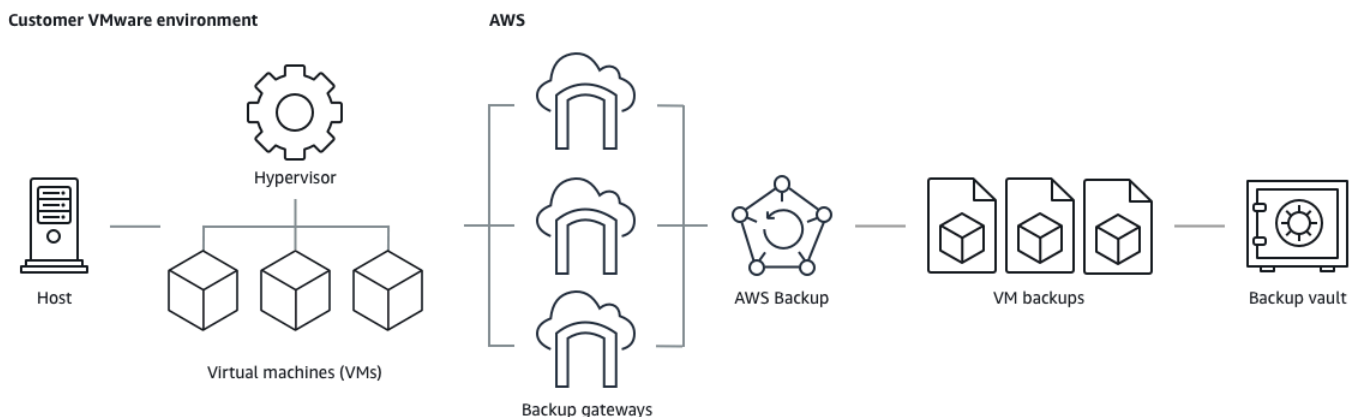
- Disques ou NVMe contrôleurs RDM (mappage de disque brut) et leurs disques
- Modes de disque indépendants persistants et indépendants non persistants

Cohérence de sauvegarde

AWS Backup, par défaut, capture les sauvegardes cohérentes avec les applications VMs en utilisant le paramètre de repos VMware des outils sur la machine virtuelle. Vos sauvegardes sont cohérentes avec les applications si celles-ci sont compatibles avec VMware Tools. Si la fonctionnalité de mise au repos n'est pas disponible, AWS Backup capture les sauvegardes cohérentes en cas de crash. Vérifiez que vos sauvegardes répondent aux besoins de votre entreprise en testant vos restaurations.

Backup gateway

Backup Gateway est AWS Backup un logiciel téléchargeable que vous déployez sur votre VMware infrastructure pour vous y VMware VMs connecter AWS Backup. La passerelle se connecte à votre serveur de gestion de machines virtuelles pour découvrir VMs, découvrir vos données VMs, chiffrer les données et les transférer efficacement vers. AWS Backup Le schéma suivant illustre la manière dont la passerelle Backup se connecte à votre VMs :



Pour télécharger le logiciel Backup Gateway, suivez la procédure pour [Utilisation des passerelles](#).

Télécharger le logiciel VM

La passerelle de sauvegarde est distribuée sous la forme d'un modèle OVF (Open Virtualization Format) que vous déployez sur votre VMware infrastructure. Le logiciel de passerelle vous connecte

VMware VMs à AWS Backup en découvrant VMs, en cryptant les données et en les transférant efficacement vers. AWS Backup

Pour obtenir le modèle OVF, utilisez la AWS Backup console :

1. Connectez-vous à la console de AWS gestion et ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, sous Ressources externes, sélectionnez Gateways.
3. Cliquez sur Create gateway (Créer une passerelle).
4. Dans la section Configurer la passerelle, téléchargez le modèle OVF et déployez-le VMware dans votre environnement.

[Pour plus d'informations sur les points de terminaison VPC \(Virtual Private Cloud\), consultez AWS Backup la section et connectivité. AWS PrivateLink](#)

Backup gateway est doté de sa propre API, qui est gérée séparément de l'API AWS Backup . Pour consulter la liste des actions de l'API Backup gateway, consultez [Actions de Backup gateway](#). Pour consulter la liste des types de données de l'API Backup gateway, consultez [Types de données Backup gateway](#).

Points de terminaison

Les utilisateurs existants qui utilisent actuellement un point de terminaison public et qui souhaitent passer à un point de terminaison d'un VPC (cloud privé virtuel) peuvent [créer une nouvelle passerelle avec un point de terminaison d'un VPC](#) en utilisant [AWS PrivateLink](#), associer l'hyperviseur existant à la passerelle, puis [supprimer la passerelle](#) contenant le point de terminaison public.

Configuration de votre infrastructure pour utiliser Backup gateway

Backup gateway nécessite les configurations réseau, de pare-feu et matérielles suivantes pour sauvegarder et restaurer vos machines virtuelles.

Configuration réseau

Backup gateway requiert que certains ports soient autorisés pour fonctionner. Autorisez les ports suivants :

1. TCP 443 sortant
 - Source : Backup gateway

- Destination : AWS
- Utilisation : autorise la passerelle Backup à communiquer avec AWS.

2. TCP 80 entrant

- Source : L'hôte que vous utilisez pour vous connecter au AWS Management Console
- Destination : Backup gateway
- Utilisation : par les systèmes locaux pour obtenir la clé d'activation Backup gateway. Le port 80 n'est utilisé que lors de l'activation de la passerelle Backup. AWS Backup ne nécessite pas que le port 80 soit accessible au public. Le niveau requis de l'accès au port 80 dépend de la configuration de votre réseau. Si vous activez votre passerelle depuis le AWS Management Console, l'hôte à partir duquel vous vous connectez à la console doit avoir accès au port 80 de votre passerelle.

3. UDP 53 sortant

- Source : Backup gateway
- Destination : serveur DNS (Domain Name Service)
- Utilisation : autorise Backup gateway à communiquer avec le DNS.

4. TCP 22 sortant

- Source : Backup gateway
- Destination : Support
- Utilisation : Permet d'accéder Support à votre passerelle pour vous aider à résoudre les problèmes. Il n'est pas nécessaire que ce port soit ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les problèmes.

5. UDP 123 sortant

- Source : client NTP
- Destination : serveur NTP
- Utilisation : par les systèmes locaux pour synchroniser l'heure de la machine virtuelle et celle de l'hôte.

6. TCP 443 sortant

- Source : Backup gateway
- Destination : VMware vCenter
- Utilisation : autorise la passerelle Backup à communiquer avec VMware vCenter.

7. TCP 443 sortant

- Source : Backup gateway

- Destination : ESXi hôtes
- Utilisation : autorise la passerelle Backup à communiquer avec les ESXi hôtes.

8. TCP 902 sortant

- Source : Backup gateway
- Destination : VMware ESXi hôtes
- Utilisation : pour le transfert de données via Backup gateway.

Les ports ci-dessus sont nécessaires pour la passerelle Backup. Consultez [Créer un point de terminaison VPC](#) pour plus d'informations sur la façon de configurer les points de terminaison Amazon VPC pour AWS Backup.

Configuration de pare-feu

La passerelle de sauvegarde nécessite l'accès aux points de terminaison de service suivants pour communiquer avec Amazon Web Services. Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, vous devez les configurer afin de permettre les communications sortantes vers AWS pour ces points de terminaison de service. L'utilisation d'un proxy HTTP entre Backup gateway et les points de service n'est pas prise en charge.

Types de terminaux

Points de terminaison standard : Support IPv4 du trafic entre votre appliance de passerelle et AWS.

Les points de terminaison de service suivants sont requis par toutes les passerelles pour les opérations de chemin de contrôle (anon-cp, client-cp, proxy-app) et de chemin de données (dp-1).

```
anon-cp.backup-gateway.region.amazonaws.com:443
client-cp.backup-gateway.region.amazonaws.com:443
proxy-app.backup-gateway.region.amazonaws.com:443
dp-1.backup-gateway.region.amazonaws.com:443
```

Points de terminaison à double pile : Support à la fois IPv6 du trafic entre votre appliance de passerelle IPv4 et AWS.

Les points de terminaison de service à double pile suivants sont requis par toutes les passerelles pour les opérations de chemin de contrôle (activation, plan de contrôle, proxy) et de chemin de données (plan de données).

```
activation-backup-gateway.region.api.aws:443
controlplane-backup-gateway.region.api.aws:443
proxy-backup-gateway.region.api.aws:443
dataplane-backup-gateway.region.api.aws:443
```

Configurez votre passerelle pour plusieurs NICs entrées VMware

Vous pouvez gérer des réseaux distincts pour votre trafic interne et externe en associant plusieurs connexions d'interface réseau virtuelle (NICs) à votre passerelle, puis en dirigeant le trafic interne (passerelle vers l'hyperviseur) et le trafic externe (passerelle vers AWS) séparément.

Par défaut, les machines virtuelles connectées à la AWS Backup passerelle disposent d'un adaptateur réseau (eth0). Ce réseau inclut l'hyperviseur, les machines virtuelles et la passerelle réseau (passerelle de sauvegarde) qui communique avec l'Internet au sens large.

Voici un exemple de configuration avec plusieurs interfaces réseau virtuelles :

```
eth0:
- IP: 10.0.3.83
- routes: 10.0.3.0/24

eth1:
- IP: 10.0.0.241
- routes: 10.0.0.0/24
- default gateway: 10.0.0.1
```

- Dans cet exemple, la connexion est à un hyperviseur avec l'adresse IP 10.0.3.123, la passerelle utilisera eth0, car l'adresse IP de l'hyperviseur fait partie du bloc 10.0.3.0/24.
- Pour se connecter à un hyperviseur via l'adresse IP 10.0.0.234, la passerelle utilisera eth1.
- Pour se connecter à une adresse IP en dehors des réseaux locaux (par exemple 34.193.121.211), la passerelle reviendra à la passerelle par défaut 10.0.0.1, qui se trouve dans le bloc 10.0.0.0/24 et passera donc par eth1.

La première séquence d'ajout d'un adaptateur réseau supplémentaire se produit dans le client vSphere :

1. Dans le client VMware vSphere, ouvrez le menu contextuel (avec un clic droit) de votre machine virtuelle de passerelle, puis choisissez Modifier les paramètres.

2. Dans l'onglet Matériel virtuel de la boîte de dialogue Propriétés de la machine virtuelle, ouvrez le menu Ajouter un nouvel appareil et sélectionnez Adaptateur réseau pour ajouter un nouvel adaptateur réseau.
3.
 - a. Développez les détails du Nouveau réseau pour configurer le nouvel adaptateur.
 - b. Assurez-vous que l'option Se connecter lors de la mise sous tension est sélectionnée.
 - c. Pour le type d'adaptateur, reportez-vous à la section Types d'adaptateur réseau dans la documentation de vCenter Server [ESXi et de vCenter Server](#).
4. Cliquez sur OK pour enregistrer les nouveaux paramètres de l'adaptateur réseau.

La séquence d'étapes suivante pour configurer un adaptateur supplémentaire s'effectue dans la console de AWS Backup passerelle (notez qu'il ne s'agit pas de la même interface que la console de AWS gestion dans laquelle les sauvegardes et les autres services sont gérés).

Une fois que la nouvelle NIC est ajoutée à la machine virtuelle de la passerelle, vous devez

- Accéder à Command Prompt et activer les nouveaux adaptateurs
- Configuration statique IPs pour chaque nouvelle carte réseau
- Définir la NIC préférée comme votre choix par défaut

Pour cela :

1. Dans le client VMware vSphere, sélectionnez la machine virtuelle de votre passerelle et lancez la console Web pour accéder à la console locale Backup Gateway.
 - Pour plus d'informations sur l'accès à une console locale, voir [Accès à la console locale Gateway avec VMware ESXi](#)
2. Quittez l'invite de commande et accédez à Configuration réseau > Configurer l'adresse IP statique et suivez les instructions de configuration pour mettre à jour la table de routage.
 - a. Attribuez une adresse IP statique dans le sous-réseau de l'adaptateur réseau.
 - b. Définissez un masque réseau.
 - c. Entrez l'adresse IP de la passerelle par défaut. Il s'agit de la passerelle réseau qui se connecte à tout le trafic en dehors du réseau local.
3. Sélectionnez Définir l'adaptateur par défaut pour désigner l'adaptateur qui sera connecté au cloud comme appareil par défaut.

4. Toutes les adresses IP de la passerelle peuvent être affichées à la fois dans la console locale et sur la page de résumé de la machine virtuelle dans VMware vSphere.

VMware autorisations

Cette section répertorie les VMware autorisations minimales requises pour l'utiliser AWS Backup gateway. Ces autorisations sont nécessaires pour que Backup gateway puisse découvrir, sauvegarder et restaurer des machines virtuelles.

Pour utiliser la passerelle Backup avec VMware Cloud™ activé AWS ou VMware Cloud™ activé AWS Outposts, vous devez utiliser l'utilisateur administrateur par défaut `cloudadmin@vmc.local` ou attribuer le CloudAdmin rôle à votre utilisateur dédié.

Pour utiliser la passerelle Backup VMware avec des machines virtuelles locales, créez un utilisateur dédié doté des autorisations répertoriées ci-dessous.

Globale

- Désactiver les méthodes
- Activer les méthodes
- Licences
- Journaliser les événements
- Gérer les attributs personnalisés
- Définir les attributs personnalisés

Balisage vSphere

- Attribuer ou annuler l'attribution d'une balise vSphere

DataStore

- Allouer de l'espace
- Consulter l'entrepôt de données
- Configurer l'entrepôt de données (pour un entrepôt de données vSAN)
- Opérations de fichiers de bas niveau
- Mettre à jour les fichiers des machines virtuelles

Host (Hôte)

- Configuration
 - Réglages avancés
 - Configuration des partitions de stockage

Dossier

- Créer un dossier

Réseau

- Attribuer un réseau

Groupe dvPort

- Créer
- Suppression

Ressource

- Attribuer une machine virtuelle au groupe de ressources

Machine virtuelle

- Modification de la configuration
 - Obtenir un contrat de location disque
 - Ajouter un disque existant
 - Ajouter un nouveau disque
 - Configuration avancée
 - Modifier les paramètres de l'
 - Configurer l'appareil brut
 - Modifier les paramètres de l'appareil
 - Supprimer le disque

- Définir une annotation
- Activer/désactiver le suivi des modifications du disque
- Modifier l'inventaire
 - Créer à partir d'un existant
 - Créer un nouveau
 - Enregistrement
 - Supprimer
 - Annuler l'enregistrement
- Interaction
 - Éteindre
 - Allumer
- Allouer
 - Autoriser l'accès disque
 - Autoriser l'accès disque en lecture seule
 - Autoriser le téléchargement de la machine virtuelle
- Gestion des instantanés
 - Créer un instantané
 - Supprimer un instantané
 - Revenir à un instantané

Utilisation des passerelles

Pour sauvegarder et restaurer vos machines virtuelles (VMs) à l'aide de AWS Backup, vous devez d'abord installer une passerelle de sauvegarde. Une passerelle est un logiciel sous la forme d'un modèle OVF (Open Virtualization Format) qui connecte Amazon Web Services Backup à votre hyperviseur, ce qui lui permet de détecter automatiquement vos machines virtuelles et de vous permettre de les sauvegarder et de les restaurer.

Une passerelle unique peut exécuter jusqu'à 4 tâches de sauvegarde ou de restauration à la fois. Pour exécuter plus de 4 tâches à la fois, créez d'autres passerelles et associez-les à votre hyperviseur.

Création d'une passerelle

Vous pouvez créer une passerelle de sauvegarde en utilisant deux approches :

- Méthode console (standard) : crée des passerelles IPv4 uniquement via la AWS Backup console avec activation automatique
- Méthode manuelle : prend en charge les deux IPv4 , IPv6 en obtenant des clés d'activation et en utilisant AWS CLI des commandes

Les deux méthodes nécessitent d'abord de télécharger et de déployer le modèle OVF (voir [Télécharger le logiciel VM](#)).

Méthode console (IPv4 uniquement)

Utilisez cette méthode pour créer une IPv4 passerelle standard via la AWS Backup console avec activation automatique.

Pour créer une passerelle NAT :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Passerelles.
3. Cliquez sur Create gateway (Créer une passerelle).
4. Dans la section Configurer une passerelle, suivez ces instructions pour télécharger et déployer le modèle OVF.

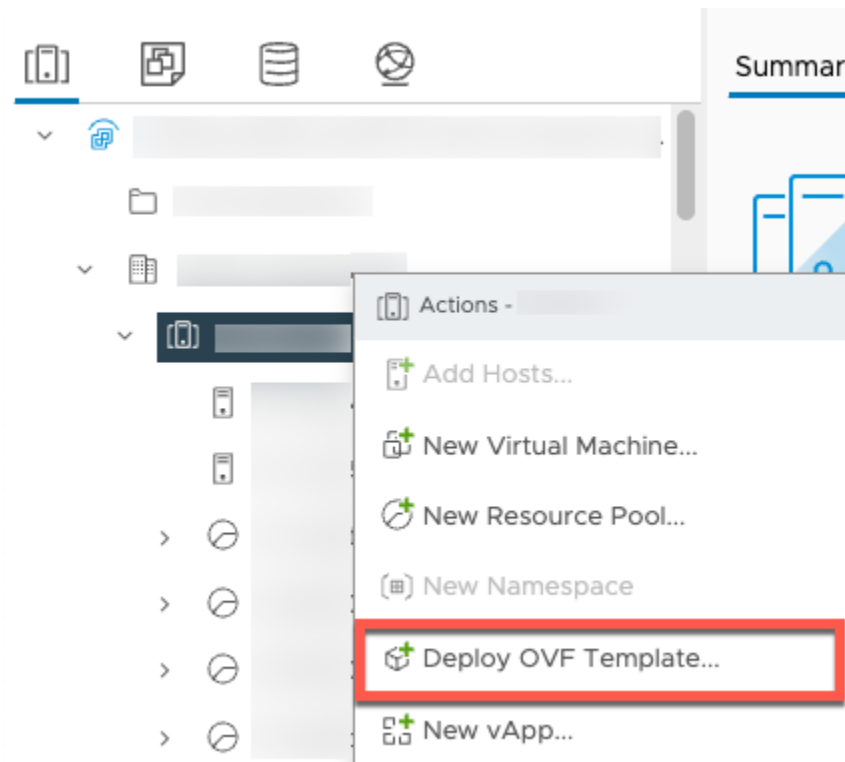
Téléchargement de VMware logiciels

Connexion de l'hyperviseur

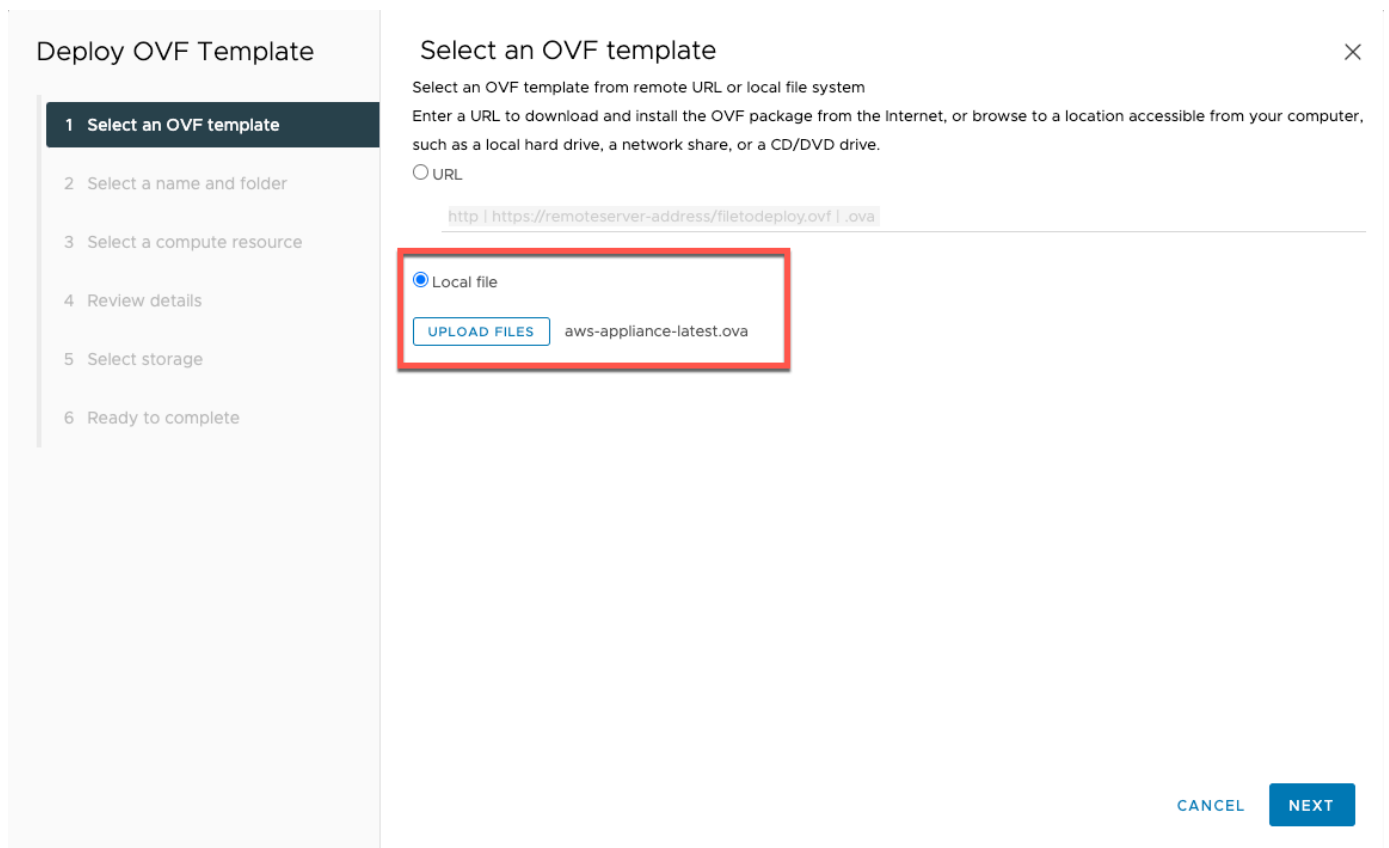
Les passerelles se connectent AWS Backup à votre hyperviseur afin que vous puissiez créer et stocker des sauvegardes de vos machines virtuelles. Pour configurer votre passerelle VMware ESXi, téléchargez le [modèle OVF](#). Le téléchargement peut prendre environ 10 minutes.

Une fois l'opération terminée, procédez comme suit :

1. Connectez-vous à l'hyperviseur de votre machine virtuelle à l'aide de VMware vSphere.
2. Cliquez avec le bouton droit sur un objet parent d'une machine virtuelle et sélectionnez Déployer le modèle OVF.



3. Choisissez Fichier local, puis chargez le fichier `aws-appliance-latest.ova` que vous avez téléchargé.



4. Suivez les étapes de l'assistant de déploiement pour le déployer. Sur la page Sélectionner le stockage, sélectionnez le format de disque virtuel Thick Provision Lazy Zeroed.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Ready to complete

Select storage

Select the storage for the configuration and disk files

Select virtual disk format

VM Storage Policy

☐ Disable Storage DRS for this storage

Thick Provision Lazy Zeroed

Thin Provision

Thick Provision Eager Zeroed

Default

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Placement
☐	vsanDatastore	--	20.74 TB	8.72 TB	13.37 TB	vSAN	Local
☐	WorkloadDatasto...	--	20.74 TB	67.44 TB	13.37 TB	vSAN	Local

2 Items

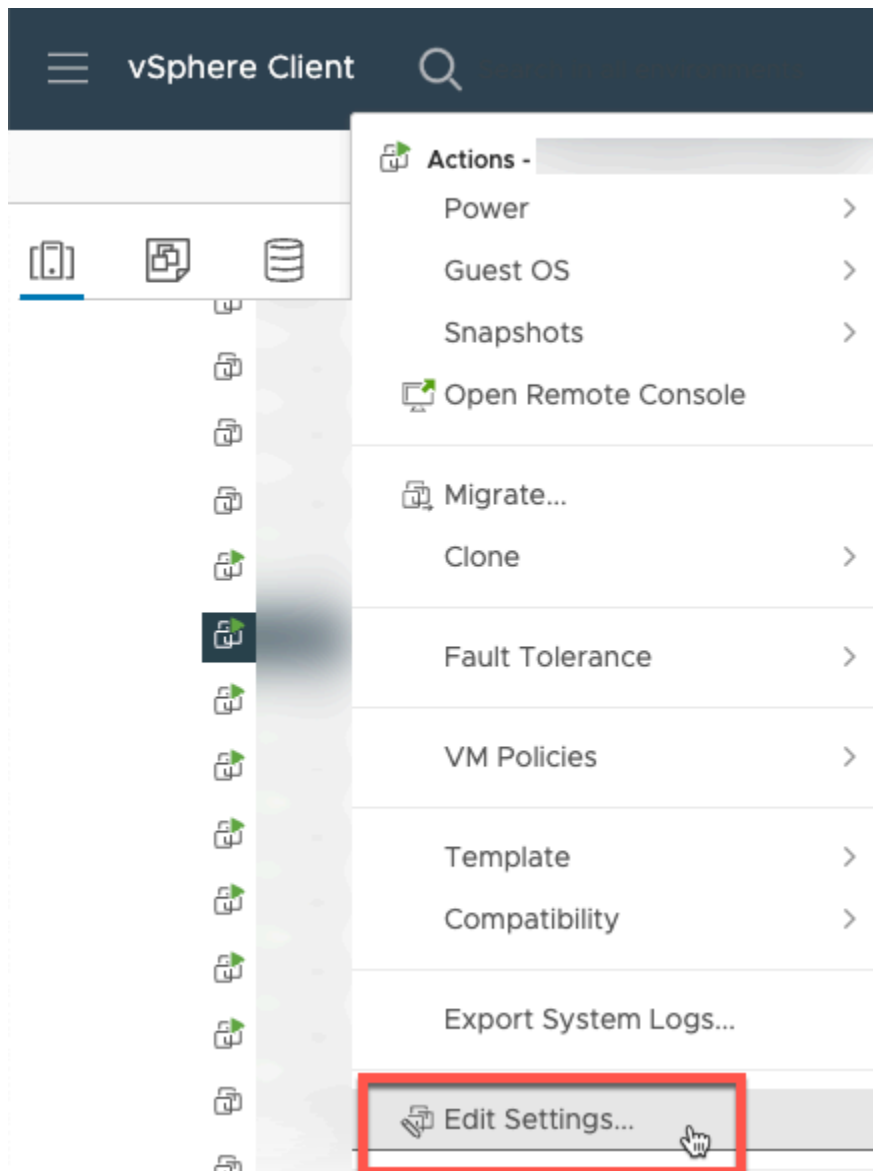
Compatibility

CANCEL

BACK

NEXT

5. Après avoir déployé l'OVF, cliquez avec le bouton droit sur la passerelle et choisissez Modifier les paramètres.



- a. Sous Options de machine virtuelle, accédez à Outils de machine virtuelle.
- b. Assurez-vous que pour Synchroniser l'heure avec l'hôte, l'option Synchroniser au démarrage et à la reprise est sélectionnée.

Edit Settings ✕

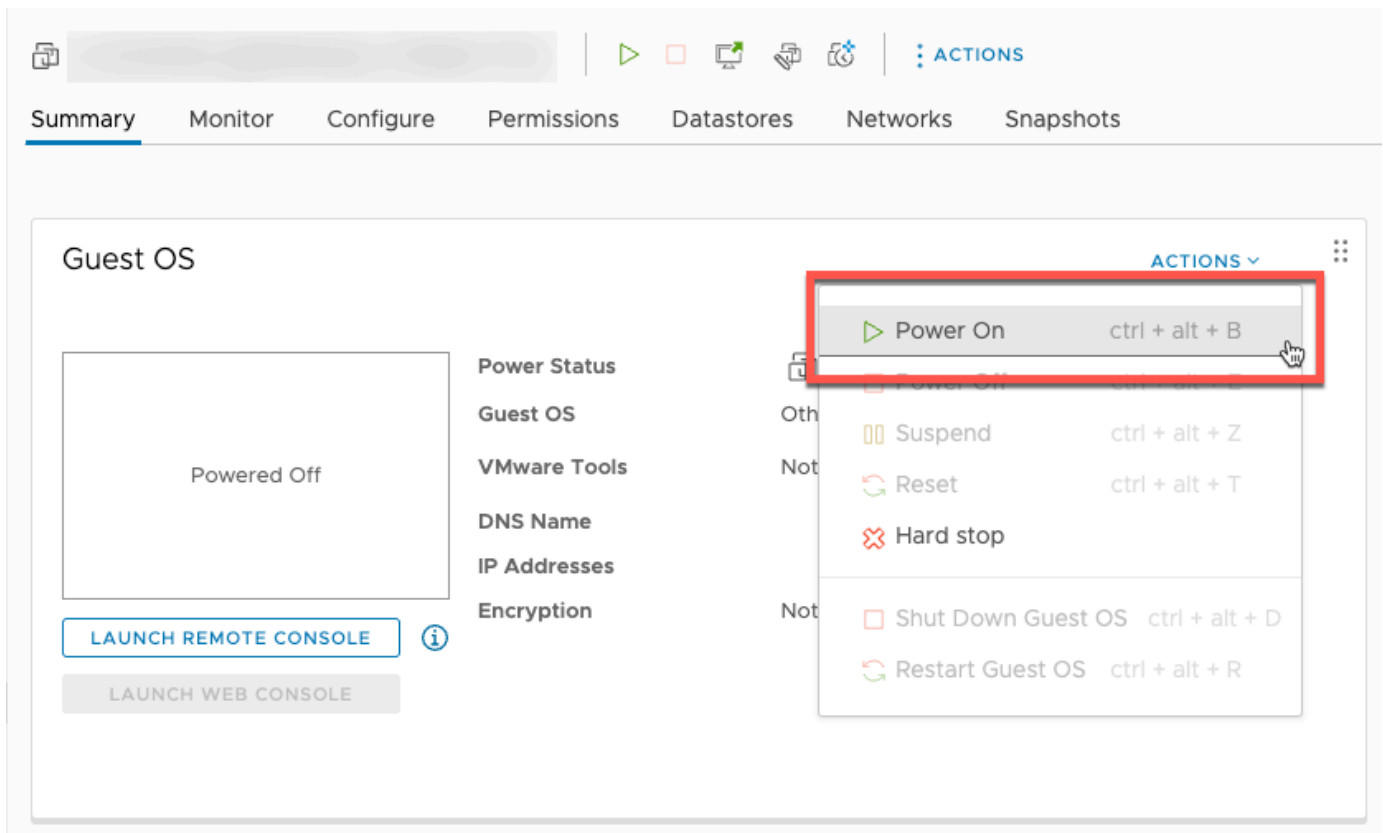
Virtual Hardware VM Options

> General Options	VM Name:
VMware Remote Console Options	☐
>	Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
▼ VMware Tools	
Power Operations	▶ Power On / Resume VM
	◻ Shut Down Guest (Default) ▼
	⏸ Suspend (Default) ▼
	↺ Restart Guest (Default) ▼
Tools Upgrades	☐ Check and upgrade VMware Tools before each power on
Synchronize Time with Host ⓘ	☒ Synchronize at startup and resume (recommended) ☐ Synchronize time periodically
Run VMware Tools Scripts	☒ After powering on ☒ After resuming ☒ Before suspending ☒ Before shutting down guest

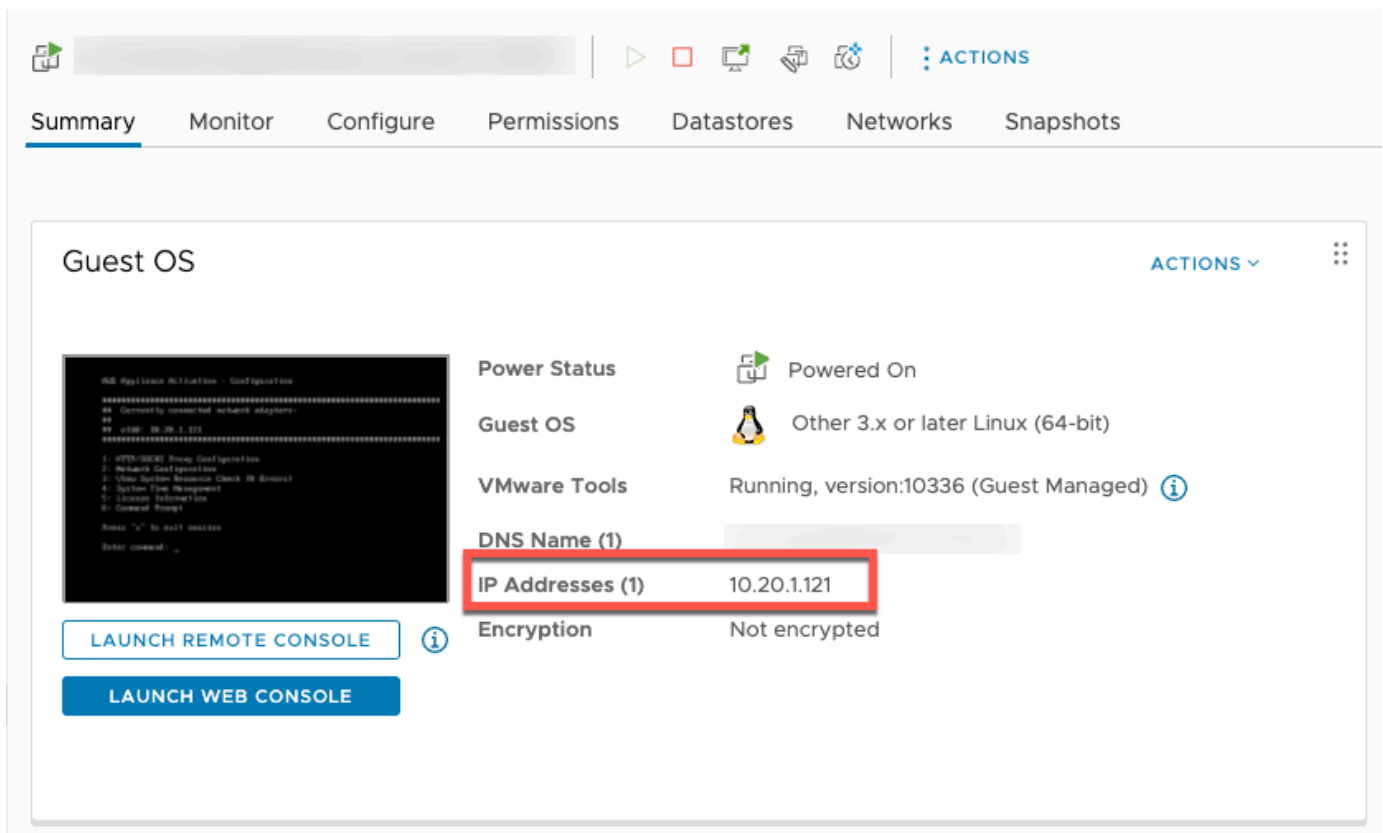
CANCEL

OK

6. Allumez la machine virtuelle en sélectionnant « Allumer » dans le menu Actions.



7. Copiez l'adresse IP depuis le résumé de la machine virtuelle et entrez-la ci-dessous.



Une fois le VMWare logiciel téléchargé, procédez comme suit :

1. Dans la section Connexion à la passerelle, saisissez l'adresse IP de la passerelle.
 - a. Pour trouver cette adresse IP, accédez à vSphere Client.
 - b. Sélectionnez votre passerelle sous l'onglet Résumé.
 - c. Copiez l'adresse IP et collez-la dans la barre de texte de la AWS Backup console.
2. Dans la section Paramètres de la passerelle,
 - a. Saisissez un Nom de passerelle.
 - b. Vérifiez la AWS région.
 - c. Choisissez si le point de terminaison est accessible au public ou hébergé dans votre cloud privé virtuel (VPC).
 - d. En fonction du point de terminaison choisi, entrez le nom DNS du point de terminaison du VPC.

Pour plus d'informations, consultez [Créer un point de terminaison VPC](#).

3. [Facultatif] Dans la section Identifications de la passerelle, vous pouvez attribuer des balises en saisissant la clé et la valeur facultative. Pour ajouter plusieurs balises, cliquez sur Ajouter une autre balise.
4. Pour terminer le processus, cliquez sur Créer une passerelle, qui vous amène à la page détaillée de la passerelle.

Création manuelle d'une passerelle (IPv4 et IPv6)

Pour obtenir de IPv6 l'aide, créez des passerelles manuellement à l'aide des clés d'activation.

IPv6 le support nécessite la version 2.x+ de l'appliance Gateway et une configuration de pare-feu supplémentaire sur les points de terminaison [à double](#) pile.

Important

IPv6 exige d'hyperviseur : si votre passerelle est activée via IPv6, vous devez créer un hyperviseur avec une IPv6 adresse. Par exemple, utilisez 2607:fda8:1001:210::252 plutôt que 10.0.0.252. Si vous associez une IPv6 passerelle à un IPv4 hyperviseur, les tâches de sauvegarde et de restauration échoueront probablement.

Obtenir une clé d'activation

Pour recevoir une clé d'activation pour votre passerelle, envoyez une demande Web à la machine virtuelle (VM) de passerelle ou utilisez la console locale de la passerelle. La machine virtuelle de passerelle renvoie une réponse contenant la clé d'activation, qui est ensuite transmise comme l'un des paramètres permettant à l>CreateGatewayAPI de spécifier la configuration de votre passerelle.

Tip

Les clés d'activation de passerelle expirent au bout de 30 minutes si elles ne sont pas utilisées.

Obtenir une clé d'activation à l'aide d'une requête Web

Les exemples suivants montrent comment obtenir une clé d'activation à l'aide d'une requête HTTP. Vous pouvez utiliser un navigateur Web, Linux curl ou une commande équivalente en procédant comme suit URLs.

Note

Remplacez les variables mis en évidence par des valeurs réelles pour votre passerelle. Les valeurs possibles sont les suivantes :

- *gateway_ip_address*- L' IPv4 adresse de votre passerelle, par exemple 172.31.29.201
- *region_code*- La région dans laquelle vous souhaitez activer votre passerelle. Voir les [Points de terminaison régionaux](#) dans le Guide de référence général AWS . Si ce paramètre n'est pas spécifié, ou si la valeur fournie est mal orthographiée ou ne correspond pas à une région valide, la commande utilisera par défaut la us-east-1 région.

Points de terminaison à double pile (support) IPv6

IPv4:

```
curl "http://gateway_ip_address/?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv4&no_red
```

IPv6:

```
curl "http://gateway_ip_address?  
activationRegion=region_code&gatewayType=BACKUP_VM&endpointType=DUALSTACK&ipVersion=ipv6&no_red
```

Obtenir une clé d'activation à l'aide de la console locale

Les exemples suivants vous montrent comment obtenir une clé d'activation à l'aide de la console locale de l'hôte de passerelle

1. Connectez-vous à la console de votre machine virtuelle.
2. Dans le menu principal Activation de l'AWS appliance - Configuration, sélectionnez 0 Obtenir la clé d'activation
3. Sélectionnez 2 Backup Gateway pour l'option de la famille de passerelles
4. Entrez la AWS région dans laquelle vous souhaitez activer votre passerelle
5. Pour le type de réseau, entrez 1 pour Public ou 2 pour point de terminaison VPC
6. Pour le type de point de terminaison, entrez 1 pour le point de terminaison standard ou 2 pour le point de terminaison à double pile
 - Pour un point de terminaison à double pile, sélectionnez 1 pour IPv4 ou 2 pour IPv6
7. La clé d'activation sera renseignée automatiquement

Création de la passerelle

Utilisez le AWS CLI pour créer la passerelle après avoir obtenu une clé d'activation :

1. Obtenir la clé d'activation à l'aide des commandes curl ou de la méthode de console locale
2. Créez une passerelle à l'aide AWS CLI, pour plus d'informations, de [CreateGateway](#) la section Référence de l'API Backup Gateway.

```
aws backup-gateway create-gateway \  
    --region region_code \  
    --activation-key activation_key \  
    --gateway-display-name gateway_name \  
    --gateway-type BACKUP_VM
```

3. Vérifiez que la passerelle apparaît dans AWS Backup la console sous Ressources externes → Passerelles

Modification ou suppression d'une passerelle

Pour modifier ou supprimer une passerelle :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Passerelles.
2. Dans la section Passerelles, choisissez une passerelle en fonction de son Nom de passerelle.
3. Pour modifier le nom de la passerelle, choisissez Modifier.
4. Pour supprimer la passerelle, choisissez Supprimer, puis Supprimer la passerelle.

Vous ne pouvez pas réactiver une passerelle supprimée. Si vous souhaitez vous connecter à nouveau à l'hyperviseur, suivez la procédure décrite dans [Création d'une passerelle](#).

5. Pour vous connecter à un hyperviseur, dans la section Hyperviseur connecté, choisissez Connecter.

Chaque passerelle se connecte à un seul hyperviseur. Cependant, vous pouvez connecter plusieurs passerelles au même hyperviseur pour augmenter la bande passante entre elles au-delà de celle de la première passerelle.

6. Pour attribuer, modifier ou gérer des balises, dans la section Balises, choisissez Gérer les balises.

Limitation de bande passante de la passerelle de sauvegarde

Note

Cette fonctionnalité sera disponible sur les nouvelles passerelles déployées après le 15 décembre 2022. Pour les passerelles existantes, cette nouvelle fonctionnalité sera disponible via une mise à jour logicielle automatique au plus tard le 30 janvier 2023. Pour mettre à jour manuellement la passerelle vers la dernière version, utilisez AWS CLI la commande [UpdateGatewaySoftwareNow](#).

Vous pouvez limiter le débit de téléchargement depuis votre passerelle AWS Backup pour contrôler la quantité de bande passante réseau utilisée par la passerelle. Par défaut, une passerelle activée n'a pas de limites de taux.

Vous pouvez configurer un calendrier de limite de bande passante à l'aide de la AWS Backup console ou de l'API via le AWS CLI () [PutBandwidthRateLimitSchedule](#). Lorsque vous utilisez

une planification de limite de débit de la bande passante, vous pouvez configurer les limites pour qu'elles changent automatiquement au cours de la journée ou de la semaine.

La limitation du taux de bande passante fonctionne en équilibrant le débit de toutes les données téléchargées, en moyenne chaque seconde. Bien qu'il soit possible que les téléchargements dépassent brièvement la limite de taux de bande passante pendant une micro ou une milliseconde donnée, cela n'entraîne généralement pas de pics importants sur de longues périodes.

Vous pouvez ajouter jusqu'à 20 intervalles. La valeur maximale du débit de téléchargement est de 8 000 000 Mbits/s.

Consultez et modifiez le calendrier de limite de bande passante pour votre passerelle à l'aide de la AWS Backup console.

Cette section explique comment afficher et modifier la planification de limite de débit de la bande passante pour votre passerelle.

Pour consulter et modifier la planification de limite de débit de la bande passante

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles. Dans le volet Passerelles, les passerelles sont affichées par nom. Cliquez sur la case d'option à côté du nom de la passerelle que vous souhaitez gérer.
3. Une fois que vous avez sélectionné une case d'option, vous pouvez cliquer sur le menu déroulant Action. Cliquez sur Actions, puis sur Modifier la planification de limite de débit de la bande passante. La planification actuelle s'affiche. Par défaut, aucune limite de débit de bande passante n'est définie pour une passerelle nouvelle ou non modifiée.

 Note

Vous pouvez également cliquer sur Gérer la planification dans la page des détails de la passerelle pour accéder à la page Modifier la bande passante.

4. (Facultatif) Choisissez Ajouter un intervalle pour ajouter un nouvel intervalle configurable à la planification. Pour chaque intervalle, saisissez les informations suivantes :
 - a. Jours de la semaine : sélectionnez le ou les jours récurrents auxquels vous souhaitez appliquer l'intervalle. Une fois sélectionnés, les jours s'affichent sous le menu déroulant. Vous pouvez les supprimer en cliquant sur le X à côté du jour.

- b. Heure de début : entrez l'heure de début de l'intervalle de bande passante, en utilisant le format 24 heures HH:MM. L'heure doit être exprimée au format UTC (temps universel coordonné).

Remarque : Votre bandwidth-rate-limit intervalle commence au début de la minute spécifiée.

- c. Heure de fin : entrez l'heure de fin de l'intervalle de bande passante, en utilisant le format 24 heures HH:MM. L'heure doit être exprimée au format UTC (temps universel coordonné).

 Important

L' bandwidth-rate-limit intervalle prend fin à la fin de la minute spécifiée. Pour planifier un intervalle se terminant au bout d'une heure, entrez 59. Pour planifier des intervalles continus consécutifs, en effectuant la transition au début de l'heure, sans interruption entre les intervalles, entrez 59 pour la minute de fin du premier intervalle. Entrez 00 pour la minute de début de l'intervalle suivant.

- d. Débit de chargement : entrez la limite de débit de téléchargement, en mégabits par seconde (Mbits/s). La valeur minimale est de 102 mégaoctets par seconde (Mbits/s).
5. (Facultatif) Répétez l'étape précédente comme vous le souhaitez jusqu'à ce que votre planification de limite de débit de la bande passante soit terminée. Si vous devez supprimer un intervalle de votre planification, choisissez Supprimer.

 Important

Les intervalles de limite de taux de bande passante ne peuvent pas se chevaucher. L'heure de début d'un intervalle doit être postérieure à l'heure de fin d'un intervalle précédent et antérieure à l'heure de début d'un intervalle suivant ; son heure de fin doit être antérieure à l'heure de début de l'intervalle suivant.

6. Lorsque vous avez terminé, cliquez sur le bouton Enregistrer les modifications.

Consultez et modifiez la planification de limite de débit de la bande passante pour votre passerelle à l'aide de l' AWS CLI.

L'action [GetBandwidthRateLimitSchedule](#) peut être utilisée pour afficher la planification de limitation de bande passante pour une passerelle spécifiée. Si aucune planification n'est définie,

la planification sera une liste vide d'intervalles. Voici un exemple d'utilisation du AWS CLI pour récupérer le planning de bande passante d'une passerelle :

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Pour modifier la planification de limitation de bande passante d'une passerelle, vous pouvez utiliser l'action [PutBandwidthRateLimitSchedule](#). Notez que vous ne pouvez mettre à jour la planification d'une passerelle que dans son ensemble, plutôt que de modifier, d'ajouter ou de supprimer des intervalles individuels. Cette action remplacera la planification précédente de limitation de bande passante de la passerelle.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Utilisation des hyperviseurs

Une fois que vous avez terminé [Création d'une passerelle](#), vous pouvez le connecter à un hyperviseur pour AWS Backup permettre de travailler avec les machines virtuelles gérées par cet hyperviseur. Par exemple, l'hyperviseur pour VMware VMs est VMware vCenter Server. Assurez-vous que votre hyperviseur est configuré avec les [autorisations nécessaires pour AWS Backup](#).

Ajout d'un hyperviseur

Pour ajouter un hyperviseur :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Choisissez Ajouter un hyperviseur.
3. Dans la section Paramètres de l'hyperviseur, saisissez le Nom de l'hyperviseur.
4. Pour Hôte du serveur vCenter, utilisez le menu déroulant pour sélectionner l'adresse IP ou le Nom de domaine complet (FQDN). Saisissez la valeur correspondante.
5. Pour permettre AWS Backup de découvrir les machines virtuelles sur l'hyperviseur, entrez le nom d'utilisateur et le mot de passe de l'hyperviseur.
6. Chiffrez votre mot de passe. Vous pouvez [spécifier ce chiffrement](#) en sélectionnant une clé KMS gérée par un service spécifique ou une clé KMS gérée par le client à l'aide du menu déroulant ou en choisissant Créer une clé KMS. Si vous ne sélectionnez pas de clé spécifique, AWS Backup chiffrera votre mot de passe à l'aide d'une clé appartenant au service.

7. Dans la section Connexion de passerelle, utilisez la liste déroulante pour spécifier la passerelle à connecter à votre hyperviseur.
8. Choisissez Tester la connexion de la passerelle pour vérifier vos entrées précédentes.
9. (Facultatif) Dans la section Identifications de l'hyperviseur, vous pouvez attribuer des balises à l'hyperviseur en choisissant Ajouter une nouvelle balise.
10. [Mappage de VMware balises](#) facultatif : vous pouvez ajouter jusqu'à 10 VMware balises que vous utilisez actuellement sur vos machines virtuelles pour générer des AWS balises.
11. Dans le panneau de configuration du groupe de journaux, vous pouvez choisir d'intégrer [Amazon CloudWatch Logs](#) pour conserver les journaux de votre hyperviseur (la [tarification standard CloudWatch des journaux](#) s'appliquera en fonction de l'utilisation). Chaque hyperviseur peut appartenir à un seul et même groupe de journaux.
 - a. Si vous n'avez pas encore créé de groupe de journaux, sélectionnez la case d'option Créer un nouveau groupe de journaux. L'hyperviseur que vous êtes en train de modifier sera associé à ce groupe de journaux.
 - b. Si vous avez déjà créé un groupe de journaux pour un autre hyperviseur, vous pouvez utiliser ce groupe de journaux pour cet hyperviseur. Sélectionnez Utiliser un groupe de journaux existant.
 - c. Si vous ne souhaitez pas la CloudWatch journalisation, sélectionnez Désactiver la journalisation.
12. Choisissez Ajouter un hyperviseur pour accéder à sa page détaillée.

 Tip

Vous pouvez utiliser Amazon CloudWatch Logs (voir étape 11 ci-dessus) pour obtenir des informations sur votre hyperviseur, notamment la surveillance des erreurs, la connexion réseau entre la passerelle et l'hyperviseur, ainsi que des informations de configuration réseau. Pour plus d'informations sur les groupes de CloudWatch journaux, consultez la section [Working with Log Groups and Log Streams](#) dans le guide de CloudWatch l'utilisateur Amazon.

Affichage des machines virtuelles gérées par un hyperviseur

Pour afficher les machines virtuelles sur un hyperviseur :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Dans la section sous Résumé de l'hyperviseur, choisissez l'onglet Machines virtuelles.
4. Dans la section Machines virtuelles connectées, une liste de machines virtuelles est automatiquement renseignée.

Affichage des passerelles connectées à un hyperviseur

Pour afficher les passerelles connectées à l'hyperviseur :

1. Choisissez l'onglet Passerelles.
2. Dans la section Passerelles connectées, une liste de passerelles est automatiquement renseignée.

Connexion d'un hyperviseur à des passerelles supplémentaires

Vos vitesses de sauvegarde et de restauration peuvent être limitées par la bande passante de la connexion entre votre passerelle et l'hyperviseur. Vous pouvez augmenter ces vitesses en connectant une ou plusieurs passerelles supplémentaires à votre hyperviseur. Vous pouvez le faire dans la section Passerelles connectées comme suit :

1. Choisissez Se connecter.
2. Sélectionnez une autre passerelle à l'aide du menu déroulant. Vous pouvez également choisir Créer une passerelle pour créer une nouvelle passerelle.
3. Choisissez Se connecter.

Modification de la configuration d'un hyperviseur

Si vous n'utilisez pas la fonctionnalité Tester la connexion de la passerelle, vous pouvez ajouter un hyperviseur avec un nom d'utilisateur ou un mot de passe incorrect. Dans ce cas, le statut de connexion de l'hyperviseur est toujours Pending. Vous pouvez également alterner le nom

d'utilisateur ou le mot de passe pour accéder à votre hyperviseur. Mettez à jour ces informations à l'aide de la procédure suivante :

Pour modifier un hyperviseur déjà ajouté :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Choisissez Modifier.
4. Le panneau supérieur s'appelle Paramètres de l'hyperviseur.
 - a. Sous Hôte du serveur vCenter, vous pouvez également modifier le FQDN (nom de domaine complet) ou l'adresse IP.
 - b. (Facultatif) Entrez le Nom d'utilisateur et le Mot de passe de l'hyperviseur.
5. Dans le panneau de configuration du groupe de journaux, vous pouvez choisir d'intégrer [Amazon CloudWatch](#) pour conserver les journaux de votre hyperviseur (la [CloudWatch tarification](#) standard s'appliquera en fonction de l'utilisation). Chaque hyperviseur peut appartenir à un seul et même groupe de journaux.
 - a. Si vous n'avez pas encore créé de groupe de journaux, sélectionnez la case d'option Créer un nouveau groupe de journaux. L'hyperviseur que vous êtes en train de modifier sera associé à ce groupe de journaux.
 - b. Si vous avez déjà créé un groupe de journaux pour un autre hyperviseur, vous pouvez utiliser ce groupe de journaux pour cet hyperviseur. Sélectionnez Utiliser un groupe de journaux existant.
 - c. Si vous ne souhaitez pas la CloudWatch journalisation, sélectionnez Désactiver la journalisation.

 Tip

Vous pouvez utiliser Amazon CloudWatch Logs (voir étape 5 ci-dessus) pour obtenir des informations sur votre hyperviseur, notamment la surveillance des erreurs, la connexion réseau entre la passerelle et l'hyperviseur, ainsi que des informations de configuration réseau. Pour plus d'informations sur les groupes de CloudWatch journaux, consultez la

section [Working with Log Groups and Log Streams](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour mettre à jour un hyperviseur par programmation, utilisez la commande de la CLI [update-hypervisor](#) et l'appel d'API. [UpdateHypervisor](#)

Suppression de la configuration d'un hyperviseur

Si vous devez supprimer un hyperviseur déjà ajouté, supprimez la configuration de l'hyperviseur et ajoutez-en une autre. Cette opération de suppression s'applique à la configuration de connexion à l'hyperviseur. Cela ne supprime pas l'hyperviseur.

Pour supprimer la configuration afin de vous connecter à un hyperviseur déjà ajouté :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Choisissez Supprimer, puis Supprimer l'hyperviseur.
4. Facultatif : remplacez la configuration de l'hyperviseur supprimée en suivant la procédure pour [Ajout d'un hyperviseur](#).

Compréhension du statut de l'hyperviseur

Ce qui suit décrit chacun des statuts possibles de l'hyperviseur et, le cas échéant, les étapes de correction. Le statut ONLINE est le statut normal de l'hyperviseur. Un hyperviseur doit avoir ce statut tout le temps ou la plupart du temps lorsqu'il est utilisé pour la sauvegarde et la restauration des données VMs gérées par l'hyperviseur.

Statuts de l'hyperviseur

Status	Signification et remédiation
ONLINE	Vous y avez ajouté un hyperviseur AWS Backup, vous lui avez associé une passerelle, et vous pouvez vous connecter à cette passerelle via votre réseau pour effectuer la sauvegarde et la restauration des machines virtuelles gérées par l'hyperviseur.

Status	Signification et remédiation
	Vous pouvez effectuer des sauvegardes à la demande et planifiées de ces machines virtuelles à tout moment.
PENDING	Vous avez ajouté un hyperviseur à AWS Backup mais : • Il n'est associé à aucune passerelle, ou • Il est associé à une ou plusieurs passerelles, mais toutes ces passerelles ont été supprimées ou ne sont pas actives. Pour modifier le statut d'un hyperviseur de PENDING à ONLINE, créez une passerelle et connectez votre hyperviseur à cette passerelle.
OFFLINE	Vous avez ajouté un hyperviseur AWS Backup et l'avez associé à une passerelle, mais la passerelle ne peut pas se connecter à l'hyperviseur via votre réseau. Pour modifier le statut d'un hyperviseur de OFFLINE à ONLINE, vérifiez l'exactitude de la configuration de votre réseau. Si le problème persiste, vérifiez que l'adresse IP ou le nom de domaine complet de votre hyperviseur est correct. S'ils sont incorrects, ajoutez à nouveau votre hyperviseur en utilisant les informations correctes et testez votre connexion à la passerelle.

Status	Signification et remédiation
ERROR	Vous avez ajouté un hyperviseur AWS Backup et l'avez associé à une passerelle, mais la passerelle ne peut pas communiquer avec l'hyperviseur. Pour modifier le statut d'un hyperviseur de ERROR à ONLINE, vérifiez que le nom d'utilisateur et le mot de passe de l'hyperviseur sont corrects. S'ils sont incorrects, modifiez la configuration de votre hyperviseur.

Étapes suivantes

Pour sauvegarder des machines virtuelles sur votre hyperviseur, consultez [Sauvegarde des machines virtuelles](#).

Sauvegarde des machines virtuelles

Après [Ajout d'un hyperviseur](#), Backup gateway répertorie automatiquement vos machines virtuelles. Vous pouvez afficher vos machines virtuelles en choisissant Hyperviseurs ou Machines virtuelles dans le volet de navigation de gauche.

- Choisissez Hyperviseurs pour afficher uniquement les machines virtuelles gérées par un hyperviseur spécifique. Avec cette vue, vous pouvez travailler avec une machine virtuelle à la fois.
- Choisissez Machines virtuelles pour afficher toutes les machines virtuelles sur tous les hyperviseurs que vous avez ajoutés à votre. Compte AWS Avec cette vue, vous pouvez travailler avec une partie ou la totalité de vos machines virtuelles sur plusieurs hyperviseurs.

Quelle que soit la vue choisie, pour effectuer une opération de sauvegarde sur une machine virtuelle spécifique, choisissez le nom de cette machine virtuelle pour ouvrir sa page détaillée. La page détaillée de la machine virtuelle constitue le point de départ des procédures suivantes.

Création d'une sauvegarde à la demande d'une machine virtuelle

Une sauvegarde [à la demande](#) est une sauvegarde complète unique que vous lancez manuellement. Vous pouvez utiliser des sauvegardes à la demande pour tester AWS Backup les fonctionnalités de sauvegarde et de restauration.

Pour créer une sauvegarde à la demande d'une machine virtuelle :

1. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).
2. [Configurer votre sauvegarde à la demande](#).
3. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).
4. Vérifiez que votre tâche de sauvegarde a le statut Completed. Dans le menu de navigation de gauche, choisissez Tâches.
5. Choisissez ID de tâche de backup pour afficher les informations relatives à la tâche de sauvegarde, telles que la Taille de sauvegarde et le temps écoulé entre la Date de création et Date de fin.

Sauvegardes de machines virtuelles incrémentielles

Les nouvelles VMware versions contiennent une fonctionnalité appelée [suivi des blocs modifiés](#), qui permet de suivre les blocs de stockage des machines virtuelles à mesure qu'ils changent au fil du temps. Lorsque vous AWS Backup sauvegardez une machine virtuelle, AWS Backup tente d'utiliser les données CBT si elles sont disponibles. AWS Backup utilise les données CBT pour accélérer le processus de sauvegarde ; sans données CBT, les tâches de sauvegarde sont souvent plus lentes et utilisent davantage de ressources d'hyperviseur. La sauvegarde peut toujours être effectuée, même lorsque les données CBT ne sont pas valides ou disponibles. Par exemple, les données CBT peuvent ne pas être valides ou ne pas être disponibles en cas d'arrêt brutal de la machine virtuelle ou de l'ESXi hôte.

Lorsque les données CBT ne sont pas valides ou disponibles, le statut de la sauvegarde affiche Successful avec un message. Dans ces cas, le message indiquera qu'en l'absence de données CBT, il a AWS Backup utilisé son propre mécanisme de détection des modifications pour effectuer la sauvegarde au lieu des VMware données CBT. Les sauvegardes suivantes essaieront à nouveau d'utiliser les données CBT et, dans la plupart des cas, les données CBT seront valides et disponibles. Si le problème persiste, consultez la section [VMware Dépannage](#) pour savoir comment y remédier.

Pour que CBT fonctionne correctement, les conditions suivantes doivent être remplies :

- L'hôte doit être ESXi 4.0 ou version ultérieure
- La machine virtuelle propriétaire des disques doit disposer du matériel version 7 ou ultérieure
- Le CBT doit être activé pour la machine virtuelle (il est activé par défaut)

Pour vérifier si le CBT est activé sur un disque virtuel, procédez comme suit :

1. Ouvrez le client vSphere et sélectionnez une machine virtuelle hors tension.
2. Cliquez avec le bouton droit sur la machine virtuelle et accédez à Modifier les paramètres > Options > Avancé/Général > Paramètres de configuration.
3. L'option `ctkEnabled` doit être égale à `True`.

Automatisation de la sauvegarde des machines virtuelles en attribuant des ressources à un plan de sauvegarde

Un [plan de sauvegarde](#) est une politique de protection des données définie par l'utilisateur qui automatise la protection des données dans de nombreux services AWS et applications tierces. Vous créez d'abord votre plan de sauvegarde en spécifiant sa fréquence de sauvegarde, sa période de rétention, sa politique de cycle de vie et de nombreuses autres options. Pour créer un plan de sauvegarde, consultez le Didacticiel de démarrage.

Après avoir créé votre plan de sauvegarde, vous attribuez des ressources AWS Backup prises en charge, notamment des machines virtuelles, à ce plan de sauvegarde. AWS Backup propose [de nombreuses méthodes pour attribuer des ressources](#), notamment en affectant toutes les ressources de votre compte, y compris ou en excluant des ressources spécifiques, ou en ajoutant des ressources avec certaines balises.

Outre ses fonctionnalités d'attribution de ressources existantes, la prise en AWS Backup charge des machines virtuelles introduit plusieurs nouvelles fonctionnalités qui vous aident à attribuer rapidement des machines virtuelles à des plans de sauvegarde. Depuis la page Machines virtuelles, vous pouvez attribuer des balises à plusieurs machines virtuelles ou utiliser la nouvelle fonctionnalité Affecter des ressources au plan. Utilisez ces fonctionnalités pour attribuer vos machines virtuelles déjà découvertes par AWS Backup Gateway.

Si vous prévoyez de découvrir et d'attribuer des machines virtuelles supplémentaires à l'avenir, et que vous souhaitez automatiser l'étape d'attribution des ressources pour inclure ces futures machines virtuelles, utilisez la nouvelle fonctionnalité Créer une affectation de groupe.

VMware Balises

Les [balises](#) sont des paires clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources.

Un VMware tag est composé d'une catégorie et d'un nom de tag. VMware les balises sont utilisées pour regrouper les machines virtuelles. Un nom de balise est une étiquette attribuée à une machine virtuelle. Une catégorie est un ensemble de noms de balises.

Dans les AWS balises, vous pouvez utiliser des caractères tels que des lettres UTF-8, des chiffres, des espaces et des caractères spéciaux. + - = . _ : /

Si vous utilisez des balises sur vos machines virtuelles, vous pouvez ajouter jusqu'à 10 balises correspondantes dans AWS Backup pour une meilleure organisation. Vous pouvez associer jusqu'à 10 VMware balises à des AWS balises. Dans la [AWS Backup console](#), vous pouvez les trouver dans Ressources externes > Machines virtuelles > AWS tags ou VMware tags.

VMware mappage des balises

Si vous utilisez des balises sur vos machines virtuelles, vous pouvez ajouter jusqu'à 10 balises correspondantes dans AWS Backup pour plus de clarté et une meilleure organisation. Les mappages s'appliquent à n'importe quelle machine virtuelle de l'hyperviseur.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans la console, accédez à Modifier l'hyperviseur (cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le nom de l'hyperviseur, puis sur Gérer les mappages).
3. Le dernier volet, le mappage des VMware balises, contient quatre champs de zone de texte dans lesquels vous pouvez saisir les informations de vos VMware balises dans les AWS balises correspondantes. Les quatre champs sont la catégorie de balise Vmware, VMware le nom de AWS balise, la clé de AWS balise et la valeur de la balise (exemple : Catégorie = OS ; nom de balise = Windows ; clé de AWS balise = OS-Windows et valeur de AWS balise = Windows).
4. Après avoir saisi vos valeurs préférées, cliquez sur Ajouter un mappage. En cas d'erreur, vous pouvez cliquer sur Supprimer pour supprimer les informations entrées.
5. Après avoir ajouté des mappages, spécifiez le rôle IAM que vous souhaitez utiliser pour appliquer ces AWS balises aux machines VMware virtuelles.

La politique [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#) contient les autorisations nécessaires. Vous pouvez associer cette politique au rôle que vous

utilisez (ou demander à un administrateur de l'associer) ou vous pouvez créer une politique personnalisée pour le rôle utilisé.

6. Enfin, cliquez sur Ajouter un hyperviseur ou Enregistrer.

La relation d'approbation du rôle IAM doit être modifiée pour ajouter les services backup-gateway.amazonaws.com et backup.amazonaws.com. Sans ce service, vous risquez de rencontrer une erreur lors du mappage des balises. Pour modifier la relation d'approbation pour un rôle existant,

1. Connectez-vous à la [console IAM](#).
2. Dans le volet de navigation de la console, choisissez Rôles.
3. Choisissez le nom du rôle que vous voulez modifier, puis sélectionnez l'onglet Relations d'approbation dans la page des détails.
4. Dans Document de stratégie, collez ce qui suit :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Choisissez Mettre à jour la politique d'approbation.

Pour plus de détails, consultez [Modification de la relation d'approbation pour un rôle existant](#) dans le Guide d'administration AWS Directory Service.

Afficher les mappages de VMware balises

Dans la [console AWS Backup](#), cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le lien du nom de l'hyperviseur pour afficher les propriétés de l'hyperviseur sélectionné. Sous le volet récapitulatif se trouvent quatre onglets, le dernier étant consacré aux mappages de VMware balises. Notez que si vous n'avez pas encore de mappage, « Aucun mappage de VMware balises » sera affiché.

À partir de là, vous pouvez synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur, vous pouvez copier des mappages vers vos hyperviseurs, vous pouvez ajouter des AWS balises mappées aux balises à la VMware sélection de sauvegarde d'un plan de sauvegarde ou vous pouvez gérer les mappages.

Dans la console, pour voir quelles balises sont appliquées à une machine virtuelle sélectionnée, cliquez sur Machines virtuelles, puis sur le nom de la machine virtuelle, puis sur AWS balises ou VMware balises. Vous pouvez afficher et gérer les balises associées à cette machine virtuelle.

Attribuez des machines virtuelles au plan à l'aide de mappages de VMware balises

Pour attribuer des machines virtuelles à un plan de sauvegarde à l'aide de balises mappées, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans la console, accédez aux mappages de VMware balises sur la page de détails de l'hyperviseur (cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le nom de l'hyperviseur).
3. Cochez la case à côté de plusieurs balises mappées pour attribuer ces balises au même plan de sauvegarde.
4. Cliquez sur Ajouter à l'attribution de ressource.
5. Choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
6. Cliquez sur Confirmer. Cela ouvre la page Affecter des ressources avec des valeurs préremplies dans le champ Affiner la sélection à l'aide de balises.

VMware balises utilisant le AWS CLI

AWS Backup utilise l'appel d'API [PutHypervisorPropertyMappings](#) pour mapper les propriétés des entités de l'hyperviseur sur site aux propriétés de. AWS

Dans le AWS CLI, utilisez l'opération `put-hypervisor-property-mappings` :

```
aws backup-gateway put-hypervisor-property-mappings \  
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \  
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \  
--iam-role-arn arn:aws:iam::account:role/roleName \  
--region AWSRegion \  
--endpoint-url URL
```

Voici un exemple :

```
aws backup-gateway put-hypervisor-property-mappings \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-  
Windows,AwsTagValue=Windows \  
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \  
--region us-east-1
```

Vous pouvez également utiliser [GetHypervisorPropertyMappings](#) pour vous aider à obtenir des informations de mappage de propriétés. Dans le AWS CLI, utilisez l'opération `get-hypervisor-property-mappings`. Voici un exemple de modèle :

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN \  
--region AWSRegion
```

Voici un exemple :

```
aws backup-gateway get-hypervisor-property-mappings \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

Synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur à l' AWS aide d'une API, d'une CLI ou d'un SDK

Vous pouvez synchroniser les métadonnées des machines virtuelles. Lorsque vous le faites, les VMware balises présentes sur la machine virtuelle qui font partie des mappages seront synchronisées. En outre, les AWS balises mappées aux VMware balises présentes sur la machine virtuelle seront appliquées à la ressource de machine AWS virtuelle.

AWS Backup utilise l'appel [StartVirtualMachinesMetadataSync](#)d'API pour synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur. Pour synchroniser les

métadonnées des machines virtuelles découvertes par l'hyperviseur avec AWS CLI, utilisez l'opération `start-virtual-machines-metadata-sync`.

Exemple de modèle :

```
aws backup-gateway start-virtual-machines-metadata-sync \  
--hypervisor-arn Hypervisor ARN \  
--region AWSRegion
```

Exemple :

```
aws backup-gateway start-virtual-machines-metadata-sync \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

Vous pouvez également utiliser [GetHypervisor](#) pour obtenir des informations sur l'hyperviseur, telles que l'hôte, l'état, le statut de la dernière synchronisation des métadonnées et également pour récupérer l'heure de la dernière synchronisation de métadonnées réussie. Dans le AWS CLI, utilisez l'opération `get-hypervisor`.

Exemple de modèle :

```
aws backup-gateway get-hypervisor \  
--hypervisor-arn Hypervisor ARN \  
--region AWSRegion
```

Exemple :

```
aws backup-gateway get-hypervisor \  
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \  
--region us-east-1
```

Pour plus d'informations, consultez la documentation de l'API [VmwareTagetVmwareToAwsTagMapping](#).

Cette fonctionnalité sera disponible sur les nouvelles passerelles déployées après le 15 décembre 2022. Pour les passerelles existantes, cette nouvelle fonctionnalité sera disponible via une mise à jour logicielle automatique au plus tard le 30 janvier 2023. Pour mettre à jour manuellement la passerelle vers la dernière version, utilisez AWS CLI la commande [UpdateGatewaySoftwareNow](#).

Exemple :

```
aws backup-gateway update-gateway-software-now \  
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \  
--region us-east-1
```

Attribution de machines virtuelles à l'aide de balises

Vous pouvez attribuer à vos machines virtuelles actuellement découvertes AWS Backup, ainsi qu'à d'autres AWS Backup ressources, une étiquette que vous avez déjà attribuée à l'un de vos plans de sauvegarde existants. Vous pouvez également créer un [nouveau plan de sauvegarde](#) et une nouvelle [attribution de ressource basée sur des balises](#). Les plans de sauvegarde vérifient les ressources nouvellement attribuées chaque fois qu'ils exécutent une tâche de sauvegarde.

Pour baliser plusieurs machines virtuelles avec la même balise :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Cochez la case à côté du Nom de la machine virtuelle pour choisir toutes vos machines virtuelles. Vous pouvez également cocher la case à côté des noms de machines virtuelles que vous souhaitez baliser.
3. Sélectionnez Add Tags (Ajouter des balises).
4. Tapez une Clé de balise.
5. Recommandé : saisissez une Valeur de balise.
6. Choisissez Confirmer.

Attribution de machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan

Vous pouvez affecter les machines virtuelles actuellement découvertes par AWS Backup à un plan de sauvegarde existant ou nouveau à l'aide de la fonctionnalité Affecter des ressources au plan.

Pour attribuer des machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Cochez la case à côté du Nom de la machine virtuelle pour choisir toutes vos machines virtuelles. Vous pouvez également cocher la case à côté des noms de plusieurs machines virtuelles pour les attribuer au même plan de sauvegarde.
3. Choisissez Affectations, puis Affecter des ressources au plan.

4. Saisissez un Nom d'attribution de ressource.
5. Choisissez un rôle IAM d'attribution de ressources pour créer des sauvegardes et gérer les points de récupération. Si vous n'avez pas de rôle IAM spécifique à utiliser, nous vous recommandons le Rôle par défaut qui dispose des autorisations appropriées.
6. Dans la section Plan de sauvegarde, choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
7. Choisissez Attribuer des ressources.
8. Facultatif : vérifiez que vos machines virtuelles sont attribuées à un plan de sauvegarde en choisissant Afficher le plan de sauvegarde. Ensuite, dans la section Attributions de ressources, choisissez le Nom de l'attribution de ressources.

Attribution de machines virtuelles à l'aide de la fonctionnalité Créer une affectation de groupe

Contrairement aux deux fonctionnalités d'attribution de ressources précédentes pour les machines virtuelles, la fonctionnalité Créer une attribution de groupe affecte non seulement les machines virtuelles actuellement découvertes par AWS Backup, mais également les machines virtuelles découvertes à l'avenir dans un dossier ou un hyperviseur que vous définissez.

De plus, vous n'avez pas besoin de cocher de case pour utiliser la fonctionnalité Créer une affectation de groupe.

Pour attribuer des machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Choisissez Affectations, puis choisissez Créer une affectation de groupe.
3. Saisissez un Nom d'attribution de ressource.
4. Choisissez un rôle IAM d'attribution de ressources pour créer des sauvegardes et gérer les points de récupération. Si vous n'avez pas de rôle IAM spécifique à utiliser, nous vous recommandons le Rôle par défaut qui dispose des autorisations appropriées.
5. Dans la section Groupe de ressources, sélectionnez le menu déroulant Type de groupe. Vos options sont Dossier ou Hyperviseur.
 - a. Choisissez Dossier pour attribuer toutes les machines virtuelles d'un dossier sur un hyperviseur. Sélectionnez un Nom de groupe de dossiers, par exemple `datacenter/vm`, à l'aide du menu déroulant. Vous pouvez également choisir d'inclure des Sous-dossiers.

 Note

Pour effectuer des attributions basées sur des dossiers, pendant le processus de découverte, balisez AWS Backup les machines virtuelles avec le dossier dans lequel elles les ont trouvées pendant le processus de découverte. Si vous déplacez ultérieurement une machine virtuelle vers un autre dossier, vous AWS Backup ne pourrez pas mettre à jour la balise pour vous en raison des meilleures pratiques en matière de AWS balisage. Cette méthode d'attribution peut entraîner la poursuite des sauvegardes des machines virtuelles que vous avez déplacées hors du dossier qui vous a été attribué.

- b. Choisissez Hyperviseur pour attribuer toutes les machines virtuelles gérées par un hyperviseur. Sélectionnez le Nom de groupe d'un ID d'hyperviseur à l'aide du menu déroulant.
6. Dans la section Plan de sauvegarde, choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
7. Choisissez Créer une affectation de groupe.
8. Facultatif : vérifiez que vos machines virtuelles sont attribuées à un plan de sauvegarde en choisissant Afficher le plan de sauvegarde. Dans la section Attributions de ressources, choisissez le Nom de l'attribution de ressources.

Étapes suivantes

Pour restaurer une machine virtuelle, consultez [Restaurez une machine virtuelle à l'aide de AWS Backup](#).

Informations sur les composants source tiers pour Backup gateway

Dans cette section, vous pouvez trouver des informations sur les outils et licences tiers dont nous dépendons pour fournir les fonctionnalités Backup gateway.

Le code source de certains composants de logiciels source tiers qui sont inclus dans le logiciel Backup gateway est disponible en téléchargement aux emplacements suivants :

- Pour les passerelles déployées sur VMware ESXi, téléchargez [sources.tgz](#).

Ce produit inclut un logiciel développé par le projet OpenSSL pour être utilisé dans le kit d'outils OpenSSL (<https://www.openssl.org/>).

Ce produit inclut un logiciel développé par VMware® vSphere Software Development Kit () <https://www.vmware.com>.

Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez [Licences tierces](#).

Composants open source pour AWS Appliance

Plusieurs outils et licences tiers sont utilisés pour fournir des fonctionnalités pour Backup gateway.

Utilisez les liens suivants pour télécharger le code source de certains composants logiciels open source inclus dans le logiciel AWS Appliance :

- [Pour les passerelles déployées sur VMware ESXi, téléchargez le fichier sources.tar](#)

Ce produit inclut un logiciel développé par le projet OpenSSL pour être utilisé dans le kit d'outils OpenSSL (<https://www.openssl.org/>). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez [Licences tierces](#).

Résolution des problèmes de machines virtuelles

Sauvegardes incrémentielles/problèmes et messages CBT

Message d'échec : "The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."

Si ce message persiste, [réinitialisez le CBT](#) comme indiqué par VMware.

Le message indique que le CBT n'était pas activé ou n'était pas disponible : « Le suivi des blocs de VMware modifications (CBT) n'était pas disponible pour cette machine virtuelle, mais la sauvegarde incrémentielle a été effectuée avec succès grâce à notre mécanisme de modification propriétaire. »

Vérifiez que le CBT est activé. Pour vérifier si le CBT est activé sur un disque virtuel, procédez comme suit :

1. Ouvrez le client vSphere et sélectionnez une machine virtuelle hors tension.
2. Cliquez avec le bouton droit sur la machine virtuelle et accédez à Modifier les paramètres > Options > Avancé/Général > Paramètres de configuration.

3. L'option `ctkEnabled` doit être égale à `True`.

S'il est activé, assurez-vous que vous utilisez les up-to-date VMware fonctionnalités. L'hôte doit être ESXi 4.0 ou une version ultérieure et la machine virtuelle possédant les disques à suivre doit être dotée d'une version matérielle 7 ou ultérieure.

Si le CBT est activé et que le logiciel et le matériel sont à jour, éteignez la machine virtuelle, puis réactivez-la. Assurez-vous que le CBT est activé. Effectuez ensuite à nouveau la sauvegarde.

VMware échec de sauvegarde

L'échec d'une VMware sauvegarde peut être lié à l'un des facteurs suivants :

Message d'échec : "Failed to process backup data. Aborted backup job." ou "Error opening disk on the virtual machine".

Causes possibles : cette erreur peut être due à un problème de configuration ; ou bien, la VMware version ou le disque n'est pas pris en charge.

Solution 1 : Assurez-vous que votre infrastructure est configurée pour utiliser une passerelle et que tous les ports requis sont ouverts.

1. Accédez à la [console de passerelle de sauvegarde](#). Notez que c'est différent de la AWS Backup console.
2. Sur la page de configuration de la passerelle Backup, entrez l'option 3 pour tester la connectivité réseau.
3. Si le test réseau est réussi, entrez X.
4. Revenez à la page de configuration de la passerelle Backup.
5. Entrez 7 pour accéder à l'invite de commande.
6. Exécutez les commandes suivantes pour vérifier la connectivité réseau :

```
ncport -d ESXi Host -p 902
```

```
ncport -d ESXi Host -p 443
```

Remède 2 : utilisez des [Soutenu VMs](#) versions.

Solution 3 : Si un dispositif de passerelle est configuré avec des serveurs DNS incorrects, la sauvegarde échoue. Pour vérifier la configuration DNS, procédez comme suit :

1. Accédez à la [console de passerelle de sauvegarde](#).
2. Sur la page de configuration de la passerelle Backup, entrez l'option 2 pour accéder à la configuration réseau.
3. Dans Configuration réseau, entrez 7 pour afficher la configuration DNS.
4. Vérifiez les adresses IP des serveurs DNS. Si l'adresse IP du serveur DNS est incorrecte, l'invite à revenir à la configuration réseau existe.
5. Dans Configuration réseau, entrez 6 pour modifier la configuration DNS.
6. Entrez les adresses IP correctes du serveur DNS. Entrez ensuite X pour terminer la configuration de votre réseau.

Pour obtenir plus d'informations sur votre hyperviseur, telles que les erreurs, la configuration réseau et la connexion, consultez la section [Modification de la configuration d'un hyperviseur](#) pour configurer l'hyperviseur pour qu'il s'intègre à Amazon CloudWatch Logs.

Défaillances de sauvegarde dues à des problèmes de connexion réseau

Message d'échec : "Failed to upload backup during data ingestion. Aborted backup job." ou "Cloud network request timed out during data ingestion".

Causes possibles : Cette erreur peut se produire si la connexion réseau est insuffisante pour gérer les téléchargements de données. Si la bande passante réseau est faible, la liaison entre la machine virtuelle et la machine virtuelle AWS Backup peut être encombrée et entraîner l'échec des sauvegardes.

La bande passante réseau requise dépend de plusieurs facteurs, notamment de la taille de la machine virtuelle, des données incrémentielles générées pour chaque sauvegarde de machine virtuelle, de la fenêtre de sauvegarde et des exigences de restauration.

Solution : Les meilleures pratiques et recommandations incluent une bande passante minimale de 1 000 Mbits/s de bande passante de téléchargement pour les VMs connexions sur site. AWS Backup Une fois la bande passante confirmée, réessayez le travail de sauvegarde.

Tâche de sauvegarde abandonnée

Message d'échec : "Failed to create backup during snapshot creation. Aborted backup job."

Cause possible : L' VMware hôte sur lequel réside le dispositif de passerelle peut rencontrer un problème.

Solution : Vérifiez la configuration de votre VMware hôte et examinez-la pour détecter tout problème. Pour plus d'informations, consultez [Modification de la configuration d'un hyperviseur](#).

Aucune passerelle disponible

Message d'échec : "No gateways available to work on job."

Cause possible : toutes les passerelles connectées sont occupées par d'autres tâches. Chaque passerelle est limitée à quatre tâches simultanées (sauvegarde ou restauration).

Pour les solutions, consultez la section suivante pour connaître les étapes à suivre pour augmenter le nombre de passerelles et pour augmenter la durée du plan de sauvegarde.

VMware échec de la tâche de sauvegarde

Message d'échec : "Abort signal detected"

Causes possibles :

- Faible bande passante réseau : une bande passante réseau insuffisante peut empêcher l'exécution des sauvegardes pendant la période d'achèvement. Lorsque la tâche de sauvegarde nécessite plus de bande passante que celle disponible, elle peut entraîner un échec et déclencher l'erreur « Abandonner le signal détecté ».
- Nombre de passerelles de sauvegarde insuffisant : si le nombre de passerelles de sauvegarde n'est pas suffisant pour gérer la rotation des sauvegardes pour toutes les entités configurées VMs, la tâche de sauvegarde peut échouer. Cela peut se produire lorsque la fenêtre du plan de sauvegarde pour terminer les sauvegardes est trop courte ou que le nombre de passerelles de sauvegarde n'est pas suffisant.
- La fenêtre d'achèvement du plan de sauvegarde est trop petite.

Remèdes :

Augmenter la bande passante : envisagez d'augmenter la capacité du réseau entre AWS et l'environnement sur site. Cette étape fournira plus de bande passante pour le processus de sauvegarde, ce qui permettra aux données de se transférer sans problème sans provoquer d'erreur. Il est recommandé de disposer d'une bande passante d'au moins 100 Mbits/s pour AWS effectuer des sauvegardes sur site VMware VMs . AWS Backup

Si une limite de débit de bande passante est configurée pour la passerelle de sauvegarde, cela peut limiter le flux de données et entraîner des échecs de sauvegarde. L'augmentation de la limite de débit

de bande passante pour garantir une capacité de transfert de données suffisante peut contribuer à réduire les défaillances. Ce réglage peut atténuer l'apparition de l'erreur « Signal d'interruption détecté ». Pour de plus amples informations, veuillez consulter [Limitation de bande passante de la passerelle de sauvegarde](#).

Augmenter le nombre de passerelles de sauvegarde : une seule passerelle de sauvegarde peut traiter jusqu'à 4 tâches de sauvegarde et de restauration à la fois. Les tâches supplémentaires seront mises en file d'attente et attendront que la passerelle soit libérée jusqu'à ce que la fenêtre de démarrage de la sauvegarde soit passée. Si la fenêtre de sauvegarde passe et que les tâches en file d'attente n'ont pas démarré, ces tâches de sauvegarde échoueront avec un « signal d'abandon détecté ». Vous pouvez augmenter le nombre de passerelles de sauvegarde pour réduire le nombre de tâches échouées. Voir [Utilisation des passerelles](#) pour plus de détails.

Augmenter la durée de la fenêtre du plan de sauvegarde : vous pouvez augmenter la durée complète pendant la durée de la fenêtre de sauvegarde dans votre plan de sauvegarde. Voir [Options et configuration d'un plan de sauvegarde](#) pour plus de détails.

Pour obtenir de l'aide pour résoudre ces problèmes, consultez le [centre de AWS connaissances](#).

Création de sauvegardes Windows VSS

Avec AWS Backup, vous pouvez sauvegarder et restaurer les applications Windows compatibles VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2 . Si l'application possède un enregistreur VSS enregistré auprès de Windows VSS, il AWS Backup crée un instantané qui sera cohérent pour cette application.

Vous pouvez effectuer des restaurations cohérentes, tout en utilisant le même service de sauvegarde géré que celui utilisé pour protéger les autres AWS ressources. Lorsque les sauvegardes Windows cohérentes avec les applications sont activées EC2, vous bénéficiez des mêmes paramètres de cohérence et de la même connaissance des applications que les outils de sauvegarde traditionnels.

Note

AWS Backup prend uniquement en charge les sauvegardes cohérentes des ressources exécutées sur Amazon EC2, en particulier les scénarios de sauvegarde dans lesquels les données des applications peuvent être restaurées en remplaçant une instance existante par une nouvelle instance créée à partir de la sauvegarde. Les types d'instances ou applications ne sont pas tous pris en charge pour les sauvegardes VSS Windows.

Pour plus d'informations, consultez la section [Créer des instantanés basés sur VSS](#) dans le guide de EC2 l'utilisateur Amazon.

Pour sauvegarder et restaurer des ressources Windows compatibles VSS exécutant Amazon EC2, suivez ces étapes pour effectuer les tâches préalables requises. Pour obtenir des instructions, consultez la section [Conditions requises pour créer des instantanés EBS basés sur Windows VSS dans](#) le guide de l'utilisateur Amazon. EC2

1. Téléchargez, installez et configurez l'agent SSM dans AWS Systems Manager. Cette étape est obligatoire. Pour obtenir des instructions, consultez la section [Utilisation de l'agent SSM sur les EC2 instances pour Windows Server](#) dans le Guide de l'AWS Systems Manager utilisateur.
2. Ajoutez une politique IAM au rôle IAM et attachez le rôle à l' EC2 instance Amazon avant d'effectuer la sauvegarde Windows VSS (Volume Shadow Copy Service). Pour obtenir des instructions, consultez la section [Utiliser une politique gérée par IAM pour accorder des autorisations pour les instantanés basés sur VSS dans le guide](#) de l'utilisateur Amazon EC2 . Pour un exemple de politique IAM, consultez [Politiques gérées pour AWS Backup](#).
3. [Téléchargez et installez les composants VSS](#) sur l'instance Windows sur Amazon EC2
4. Activez VSS dans AWS Backup :
 1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
 2. Sur le tableau de bord, choisissez le type de sauvegarde que vous souhaitez créer, soit Créer un backup à la demande, soit Gérer les plans de backup. Fournissez les informations nécessaires pour votre type de sauvegarde.
 3. Lorsque vous attribuez des ressources, choisissez EC2. La sauvegarde Windows VSS n'est actuellement prise en charge que pour les EC2 instances.
 4. Dans la section Paramètres avancés, choisissez Windows VSS. Cela vous permet d'effectuer des sauvegardes Windows VSS cohérentes avec les applications.
 5. Créez votre sauvegarde.

Une tâche de sauvegarde dont le statut est `Completed` ne garantit pas la réussite de la partie VSS ; l'inclusion de VSS se fait dans la mesure du possible. Procédez comme suit pour déterminer si une sauvegarde est cohérente avec les applications, si elle résiste aux pannes ou si elle a échoué :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sous Mon compte dans le menu de navigation de gauche, cliquez sur Tâches.
3. Un statut `Completed` indique une tâche réussie cohérente par rapport aux applications (VSS).

Un statut `Completed with issues` indique que l'opération VSS a échoué, de sorte que seule une sauvegarde en cas de panne a réussi. Ce statut comportera également un message contextuel `"Windows VSS Backup Job Error encountered, trying for regular backup"`.

En cas d'échec de la sauvegarde, le statut sera `Failed`.

4. Pour afficher des informations supplémentaires sur la tâche de sauvegarde, cliquez sur la tâche individuelle. Par exemple, les détails peuvent être `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Les sauvegardes compatibles VSS avec une cible autre que Windows ou un composant Windows non VSS dont la tâche est réussie seront cohérentes en cas de crash sans VSS.

Instances Amazon EC2 non prises en charge

Les types d' EC2 instances Amazon suivants ne sont pas pris en charge pour les sauvegardes Windows compatibles VSS, car il s'agit de petites instances susceptibles de ne pas effectuer la sauvegarde correctement.

- `t3.nano`
- `t3.micro`
- `t3a.nano`
- `t3a.micro`
- `t2.nano`
- `t2.micro`

Sauvegarde et copie de balises

Vous pouvez copier des sauvegardes Régions AWS sur plusieurs Comptes AWS sites, à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié pour la plupart des types de ressources, bien que les sauvegardes situées dans des niveaux de stockage à froid ou d'archivage ne puissent pas être copiées. Consultez [the section called “Disponibilité des fonctionnalités par ressource”](#) et [Chiffrement pour obtenir une copie de sauvegarde vers un autre compte ou Région AWS](#) pour plus de détails.

Vous pouvez également automatiser une séquence de copies entre comptes et entre régions pour la plupart des ressources prises en charge, à l'exception d'Amazon RDS et Aurora. Pour les instantanés Amazon RDS et Aurora, l'automatisation des copies entre comptes ou entre régions est AWS Backup uniquement prise en charge en fonction de la manière dont ces services créent leurs clés de chiffrement (la copie d'un instantané de cluster de bases de données multi-AZ n'est pas prise en charge).

Certains types de ressources disposent à la fois d'une fonctionnalité de sauvegarde continue et d'une copie entre régions et entre comptes. Lorsqu'une copie entre régions ou entre comptes d'une sauvegarde continue est réalisée, le point de restauration copié (sauvegarde) devient une sauvegarde instantanée (périodique) (non disponible pour tous les types de ressources prenant en charge les deux types de sauvegarde). Selon le [type de ressource](#), les instantanés peuvent être une copie incrémentielle ou une copie complète. PITR (Point-in-Time Restore) n'est pas disponible pour ces copies.

Important

Les copies conservent leur configuration source, y compris les dates de création et la période de conservation. La date de création fait référence à la date de création de la source, et non à la date de création de la copie. Vous pouvez annuler la période de conservation.

La configuration de la sauvegarde source copiée remplace le paramètre d'expiration de sa copie si la période de conservation des copies est définie sur Toujours dans la AWS Backup console (ou si la [DeleteAfterDays](#) valeur est définie sur -1 dans la demande d'API) ; en d'autres termes, une copie dont le paramètre de conservation est défini pour ne jamais expirer conservera la date d'expiration de son point de récupération source.

Si vous souhaitez que la copie de votre sauvegarde n'expire jamais, définissez vos sauvegardes source pour qu'elles n'expirent jamais ou spécifiez que votre copie expire 100 ans après sa création.

Réessayer de copier la tâche

AWS Backup met en œuvre la stratégie de nouvelle tentative suivante pour les tâches de copie : AWS Backup en cas d'erreur système, la tâche de copie entre dans une phase de nouvelle tentative qui dure 2 heures. Pendant ce temps, l'état de la tâche de copie reste CREATED inchangé pendant que le système tente régulièrement de lancer la tâche. Si la tâche démarre correctement dans cette fenêtre, elle passe à l'`RUNNING` état actuel.

Si les problèmes persistent au-delà de la période de réessai de 2 heures, l'équipe de AWS Backup service est automatiquement alertée. L'équipe enquête ensuite et résout tous les problèmes sous-jacents. Une fois la résolution résolue, ils réessaient manuellement la demande de copie, en s'assurant que les tâches de copie sont terminées comme demandé.

Le processus de nouvelle tentative d'une tâche de copie est différent du processus de nouvelle tentative d'une tâche de sauvegarde, qui utilise une fenêtre de démarrage définie avec des tentatives régulières jusqu'à la réussite ou à l'expiration. Le mécanisme de copie fournit un niveau de fiabilité supplémentaire en intégrant l'intervention directe de l'équipe de service en cas de problèmes persistants.

Table des matières

- [Création de copies de sauvegarde sur Régions AWS](#)
- [Création de copies de sauvegarde entre Comptes AWS](#)
- [Copier les balises sur les sauvegardes](#)

Création de copies de sauvegarde sur Régions AWS

En utilisant AWS Backup, vous pouvez copier des sauvegardes Régions AWS sur plusieurs à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. La réplication entre régions est particulièrement utile en cas d'exigences de continuité d'activité ou de conformité pour stocker les sauvegardes à une distance minimale de vos données de production. Pour un didacticiel vidéo, consultez [Managing cross-Region copies of backups](#).

Lorsque vous copiez une sauvegarde vers un nouveau Région AWS pour la première fois, AWS Backup copie la sauvegarde dans son intégralité. En général, si un service prend en charge les sauvegardes incrémentielles, les copies suivantes de cette sauvegarde Région AWS seront incrémentielles. AWS Backup chiffrera à nouveau votre copie à l'aide de la clé gérée par le client de votre coffre-fort de destination.

Amazon EBS constitue une exception, car la modification de l'état de chiffrement d'un instantané pendant une opération de copie [entraîne une copie complète \(et non incrémentielle\)](#).

Prérequis

- La plupart des ressources AWS Backup prises en charge prennent en charge la sauvegarde entre régions. Pour plus de détails, reportez-vous à la section [Disponibilité des fonctionnalités par ressource](#).

- La plupart des AWS régions prennent en charge la sauvegarde interrégionale. Pour plus de détails, reportez-vous à la section [Disponibilité des fonctionnalités par Région AWS](#).
- AWS Backup ne prend pas en charge les copies interrégionales destinées au stockage dans des niveaux froids.

Chiffrement des copies entre régions

Consultez la section [Chiffrement pour une copie de sauvegarde vers un autre compte ou Région AWS](#) pour plus de détails sur le fonctionnement du chiffrement pour les tâches de copie.

Considérations relatives à la copie entre régions avec des ressources spécifiques

Amazon RDS

Vous ne pouvez pas [copier un groupe d'options](#) dans un autre Région AWS. En cas de tentative, vous pouvez obtenir un message d'erreur, tel que « Le cliché nécessite un groupe d'options cible avec les options suivantes :... »

Vous devez saisir les mêmes groupes d'options dans la cible Région AWS lorsque vous créez une nouvelle copie interrégionale d'un instantané Amazon RDS.

Exécution d'une sauvegarde entre régions à la demande

Pour copier une sauvegarde existante à la demande

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Choisissez Coffres-forts de sauvegarde.
3. Choisissez le coffre-fort qui contient le point de récupération à copier.
4. Dans la section Sauvegardes, sélectionnez un point de récupération à copier.
5. À l'aide du bouton déroulant Actions, choisissez Copier.
6. Entrez les valeurs suivantes :

Copier vers la destination

Choisissez la destination Région AWS de la copie. Vous pouvez ajouter une nouvelle règle de copie par copie à une nouvelle destination.

Coffre-fort de sauvegarde de destination

Choisissez le coffre-fort de sauvegarde de destination pour la copie.

Transition vers le stockage à froid

Choisissez le moment où vous souhaitez transférer la copie de sauvegarde vers le stockage à froid. Les sauvegardes transférées vers un stockage à froid doivent y être stockées pendant un minimum de 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau [Disponibilité des fonctionnalités par ressource](#). L'expression de stockage à froid est ignorée pour les autres ressources.

Période de conservation

Spécifiez le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid.

Rôle IAM

Choisissez le rôle IAM à utiliser lors de la création de la copie. AWS Backup Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS Backup permet d'assumer le rôle. Si vous choisissez Par défaut et que le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle sera créé pour vous avec les autorisations appropriées.

7. Choisissez Copier.

Planification de la sauvegarde entre régions

Vous pouvez utiliser un plan de sauvegarde planifié pour copier des sauvegardes entre Régions AWS.

Pour copier une sauvegarde à l'aide d'un plan de sauvegarde planifié

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans Mon compte, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sur la page Créer un plan de sauvegarde, choisissez Créer un nouveau plan.
4. Pour Nom du plan de sauvegarde, entrez le nom de votre plan de sauvegarde.

5. Dans la section Configuration de règle de backup, ajoutez une règle de sauvegarde qui définit un calendrier de sauvegarde, une fenêtre de sauvegarde et des règles de cycle de vie. Vous pourrez ajouter d'autres règles de sauvegarde ultérieurement.
 - a. Pour Nom de la règle de sauvegarde, entrez un nom pour votre règle.
 - b. Pour Coffre de sauvegarde, choisissez un coffre-fort dans la liste. Les points de récupération pour cette sauvegarde seront enregistrés dans ce coffre-fort. Vous pouvez créer un nouveau coffre-fort de sauvegarde.
 - c. Pour Fréquence de sauvegarde, choisissez la fréquence à laquelle vous souhaitez effectuer des sauvegardes.
 - d. Pour les services prenant en charge le PITR, si vous souhaitez bénéficier de cette fonctionnalité, choisissez Activer les sauvegardes continues pour la point-in-time restauration (PITR). Pour obtenir une liste des services qui prennent en charge la PITR, consultez cette section du tableau [Disponibilité des fonctionnalités par ressource](#).
 - e. Pour Fenêtre de sauvegarde, choisissez Utiliser la fenêtre de sauvegarde par défaut – recommandé. Vous pouvez personnaliser la fenêtre de sauvegarde.
 - f. Pour Copier vers la destination, choisissez la Région AWS de destination de votre copie de sauvegarde. Votre sauvegarde sera copiée dans cette région. Vous pouvez ajouter une nouvelle règle de copie par copie à une nouvelle destination. Entrez ensuite les valeurs suivantes :

Copier dans le coffre-fort d'un autre compte

Ne désactivez pas cette option. Pour en savoir plus sur la copie entre comptes, voir [Création de copies de sauvegarde](#) entre comptes Comptes AWS

Coffre-fort de sauvegarde de destination

Choisissez le coffre-fort de sauvegarde dans la région de destination où AWS Backup vous copierez votre sauvegarde.

Si vous souhaitez créer un nouveau coffre-fort de sauvegarde pour une copie entre régions, choisissez Créer un coffre de backup. Entrez les informations dans l'assistant. Choisissez ensuite Créer un coffre de sauvegarde.

6. Choisissez Créer un plan.

Création de copies de sauvegarde entre Comptes AWS

Vous pouvez en AWS Backup sauvegarder plusieurs Comptes AWS à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. Utilisez une sauvegarde entre comptes si vous souhaitez copier en toute sécurité vos sauvegardes sur un ou plusieurs Comptes AWS sites de votre organisation pour des raisons opérationnelles ou de sécurité. Si votre sauvegarde d'origine est supprimée par inadvertance, vous pouvez copier la sauvegarde de son compte de destination vers son compte source, puis démarrer la restauration. Pour ce faire, vous devez disposer de deux comptes appartenant à la même organisation dans le service AWS Organizations . Pour plus d'informations, consultez [Didacticiel : Création et configuration d'une organisation](#) dans le Guide de l'utilisateur Organizations.

Dans votre compte de destination, vous devez créer un coffre-fort de sauvegarde. Vous attribuez ensuite une clé gérée par le client pour chiffrer les sauvegardes dans le compte de destination, ainsi qu'une politique d'accès basée sur les ressources pour autoriser l'accès AWS Backup aux ressources que vous souhaitez copier. Dans le compte source, si vos ressources sont chiffrées à l'aide d'une clé gérée par le client, vous devez partager cette clé gérée par le client avec le compte de destination. Vous pouvez ensuite créer un plan de sauvegarde et choisir un compte de destination faisant partie de votre unité organisationnelle dans AWS Organizations.

Lorsque vous copiez une sauvegarde sur plusieurs comptes pour la première fois, AWS Backup copie la sauvegarde dans son intégralité. En général, si un service prend en charge les sauvegardes incrémentielles, les copies suivantes de cette sauvegarde dans le même compte sont incrémentielles. AWS Backup chiffre à nouveau votre copie à l'aide de la clé gérée par le client de votre coffre-fort de destination.

Prérequis

- Avant de gérer les ressources sur plusieurs Comptes AWS AWS Backup entrées, vos comptes doivent appartenir à la même organisation dans le AWS Organizations service.
- La plupart des ressources prises en charge par AWS Backup prennent en charge la sauvegarde entre comptes. Pour plus de détails, reportez-vous à la section [Disponibilité des fonctionnalités par ressource](#).
- La plupart des AWS régions prennent en charge la sauvegarde entre comptes. Pour plus de détails, reportez-vous à la section [Disponibilité des fonctionnalités par Région AWS](#).
- AWS Backup ne prend pas en charge les copies entre comptes pour le stockage dans des niveaux froids.

Configuration de la sauvegarde entre comptes

De quoi avez-vous besoin pour créer des sauvegardes entre comptes ?

- Un compte source

Le compte source est le compte où résident vos AWS ressources de production et vos sauvegardes principales.

L'utilisateur du compte source lance l'opération de sauvegarde entre comptes. L'utilisateur ou le rôle du compte source doit disposer des autorisations d'API appropriées pour lancer l'opération. Les autorisations appropriées peuvent être la politique AWS gérée `AWSBackupFullAccess`, qui permet un accès complet aux AWS Backup opérations, ou une politique gérée par le client qui autorise des actions telles que `ec2:ModifySnapshotAttribute`. Pour plus d'informations sur les types de politiques, consultez [Politiques gérées par AWS Backup](#).

- Un compte de destination

Le compte de destination est le compte sur lequel vous souhaitez conserver une copie de votre sauvegarde. Vous pouvez choisir plusieurs comptes de destination. Le compte de destination doit se trouver dans la même organisation que le compte source dans AWS Organizations.

Vous devez « Autoriser » la stratégie d'accès `backup:CopyIntoBackupVault` à votre coffre-fort de sauvegarde de destination. L'absence de cette politique empêchera toute tentative de copie sur le compte de destination.

- Un compte de gestion dans AWS Organizations

Le compte de gestion est le compte principal de votre organisation, tel que défini par AWS Organizations, que vous utilisez pour gérer la sauvegarde entre comptes sur l'ensemble de vos Comptes AWS. Pour utiliser la sauvegarde entre comptes, vous devez également activer l'approbation de service. Après avoir activé l'approbation de service, vous pouvez utiliser n'importe quel compte de l'organisation comme compte de destination. Depuis votre compte de destination, vous pouvez choisir les coffres-forts à utiliser pour la sauvegarde entre comptes.

- Activation de la sauvegarde entre comptes dans la console AWS Backup

Pour plus d'informations sur la sécurité, consultez [Remarques de sécurité pour la sauvegarde entre comptes](#).

Pour utiliser la sauvegarde entre comptes, vous devez activer la fonctionnalité de sauvegarde entre comptes. Vous devez ensuite « Autoriser » la stratégie d'accès backup:CopyIntoBackupVault dans votre coffre-fort de sauvegarde de destination.

EC2 Offres Amazon [EC2 autorisées AMLs](#). Si ce paramètre est activé dans votre compte, ajoutez l'identifiant de votre compte source à votre liste d'autorisation. Dans le cas contraire, l'opération de copie échouera avec un message d'erreur, tel que « AML source introuvable dans la région ».

Activer la sauvegarde entre comptes

1. Connectez-vous à l'aide des informations d'identification AWS Organizations de votre compte de gestion. La sauvegarde entre comptes ne peut être activée ou désactivée qu'à l'aide de ces informations d'identification.
2. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
3. Dans Mon compte, choisissez Paramètres.
4. Pour Backup entre comptes, choisissez Activer.
5. Dans Coffres de sauvegarde, choisissez votre coffre-fort de destination.

Pour la copie entre comptes, le coffre source et le coffre de destination se trouvent dans des comptes différents. Passez au compte auquel appartient le compte de destination, si nécessaire.

6. Dans la section Stratégie d'accès, « Autorisez » backup:CopyIntoBackupVault. Par exemple, choisissez Ajouter des autorisations, puis Autoriser l'accès à un coffre de sauvegarde depuis l'organisation. Toute action entre comptes autre que backup:CopyIntoBackupVault sera rejetée.
7. Désormais, n'importe quel compte de votre organisation peut partager le contenu de son coffre-fort de sauvegarde avec n'importe quel autre compte de votre organisation. Pour de plus amples informations, veuillez consulter [Partage d'un coffre-fort de sauvegarde avec un autre compte AWS](#). Pour limiter les comptes autorisés à recevoir le contenu des coffres-forts de sauvegarde d'autres comptes, consultez [Configuration de votre compte en tant que compte de destination](#).

Planification d'une sauvegarde entre comptes

Vous pouvez utiliser un plan de sauvegarde planifié pour copier des sauvegardes entre Comptes AWS.

Pour copier une sauvegarde à l'aide d'un plan de sauvegarde planifié

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans Mon compte, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sur la page Créer un plan de sauvegarde, choisissez Créer un nouveau plan.
4. Pour Nom du plan de sauvegarde, entrez le nom de votre plan de sauvegarde.
5. Dans la section Configuration de règle de backup, ajoutez une règle de sauvegarde qui définit un calendrier de sauvegarde, une fenêtre de sauvegarde et des règles de cycle de vie. Vous pourrez ajouter d'autres règles de sauvegarde ultérieurement.

Pour Nom de la règle, entrez un nom pour votre règle.

6. Dans la section Planification, sous Fréquence, choisissez la fréquence à laquelle vous souhaitez que la sauvegarde soit effectuée.
7. Pour Fenêtre de sauvegarde, choisissez Utiliser la fenêtre de sauvegarde par défaut (recommandé). Vous pouvez personnaliser la fenêtre de sauvegarde.
8. Pour Coffre de sauvegarde, choisissez un coffre-fort dans la liste. Les points de récupération pour cette sauvegarde seront enregistrés dans ce coffre-fort. Vous pouvez créer un nouveau coffre-fort de sauvegarde.
9. Dans la section Générer une copie – facultatif, entrez les valeurs suivantes :

Région de destination

Choisissez la destination Région AWS de votre copie de sauvegarde. Votre sauvegarde sera copiée dans cette région. Vous pouvez ajouter une nouvelle règle de copie par copie à une nouvelle destination.

Copier dans le coffre-fort d'un autre compte

Basculez pour choisir cette option. L'option devient bleue lorsqu'elle est sélectionnée. L'option ARN du coffre externe apparaît.

ARN du coffre-fort externe

Entrez l'Amazon Resource Name (ARN) du compte de destination. L'ARN est une chaîne qui contient l'identifiant du compte et son Région AWS. AWS Backup copiera la sauvegarde dans le coffre-fort du compte de destination. La liste Région de destination est automatiquement mise à jour en fonction de la région dans l'ARN du coffre-fort externe.

Pour Autoriser l'accès au coffre de sauvegarde, choisissez Autoriser. Choisissez ensuite Autoriser dans l'assistant qui s'ouvre.

AWS Backup a besoin d'autorisations pour accéder au compte externe afin de copier la sauvegarde à la valeur spécifiée. L'assistant présente l'exemple de politique suivant qui fournit cet accès.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

Transition vers le stockage à froid

Choisissez le moment pour effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d'expiration (suppression) de la copie. Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau [Disponibilité des fonctionnalités par ressource](#). L'expression de stockage à froid est ignorée pour les autres ressources.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid.

 Note

Lorsque les sauvegardes expirent et sont marquées pour suppression dans le cadre de votre politique de cycle de vie, AWS Backup supprime les sauvegardes à un moment choisi au hasard au cours des 8 heures suivantes. Cette fenêtre permet de garantir des performances constantes.

10. Choisissez Balises ajoutées à des points de récupération pour ajouter des balises à vos points de récupération.
11. Pour les paramètres de sauvegarde avancés, choisissez Windows VSS pour activer les instantanés compatibles avec les applications pour le logiciel tiers sélectionné qui s'exécute sur celui-ci. EC2
12. Choisissez Créer un plan.

Exécution d'une sauvegarde entre comptes à la demande

Vous pouvez copier une sauvegarde Compte AWS sur un autre à la demande.

Pour copier une sauvegarde à la demande

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Pour Mon compte, choisissez Coffre de sauvegarde pour voir tous vos coffres-forts de sauvegarde répertoriés. Vous pouvez filtrer en fonction du nom ou de la balise du coffre-fort de sauvegarde.
3. Choisissez l'ID de point de récupération de la sauvegarde que vous souhaitez copier.
4. Choisissez Copier.
5. Développez Détails de la sauvegarde pour voir les informations relatives au point de récupération que vous copiez.
6. Dans la section Copier la configuration, choisissez une option dans la liste Région de destination.
7. Choisissez Copier dans le coffre d'un autre compte. L'option devient bleue lorsqu'elle est sélectionnée.

8. Entrez l'Amazon Resource Name (ARN) du compte de destination. L'ARN est une chaîne qui contient l'identifiant du compte et son Région AWS. AWS Backup copiera la sauvegarde dans le coffre-fort du compte de destination. La liste Région de destination est automatiquement mise à jour en fonction de la région dans l'ARN du coffre-fort externe.
9. Pour Autoriser l'accès au coffre de sauvegarde, choisissez Autoriser. Choisissez ensuite Autoriser dans l'assistant qui s'ouvre.

Pour créer la copie, il AWS Backup faut des autorisations pour accéder au compte source. L'assistant affiche un exemple de politique qui fournit cet accès. Cette politique est présentée ci-après.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountCopyIntoBackupVault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

10. Pour Transition vers le stockage à froid, choisissez le moment pour effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d'expiration (suppression) de la copie. Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau [Disponibilité des fonctionnalités par ressource](#). L'expression de stockage à froid est ignorée pour les autres ressources.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid.

11. Pour Rôle IAM, spécifiez le rôle IAM (tel que le rôle par défaut) autorisé à rendre votre sauvegarde disponible pour une copie. L'acte de copie est effectué par le rôle lié au service de votre compte de destination.
12. Choisissez Copier. Selon la taille de la ressource que vous copiez, ce processus peut prendre plusieurs heures. Une fois la tâche de copie terminée, vous verrez la copie dans l'onglet Tâches de copie du menu Tâches.

Clés de chiffrement et copies entre comptes

Consultez la section [Chiffrement pour une copie de sauvegarde vers un autre compte ou Région AWS](#) pour plus de détails sur le fonctionnement du chiffrement pour les tâches de copie.

Pour obtenir de l'aide supplémentaire pour résoudre les problèmes de copie entre comptes, consultez le [centre de AWS connaissances](#).

Restaurer une sauvegarde de l'un Compte AWS à l'autre

AWS Backup ne prend pas en charge la récupération de ressources de l'un Compte AWS à l'autre. Toutefois, vous pouvez copier une sauvegarde d'un compte vers un autre, puis la restaurer dans ce compte. Par exemple, vous ne pouvez pas restaurer une sauvegarde du compte A vers le compte B, mais vous pouvez copier une sauvegarde du compte A vers le compte B, puis la restaurer dans le compte B.

La restauration d'une sauvegarde d'un compte à un autre est un processus en deux étapes.

Pour restaurer une sauvegarde d'un compte à un autre

1. Copiez la sauvegarde de la source Compte AWS vers le compte sur lequel vous souhaitez effectuer la restauration. Pour obtenir des instructions, consultez [Configuration de la sauvegarde entre comptes](#).
2. Suivez les instructions appropriées à votre ressource pour restaurer la sauvegarde.

Partage d'un coffre-fort de sauvegarde avec un autre compte AWS

AWS Backup vous permet de partager un coffre-fort de sauvegarde avec un ou plusieurs comptes, ou avec l'ensemble de votre organisation AWS Organizations. Vous pouvez partager un coffre-fort de sauvegarde de destination avec un compte AWS source, un utilisateur ou un rôle IAM source.

Pour partager un coffre-fort de sauvegarde de destination

1. Choisissez AWS Backup, puis Coffres de sauvegarde.
2. Choisissez le nom du coffre-fort de sauvegarde que vous souhaitez partager.
3. Dans le volet Stratégie d'accès, choisissez le menu déroulant Ajouter des autorisations.
4. Choisissez Autoriser l'accès au niveau du compte à un coffre de sauvegarde. Vous pouvez également choisir d'autoriser l'accès au niveau de l'organisation ou au niveau du rôle.
5. Entrez l'AccountID du compte que vous souhaitez partager avec ce coffre-fort de sauvegarde de destination.
6. Choisissez Enregistrer la stratégie.

Vous pouvez utiliser les politiques IAM pour partager votre coffre-fort de sauvegarde.

Partage d'un coffre-fort de sauvegarde de destination avec un Compte AWS ou un rôle IAM

La politique suivante partage un coffre-fort de sauvegarde avec un compte numéro 444455556666 et le rôle IAM SomeRole dans le compte numéro 111122223333.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action": "backup:CopyIntoBackupVault",
    }
  ]
}
```

```

    "Resource": "*"
  }
]
}

```

Partagez un coffre-fort de sauvegarde de destination dans lequel une unité organisationnelle AWS Organizations

La politique suivante partage un coffre-fort de sauvegarde avec les unités organisationnelles qui utilisent leur `PrincipalOrgPaths`.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
          ]
        }
      }
    }
  ]
}

```

Partagez un coffre-fort de sauvegarde de destination avec une organisation dans AWS Organizations

La politique suivante partage un coffre-fort de sauvegarde avec l'organisation portant l'`PrincipalOrgID` « o-a1b2c3d4e5 ».

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": [
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Configuration de votre compte en tant que compte de destination

Lorsque vous activez pour la première fois les sauvegardes entre comptes à l'aide de votre compte de AWS Organizations gestion, tout utilisateur d'un compte membre peut configurer son compte comme compte de destination. Nous vous recommandons de définir une ou plusieurs des politiques de contrôle des services suivantes (SCPs) AWS Organizations afin de limiter vos comptes de destination. Pour en savoir plus sur l'attachement de politiques de contrôle des services aux AWS Organizations nœuds, consultez la section [Attacher et détacher des politiques de contrôle des services](#).

Limitation des comptes de destination à l'aide de balises

Lorsqu'elles sont associées à une AWS Organizations racine, une unité d'organisation ou un compte individuel, cette politique limite les destinations de copies de cette racine, de cette unité d'organisation ou de ce compte aux seuls comptes dotés de coffres-forts de sauvegarde que vous avez marqués `DestinationBackupVault`. L'autorisation `"backup:CopyIntoBackupVault"` contrôle le comportement d'un coffre-fort de sauvegarde et, dans ce cas, les coffres-forts de sauvegarde de destination valides. Utilisez cette politique, ainsi que la balise correspondante

appliquée aux coffres-forts de destination approuvés, pour contrôler les destinations des copies entre comptes uniquement vers les comptes approuvés et les coffres-forts de sauvegarde.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/DestinationBackupVault": "true"
        }
      }
    }
  ]
}
```

Limitation des comptes de destination à l'aide de numéros de compte et de noms de coffres

Lorsqu'elles sont associées à une AWS Organizations racine, une unité d'organisation ou un compte individuel, cette politique limite les copies provenant de cette racine, de cette unité d'organisation ou de ce compte à deux comptes de destination uniquement. L'autorisation "backup:CopyFromBackupVault" contrôle le comportement d'un point de récupération dans le coffre-fort de sauvegarde et, dans ce cas, les destinations vers lesquelles vous pouvez copier ce point de récupération. Le coffre-fort source n'autorisera les copies vers le premier compte de destination (112233445566) que si un ou plusieurs noms de coffre-fort de sauvegarde de destination commencent par cab-. Le coffre-fort source n'autorisera les copies vers le deuxième compte de destination (123456789012) que si la destination est le seul coffre-fort de sauvegarde nommé fort-knox.

Limitez les comptes de destination à l'aide d'unités organisationnelles dans AWS Organizations

Lorsque vous êtes connecté à une AWS Organizations racine ou à une unité d'organisation qui contient votre compte source, ou lorsqu'il est attaché à votre compte source, la politique suivante limite les comptes de destination aux comptes compris dans les deux cas spécifiés OUs.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "backup:CopyFromBackupVault",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringNotLike": {
          "backup:CopyTargetOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/ou-jkl0-awsdddddd/"
          ]
        }
      }
    }
  ]
}
```

Remarques de sécurité pour la sauvegarde entre comptes

Tenez compte des éléments suivants lors de l'exécution de sauvegardes entre comptes dans AWS Backup :

- Le coffre-fort de destination ne peut pas être le coffre-fort par défaut. Cela est dû au fait que le coffre-fort par défaut est chiffré avec une clé qui ne peut pas être partagée avec d'autres comptes.
- Les sauvegardes entre comptes peuvent continuer à s'exécuter pendant 15 minutes au maximum après avoir désactivé la sauvegarde entre comptes. Cela est dû à une cohérence à terme et peut entraîner le démarrage ou la fin de certaines tâches entre comptes, même après avoir désactivé la sauvegarde entre comptes.
- Si le compte de destination quitte l'organisation ultérieurement, ce compte conservera les sauvegardes. Pour éviter toute fuite de données potentielle, ajoutez une autorisation de refus à l'autorisation `organizations:LeaveOrganization` dans une politique de contrôle des services (SCP) attachée au compte de destination. Pour plus d'informations SCPs, voir [Supprimer un compte membre de votre organisation](#) dans le Guide de l'utilisateur des Organizations.

- Si vous supprimez un rôle de copie lors d'une copie entre comptes, vous ne pouvez pas annuler le partage des instantanés du compte source une fois la tâche de copie terminée. Dans ce cas, la tâche de sauvegarde se termine, mais le statut de la tâche de copie indique Impossible d'annuler le partage de l'instantané.

Copier les balises sur les sauvegardes

En général, AWS Backup copie les balises des ressources qu'il protège vers vos points de récupération. Pour plus d'informations sur la copie des balises lors d'une restauration, consultez [Copie de balises lors d'une restauration](#).

Par exemple, lorsque vous sauvegardez un EC2 volume Amazon, AWS Backup copie ses balises de ressources de groupe et individuelles dans l'instantané obtenu, sous réserve des conditions suivantes :

- Pour obtenir la liste des autorisations spécifiques aux ressources requises pour enregistrer les balises de métadonnées sur les sauvegardes, consultez [Autorisations requises pour affecter des balises aux sauvegardes](#).
- Les balises initialement associées à une ressource et les balises attribuées lors de la sauvegarde sont attribuées aux points de restauration stockés dans un coffre de sauvegarde, jusqu'à un maximum de 50 (il s'agit d'une AWS limitation). Les balises attribuées lors de la sauvegarde sont prioritaires et les deux jeux de balises sont copiés par ordre alphabétique.
- DynamoDB ne prend pas en charge l'attribution de balises aux sauvegardes, sauf si vous activez d'abord [Sauvegarde DynamoDB avancée](#).
- Les volumes Amazon EBS attachés aux EC2 instances Amazon sont des ressources imbriquées. Les balises des volumes Amazon EBS attachés aux EC2 instances Amazon sont des balises imbriquées. Si vous AWS Backup ne parvenez pas à copier les balises imbriquées, la tâche de sauvegarde échoue.
- Lorsqu'une EC2 sauvegarde Amazon crée un point de récupération d'image et un ensemble de snapshots, elle AWS Backup copie les balises dans l'AMI qui en résulte. Si AWS Backup vous ne parvenez pas à copier les balises des volumes associés à l' EC2 instance Amazon vers les instantanés qui en résultent, la tâche de sauvegarde échoue.

Si vous copiez votre sauvegarde vers une autre sauvegarde Région AWS, AWS Backup copie toutes les balises de la sauvegarde d'origine vers la destination Région AWS.

Suppression d'une sauvegarde

Nous vous recommandons de AWS Backup supprimer automatiquement les sauvegardes dont vous n'avez plus besoin en configurant votre cycle de vie lors de la création de votre plan de sauvegarde. Par exemple, si vous définissez le cycle de vie de votre plan de sauvegarde de manière à conserver vos points de restauration pendant un an, AWS Backup vous supprimerez automatiquement le 1er janvier 2022 les points de récupération créés le 1er janvier 2021 ou dans les heures qui ont suivi. (AWS Backup répartit ses suppressions de manière aléatoire dans les 8 heures suivant l'expiration du point de récupération afin de maintenir les performances.) Pour en savoir plus sur la configuration de votre politique de rétention du cycle de vie, consultez [Création d'un plan de sauvegarde](#).

Toutefois, vous pouvez souhaiter supprimer manuellement un ou plusieurs points de récupération. Par exemple :

- Vous avez des points de récupération EXPIRED. Ces points de restauration n'ont pas AWS Backup pu être supprimés automatiquement car vous avez supprimé ou modifié la politique IAM d'origine que vous avez utilisée pour créer votre plan de sauvegarde. Lorsqu'il AWS Backup a tenté de les supprimer, il n'était pas autorisé à le faire.

Des points de récupération expirés peuvent également être créés si un point de EC2 récupération Amazon EBS ou Amazon AWS géré est doté d'un Amazon EBS Snapshot Lock et n' AWS Backup est pas en mesure de terminer le processus de cycle de vie qui entraînerait normalement la suppression du point de récupération. Notez que ces points de récupération expirés peuvent être restaurés depuis la EC2 console et l'[API](#) Amazon ou depuis la console et l'[API](#) Amazon EBS.

Warning

Vous continuerez à enregistrer les points de récupération expirés sur votre compte. Cela peut augmenter vos coûts de stockage.

Après le 6 août 2021, le point de restauration cible AWS Backup sera affiché comme expiré dans son coffre-fort de sauvegarde. Vous pouvez passer votre souris sur le statut Expiré rouge pour afficher un message de statut contextuel expliquant pourquoi il n'a pas été possible de supprimer la sauvegarde. Vous pouvez également choisir Actualiser pour recevoir les informations les plus récentes.

- Vous ne souhaitez plus qu'un plan de sauvegarde fonctionne comme vous l'avez configuré. La mise à jour du plan de sauvegarde affecte les futurs points de récupération qu'il créera, mais

n'affecte pas le point de récupération déjà créé. Pour en savoir plus, consultez [Mise à jour d'un plan de sauvegarde](#).

- Vous devez effectuer un nettoyage après avoir terminé un test ou un didacticiel.

Suppression manuelle de sauvegardes

Pour supprimer manuellement des points de récupération

1. Dans le volet de navigation de la AWS Backup console, sélectionnez Backup vaults.
2. Sur la page Backup vaults (Coffres-forts de sauvegarde), choisissez le coffre-fort de sauvegarde dans lequel vous avez stocké les sauvegardes.
3. Choisissez les points de récupération, puis sélectionnez Actions, Supprimer.
4. 1. Si votre liste contient une sauvegarde continue, choisissez l'une des options suivantes. Chaque sauvegarde continue possède un point de récupération unique.
 - Supprimer définitivement mes données de sauvegarde ou Supprimer le point de récupération. En sélectionnant l'une de ces options, vous arrêtez les futures sauvegardes continues et supprimez également vos données de sauvegarde continue existantes.

Note

Consultez [Sauvegardes et point-in-time restauration continues \(PITR\)](#) les considérations relatives à la sauvegarde continue sur Amazon S3, Amazon RDS et Aurora.

- Conservez mes données de sauvegarde en continu ou dissociez le point de restauration. En sélectionnant l'une de ces options, vous arrêtez les futures sauvegardes continues, mais vous conservez vos données de sauvegarde continues existantes jusqu'à leur expiration, conformément à votre période de rétention.

Un point de restauration continue (sauvegarde) Amazon S3 dissocié restera dans son coffre de sauvegarde, mais son état passera à STOPPED.

2. Pour supprimer tous les points de récupération sélectionnés, tapez Supprimer, puis choisissez Supprimer les points de récupération.
3. AWS Backup commence à soumettre vos points de récupération pour suppression et affiche une barre de progression. Gardez l'onglet de votre navigateur ouvert et ne quittez pas cette page pendant le processus de soumission.

4. À la fin du processus de soumission, vous AWS Backup présente un statut dans la bannière. Le statut peut être :
 - Soumis avec succès. Vous pouvez choisir Afficher la progression du statut de suppression de chaque point de récupération.
 - Échec de l'envoi. Vous pouvez choisir Afficher la progression du statut de suppression de chaque point de récupération ou Réessayer votre soumission.
 - Un résultat mitigé : certains points de récupération ont été soumis avec succès alors que d'autres points de récupération n'ont pas été soumis.
5. Si vous choisissez Afficher la progression, vous pouvez consulter l'État de la suppression de chaque sauvegarde. Si un statut de suppression est Échec ou Expiré, vous pouvez cliquer sur ce statut pour en connaître la raison. Vous pouvez également choisir de Réessayer les suppressions qui ont échoué.

Résolution des problèmes liés aux suppressions manuelles

Dans de rares cas, il se peut que votre demande de suppression ne soit pas traitée. AWS Backup utilise le rôle lié au service [AWSServiceRoleForBackup](#) pour effectuer des suppressions.

Si votre demande de suppression échoue, vérifiez que votre rôle IAM est autorisé à créer des rôles liés à un service. Plus précisément, vérifiez que votre rôle IAM possède l'action `iam:CreateServiceLinkedRole`. Si ce n'est pas le cas, ajoutez cette autorisation au rôle utilisé pour créer une sauvegarde. L'ajout de cette autorisation permet AWS Backup d'effectuer des suppressions manuelles.

Si, une fois que vous avez confirmé l'action `iam:CreateServiceLinkedRole` pour votre rôle IAM, vos points de récupération sont toujours bloqués avec le statut `DELETING`, nous étudierons probablement votre problème. Terminez votre suppression manuelle avec les étapes suivantes :

1. Configurez un rappel pour revenir dans 2 à 3 jours.
2. Après 2 à 3 jours, vérifiez les points de suppression `EXPIRED` récents résultant de votre première opération de suppression manuelle.
3. Supprimez manuellement ces points de récupération `EXPIRED`.

Pour plus d'informations sur les rôles, consultez [Utilisation des rôles liés à un service](#) et [Ajout et suppression d'autorisations basées sur l'identité IAM](#).

Backup et modification des balises

Après avoir créé une sauvegarde à l'aide de AWS Backup, vous pouvez modifier le cycle de vie ou les balises de la sauvegarde. Le cycle de vie définit à quel moment une sauvegarde est transférée vers un stockage à froid et quand elle expire. AWS Backup effectue la transition et valide l'expiration des sauvegardes automatiquement, conformément au cycle de vie que vous définissez.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau [Disponibilité des fonctionnalités par ressource](#). L'expression de stockage à froid est ignorée pour les autres ressources.

Note

La modification des balises d'une sauvegarde à l'aide de la AWS Backup console n'est prise en charge que pour les sauvegardes des systèmes de fichiers Amazon Elastic File System (Amazon EFS) et Amazon DynamoDB Advanced.

Les balises qui ont été ajoutées au point de récupération lors de la création d'autres ressources apparaîtront toujours, mais elles seront grisées et ne seront pas modifiables.

Même si ces balises ne sont pas modifiables dans la AWS Backup console, vous pouvez modifier les balises des sauvegardes de ces autres services à l'aide de la console ou de l'API du service.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Lorsque vous mettez à jour le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) », la valeur doit être au minimum l'âge de la sauvegarde plus une journée. Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Voici un exemple de mise à jour du cycle de vie d'une sauvegarde.

Pour modifier le cycle de vie d'une sauvegarde

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).

3. Dans la section Backups (Sauvegardes), choisissez une sauvegarde.
4. Sur la page des détails de la sauvegarde, choisissez Edit (Modifier).
5. Configurez les paramètres du cycle de vie, puis choisissez Save (Enregistrer).

Recherche de sauvegardes

Aperçu

Avec AWS Backup, vous pouvez créer des sauvegardes, également appelées points de restauration, des AWS ressources. Vous pouvez rechercher des sauvegardes de certains types de ressources, tels qu'Amazon S3 et Amazon EBS, ainsi que des éléments et des fichiers au sein de ces sauvegardes à l'aide de la AWS Backup console ou de la ligne de commande.

AWS Backup vous permet de rechercher dans les métadonnées de vos sauvegardes des types de ressources pris en charge de manière granulaire des fichiers ou des objets correspondant aux propriétés que vous avez définies dans votre recherche, telles que la taille, la date de création et le type de ressource. Vous pouvez aller encore plus loin en définissant les propriétés des éléments que vous souhaitez localiser.

Créez d'abord un index de sauvegarde que vous souhaitez inclure dans une future recherche. La création d'index de sauvegarde peut être automatisée par le biais d'un plan de sauvegarde ou vous pouvez en créer un manuellement pour n'importe quel point de restauration existant. Lorsque vous êtes prêt à effectuer une recherche, définissez les propriétés de sauvegarde et d'élément que vous souhaitez voir apparaître dans les résultats de recherche. Vous pouvez éventuellement restaurer la sauvegarde ou l'élément que vous avez recherché lors de la recherche.

Ce document décrit les étapes à suivre pour créer un index de sauvegarde, rechercher des sauvegardes indexées, effectuer une restauration à partir des résultats de recherche et résoudre les problèmes liés à l'index et aux fonctions de recherche dans AWS Backup.

Cas d'utilisation pour les index de sauvegarde et la recherche

Vous êtes peut-être un administrateur qui souhaite récupérer un fichier ou un objet spécifique. Au lieu d'identifier ou de deviner manuellement quelles sauvegardes contiennent les données, vous pouvez effectuer une recherche dans les métadonnées de vos points de restauration et restaurer la sauvegarde, les fichiers ou les objets exacts dont vous avez besoin.

Restaurer une sauvegarde complète juste pour trouver l'élément spécifique qui pourrait s'y trouver peut prendre des heures, voire des jours. Au lieu de cela, grâce à une recherche de sauvegarde, vous pouvez rechercher et restaurer uniquement le fichier ou l'objet dont vous avez besoin.

Les recherches de sauvegarde sont utiles pour les administrateurs de sauvegarde, les opérateurs de sauvegarde, les propriétaires de données et les autres professionnels de l'informatique qui interagissent avec la sauvegarde, la restauration et la conformité des données.

Accès

Avant de créer un index et une recherche, votre compte doit disposer des autorisations requises pour les opérations.

Autorisations d'index

Pour les opérations d'indexation, AWS Backup les authentications sont basées sur le rôle IAM, et non sur les informations d'identification de l'utilisateur (pour les spécificités de l'utilisateur IAM et du rôle IAM, voir). [Authentification](#)

Les autorisations suivantes sont requises pour créer un index d'une sauvegarde EBS. Ces autorisations sont contenues dans la politique gérée [AWSBackupServiceRolePolicyForIndexing](#):

- `ec2:DescribeSnapshots`
- `ebs:ListSnapshotBlocks`
- `ebs:GetSnapshotBlock`
- `kms:Decrypt`

Aucune autorisation d'index n'est requise pour créer un index S3.

Autorisations de recherche

Les autorisations suivantes sont requises pour créer une recherche. Ces autorisations sont contenues dans la politique gérée [AWSBackupSearchOperatorAccess](#):

- `backup:ListIndexedRecoveryPointsForSearch`
- `backup:SearchRecoveryPoint`

Si vous choisissez de chiffrer les résultats de recherche à l'aide d'une AWS KMS clé gérée par le client, assurez-vous que les autorisations suivantes figurent dans la clé :

- `kms:GenerateDataKey`
- `kms:Decrypt`

Flux de processus

Une recherche de sauvegarde comporte trois étapes, plus une quatrième étape de restauration facultative lorsque vous souhaitez restaurer les éléments renvoyés lors de votre recherche.

Indexez vos sauvegardes : activez l'indexation dans vos plans de sauvegarde ou créez manuellement un index de sauvegarde via la console ou la CLI pour chaque sauvegarde existante (point de restauration) pour laquelle vous souhaitez être éligible aux recherches.

Rechercher dans les métadonnées de sauvegarde un point de récupération, un fichier ou un objet : Spécifiez les propriétés des sauvegardes et des éléments que vous souhaitez rechercher dans votre recherche, par exemple dans vos compartiments S3 créés entre le 2 et le 6 avril avec des balises de `Administration` et pour des objets de plus de 100 Mo avec le nom de la clé contenant. `Admin`

Vérifiez les résultats de la recherche : si vous trouvez le point de récupération ou l'élément que vous recherchez, vous avez la possibilité de le restaurer. Si vous n'avez pas trouvé le point de récupération ou l'élément, vous pouvez affiner les propriétés de sauvegarde et les propriétés de l'élément, puis lancer une nouvelle recherche.

Restaurer des éléments spécifiques (facultatif) : Spécifiez les chemins de fichiers ou les éléments à restaurer, ainsi que les conditions de restauration.

Index des sauvegardes

Pour être consultable, une sauvegarde (point de restauration) doit d'abord avoir un index correspondant.

La création d'index de sauvegarde peut être activée dans un plan de sauvegarde afin que chaque future sauvegarde soit également associée à un index de sauvegarde. Vous pouvez également créer un index lors de la création d'une sauvegarde à la demande.

Vous pouvez également créer rétroactivement un index pour un point de récupération existant, soit à partir de l'écran détaillé du point de récupération Vault dans la AWS Backup console, soit via AWS CLI.

Les points de restauration des types de ressources pris en charge peuvent disposer d'un index de sauvegarde s'ils sont stockés dans un coffre de sauvegarde standard (les points de restauration d'un coffre-fort logique isolé ne prennent actuellement pas en charge les index de sauvegarde).

Indexes de sauvegarde S3

Une sauvegarde S3 peut être périodique, c'est-à-dire qu'elle est planifiée à intervalle fixe en fonction de votre plan de sauvegarde. Chaque fois qu'une sauvegarde périodique est créée, un index de sauvegarde est créé pour celle-ci. Une sauvegarde S3 peut également être continue, chaque modification de la sauvegarde étant enregistrée. Étant donné que de nombreuses modifications peuvent être apportées chaque jour, un seul index de sauvegarde est créé par jour pour une sauvegarde continue.

Le premier index de sauvegarde créé pour un point de restauration S3 continu est complet ; les index suivants pour le même point de restauration peuvent être incrémentiels.

Index de sauvegarde EBS

Chaque index de sauvegarde créé pour un point de restauration EBS est complet (et non incrémentiel).

AWS Backup tente de réparer automatiquement les problèmes liés aux snapshots lors de la création d'un index de sauvegarde. Si un système de fichiers était dans un état sale lors de la création du point de restauration, il AWS Backup tentera automatiquement de le restaurer. Si cette restauration échoue, la tâche de création d'index échouera également.

La nature de l'instantané détermine s'il peut être indexé :

Peut être indexé :

- Systèmes de fichiers : ext2, ext3, ext4, vfat, xfs et ntfs

Impossible d'indexer :

- Instantanés au niveau de l'archivage (stockage à froid)
- RAID et autres options de stockage multidisque
- Liens symboliques
- Liens physiques

Étapes de création d'un index de sauvegarde

Console

Ajoutez la création d'index de sauvegarde à votre plan de sauvegarde.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Backup plans sous Mon compte dans la barre de navigation de gauche.
3. Dans le volet Backup plans, sélectionnez le lien portant le nom du plan dans lequel vous souhaitez ajouter la création d'index.
4. Dans le deuxième volet Règles de sauvegarde, sélectionnez Ajouter une règle de sauvegarde.
5. Faites défiler l'écran vers le bas jusqu'au volet Backup indexes. Cochez la case à côté du ou des types de ressources pour lesquels vous souhaitez créer un index.

À chaque nouvelle sauvegarde créée par ce plan, un index correspondant à ce point de restauration sera également créé simultanément.

Création d'un index pour un point de récupération existant

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Vault dans la barre de navigation de gauche.
3. Sélectionnez le lien situé sous la colonne Nom du coffre-fort dans laquelle est stockée la sauvegarde dans laquelle vous souhaitez créer un index de sauvegarde.
4. Cochez le point de récupération pour lequel vous souhaitez créer un index de sauvegarde.
5. Sélectionnez le bouton Action, puis sélectionnez Créer un index.

Lors de la création de l'index, il aura le statut d'index de In progress. Une fois que le statut est passé à Available, le point de récupération peut être inclus dans une recherche.

Créez un index lorsque vous créez une sauvegarde à la demande.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Consultez les étapes de [Création d'une sauvegarde à la demande à l'aide de AWS Backup](#) création d'une sauvegarde à la demande à l'aide de AWS Backup.
3. Dans les paramètres, si vous avez choisi un type de ressource qui prend en charge l'indexation et la recherche, l'élément de ligne Backup search index sera affiché. Activez

l'option Créer un index de recherche de sauvegarde pour qu'un index soit créé en même temps que cette sauvegarde à la demande.

AWS CLI

Création d'un index de sauvegarde via la CLI

Utilisez la AWS CLI commande [create-backup-plan](#) pour créer un nouveau plan de sauvegarde. Vous pouvez également l'[update-backup-plan](#) utiliser pour modifier un plan existant.

Pour l'une ou l'autre opération `--backup-plan -rules`, incluez dans le paramètre `IndexActions`.

Consultez [IndexActions](#) le Guide [BackupRuleInput](#) de référence des AWS Backup API pour plus d'informations.

Une fois qu'un point de récupération possède un index, vous pouvez mettre à jour ses paramètres.

Exemple :

```
aws backup update-recovery-point-index-settings
--recovery-point-arn arn:aws:ec2:us-west-2::snapshot/snap-012345678901234567

--backup-vault-name [vaultname] //
--index ENABLED
--endpoint-url [URL]
--iam-role-arn arn:aws:iam::012345678901:role/Admin
```

Recherches

Une fois que vous avez une ou plusieurs sauvegardes avec un index, vous pouvez rechercher ces sauvegardes indexées via la AWS Backup console ou via AWS CLI.

Lorsque vous créez une recherche, vous sélectionnez un type de ressource. Les résultats renvoient uniquement les points de récupération contenant ce type, tels que des compartiments S3 ou des instantanés EBS.

Vous spécifiez ensuite les propriétés des sauvegardes (points de restauration) que vous souhaitez inclure dans la recherche. Vous pouvez spécifier jusqu'à 9 propriétés. Les types de propriétés inclus plusieurs fois renvoient des résultats correspondant à toutes les valeurs incluses.

Spécifiez les propriétés des éléments que vous souhaitez trouver dans les points de récupération renvoyés, notamment le nom du compartiment ou la taille du fichier. Affinez vos résultats en incluant plusieurs propriétés.

Si une valeur pour une propriété d'élément est incluse lorsque vous créez une recherche via la AWS Backup console, les résultats renverront uniquement les éléments correspondant à cette propriété d'élément (logique ET). Si vous répétez la même propriété d'élément, mais avec des valeurs différentes, les résultats renverront tous les éléments correspondant à l'une des valeurs incluses (logique OR). Par exemple, si vous incluez deux chemins de fichier EBS, tous les éléments des points de récupération inclus dans la recherche qui correspondent à l'un ou l'autre des chemins de fichier figureront dans les résultats de la recherche.

- Les propriétés des éléments S3 incluent l'heure de création, les Etags, la clé d'objet, la taille de l'objet et l'ID de version.
- Les propriétés des éléments EBS que vous pouvez utiliser pour filtrer votre recherche incluent l'heure de création, le chemin du fichier, l'heure de dernière modification et la taille.

Vous pouvez éventuellement inclure un identifiant de AWS KMS clé pour chiffrer vos résultats. Si aucune clé n'est incluse, AWS Backup utilisera une clé appartenant au service pour chiffrer les résultats.

Console

Rechercher des éléments dans vos sauvegardes

Il existe plusieurs chemins pour créer une recherche dans les sauvegardes indexées :

Vous pouvez trouver votre point de récupération préféré en accédant à Backup Vaults et en sélectionnant le point de récupération spécifique que vous souhaitez rechercher. Sélectionnez ensuite Rechercher. Vous pouvez également lancer une recherche depuis la page de détails du point de récupération.

Lors d'une restauration où vous souhaitez inclure des éléments spécifiques, vous pouvez effectuer des recherches dans vos sauvegardes afin de localiser les URL ou les chemins de fichiers contenant ces éléments.

Pour effectuer une recherche dans plusieurs sauvegardes, suivez les étapes suivantes :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à Rechercher dans le menu de navigation de gauche.
3. Sélectionnez Créer une recherche dans la section Historique des recherches.
4. Sélectionnez un type de ressource. Vous devez sélectionner un type de ressource pour chaque recherche. Si vous modifiez le type de ressource après avoir saisi des champs supplémentaires, vos entrées seront perdues et vous devrez les saisir à nouveau.
5. Choisissez entre 1 et 9 propriétés de sauvegarde pour affiner les points de restauration qui seront renvoyés lors de votre recherche.

AWS Backup analysera toutes vos sauvegardes contenant un index. Il ne renverra que les points de restauration correspondant à toutes les différentes propriétés de sauvegarde.

Par exemple `backup creation date = May 20, 2019 through May 23, 2019`,
`backup tag = "savings"` et inclusivement.

Vous pouvez inclure plusieurs valeurs de la même propriété, telles que trois balises différentes. Si la propriété est répétée avec des valeurs différentes, la recherche renverra tous les éléments correspondant à l'une des valeurs spécifiées (logique « OU »). Par exemple, `backup tag = "savings" backup tag = "checking"; backup creation date = May 20, 2019 through May 23, 2019, inclusif; et backup creation date = May 20, 2020 through May 23, 2020, inclusif`.

Une plage de dates de création de sauvegarde est considérée comme une propriété de sauvegarde. Une seule plage de dates de création de sauvegarde peut être incluse en tant que propriété de sauvegarde.

6. Choisissez entre 1 et 9 propriétés d'article pour affiner davantage les résultats de votre recherche.

Vous pouvez inclure plusieurs valeurs d'une même propriété. Si la propriété est répétée avec des valeurs différentes, la recherche renvoie tous les éléments correspondant à l'une des valeurs spécifiées.

7. Facultatif : pour chiffrer les résultats de votre recherche, vous pouvez spécifier une AWS KMS clé existante à l'aide du menu déroulant ou de l'ARN, ou vous pouvez créer une nouvelle clé KMS.
8. AWS Backup recommande de créer un nom de tâche de recherche unique.

9. Sélectionnez Lancer la recherche.

Un avertissement peut s'afficher indiquant que votre recherche peut inclure un grand nombre de points de récupération. La meilleure pratique consiste à revenir aux propriétés de sauvegarde et à sélectionner des critères supplémentaires pour affiner la recherche. La réduction du nombre de sauvegardes lors d'une recherche peut entraîner une baisse des coûts.

AWS CLI

Utilisez la AWS CLI commande [start-search-job](#).

Paramètres requis :

```
--search-scope // defines the backup properties you wish to include in the search
```

Paramètres facultatifs :

```
--client-token // string
--encryption-key-arn // if not included, AWS Backup uses service-owned key to
encrypt results
--item-filters // accepted keys and values depend on which resource type is included
in the search
--name // If not included, AWS Backup auto-assigns a name
```

Les filtres d'articles S3 acceptés sont les suivants :

```
--object-keys // string
--sizes // long condition
--creation-times // time condition
--version-ids // string
--etags // string
```

Les filtres d'articles EBS acceptés sont les suivants :

```
--file-paths //
--sizes //
--creation-times //
--last-modification-time //
```

Arrêter une recherche

Vous pouvez arrêter une tâche de recherche si elle est en statut `RUNNING`.

Une tâche de recherche se poursuit jusqu'à ce qu'elle atteigne le `COMPLETED` `FAILED` statut (ou le statut en cas d'erreur). Vous pouvez interrompre une tâche `RUNNING` de recherche si vous souhaitez mettre fin à une tâche de recherche en cours, ce qui peut être souhaitable si vous avez trouvé la sauvegarde ou l'élément que vous recherchiez avant la fin de la tâche.

- Dans la AWS Backup console, sélectionnez le bouton Arrêter la recherche d'une tâche.
- Dans la CLI, envoyez l'opération `stop-search-job` avec l'identifiant de tâche de recherche que vous souhaitez arrêter.

Résultats de la recherche

Une fois qu'une tâche de recherche a commencé, elle commence à agréger les résultats même si elle a un `Running` statut. Pendant qu'une tâche de recherche est en cours d'exécution et jusqu'à ce qu'elle soit terminée, des résultats partiels sont disponibles :

- Dans la console, les résultats s'affichent au fur et à mesure qu'ils sont extraits lors de la recherche. Les résultats ne sont pas actualisés automatiquement, mais vous pouvez consulter les derniers en sélectionnant le bouton d'actualisation. Pour afficher les résultats au-delà des 1 000 premiers éléments, sélectionnez Exporter les résultats.
- Les opérations de la CLI [get-search-job](#) et les statuts des tâches de recherche [list-search-jobs](#) renvoyées. Si le statut de la tâche est `RUNNING`, l'opération renvoie une liste incomplète.

Les résultats d'une tâche de recherche sont disponibles dans la console et via la CLI pendant 7 jours une fois la recherche arrêtée ou terminée. Pendant ce temps, vous pouvez exporter les résultats vers votre compartiment Amazon S3 préféré afin de pouvoir accéder aux résultats au-delà de cette période.

Chaque tâche de recherche contient des informations détaillées, disponibles dans la console ou via la CLI, notamment les points de récupération recherchés, le nom et le statut de la recherche, sa description, sa date et heure de création et d'achèvement, ainsi que des informations sur les objets ou éléments renvoyés ainsi que le nombre d'éléments et de points de récupération scannés.

Si les résultats ne contiennent pas le point de récupération, l'élément ou l'objet que vous recherchez, vous pouvez créer une nouvelle recherche avec des propriétés de sauvegarde et d'élément différentes. Chaque recherche est facturée individuellement.

Chaque type de ressource présente des considérations uniques en ce qui concerne les résultats de la recherche :

- Une recherche de points de récupération S3 ne renverra pas de marqueurs de suppression dans le résultat de la recherche, même si ces objets correspondent aux propriétés d'élément spécifiées dans la recherche.
- Les résultats d'une recherche EBS peuvent avoir une valeur nulle pour l'heure de création des systèmes de fichiers dans lesquels ce champ n'est pas pris en charge. Ces systèmes de fichiers peuvent inclure, sans toutefois s'y limiter, vfat, ext2/3 et les versions de XFS antérieures à la version 5.

Exporter les résultats de recherche vers un compartiment S3

AWS Backup conserve les résultats de recherche pendant 7 jours, à compter de l'heure et de la date d'achèvement. Ces résultats sont consultables dans la AWS Backup console ou peuvent être récupérés via l'opération CLI. `list-search-job-results`

Une bonne pratique consiste à exporter les résultats de recherche vers un compartiment S3 afin de conserver les résultats au-delà de la période de rétention de 7 jours. La tâche d'exportation créera un dossier nommé `Export Job ID` dans le compartiment que vous avez désigné, puis exportera les résultats vers ce dossier. Une fois que les résultats y sont exportés, ils sont disponibles tant que vous conservez le bucket.

Vous pouvez exporter les résultats de recherche de n'importe quel type de ressource pris en charge, et pas simplement d'une recherche S3.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à Offres d'emploi > Rechercher des offres d'emploi.
3. Sélectionnez les résultats de recherche d'emploi.
4. Cochez la case à côté du ou des résultats que vous souhaitez exporter.
5. Sélectionnez Exporter vers S3.

6. Choisissez le compartiment S3 de destination pour la tâche d'exportation.
7. Une fois que vous avez configuré tous les champs, sélectionnez Exporter.

L'action d'exportation crée une tâche d'exportation. Elles sont consultables dans Tâches > Exporter les tâches. Une fois qu'une tâche d'exportation a atteint le COMPLETED statut, les informations relatives aux résultats de recherche sont disponibles dans le compartiment S3 pour être récupérées ou téléchargées sous la forme d'un ou de plusieurs fichiers .csv.

AWS CLI

Utilisez la AWS CLI commande [start-search-result-export-job](#).

Paramètres requis :

```
--search-job-identifier  
--export-specification
```

Paramètres facultatifs :

```
--client-token  
--role-arn  
--tags
```

L'opération reviendra `ExportJobArn` et `ExportJobIdentifier`.

Utilisez [list-search-result-export-jobs](#) pour récupérer les statuts des tâches d'exportation.

Considérations relatives aux coûts et meilleures pratiques

Chaque création d'index de sauvegarde et chaque tâche de recherche entraînent des frais. Chaque index de sauvegarde est soumis à des frais de stockage. Chaque restauration à partir des résultats de recherche (comme toutes les autres tâches de restauration) est facturée. Pour en savoir plus, consultez [AWS Backup les tarifs](#).

Vous pouvez limiter les résultats renvoyés par une tâche de recherche en incluant plusieurs propriétés de sauvegarde et d'élément ; cela peut se traduire par un coût inférieur à celui d'une recherche couvrant tous les points de récupération possibles.

Restaurer à partir de la recherche

De nombreux clients choisissent d'effectuer des recherches dans leurs sauvegardes, ainsi que dans les objets ou fichiers qu'elles contiennent, pour trouver un point de restauration ou des éléments spécifiques à restaurer. Consultez [Restaurer une sauvegarde par type de ressource](#) pour plus d'informations sur les restaurations en général.

Vous pouvez effectuer une restauration à partir des résultats de recherche dans la AWS Backup console en accédant à Tâches > Rechercher des résultats de tâches > Restaurer. Pour effectuer une restauration AWS CLI complète, utilisez [start-restore-job](#) des métadonnées spécifiques au type de ressource, au point de récupération et aux éléments concernés par la restauration.

Consultez [Restaurez les données S3 à l'aide de AWS Backup](#) pour plus d'informations sur la façon de restaurer un point de récupération avec des données S3, de restaurer un compartiment S3 ou de restaurer jusqu'à cinq objets ou dossiers avec un compartiment S3.

Consultez [Restaurer un volume Amazon EBS](#) pour plus d'informations sur la restauration d'un instantané EBS sur un nouveau volume attaché à une EC2 instance.

Hiérarchisation des sauvegardes

Aperçu

AWS Backup propose un niveau de stockage à chaud à moindre coût pour les sauvegardes Amazon S3, qui permet de réduire les coûts de stockage à long terme jusqu'à 30 % tout en conservant des capacités de protection et de restauration de niveau professionnel. Le niveau économique offre les mêmes performances et fonctionnalités que le niveau de stockage à chaud. Vous pouvez configurer la hiérarchisation pour déplacer les données de sauvegarde S3 vers un stockage optimisé en fonction de l'âge des objets contenus dans vos coffres-forts de sauvegarde.

AWS Backup la hiérarchisation permet d'optimiser les coûts de stockage des données de sauvegarde S3 qui sont conservées pendant de longues périodes en raison de la conformité réglementaire, de la préparation aux sinistres et des stratégies de protection contre les ransomwares. Vous pouvez configurer la hiérarchisation pour toutes les sauvegardes S3 pour tous les coffres-forts d'un compte, ou créer des configurations ciblées pour des coffres-forts et des ressources protégées spécifiques.

Créez d'abord une configuration hiérarchisée qui spécifie quelles ressources S3 doivent être hiérarchisées et après combien de jours (minimum 60 jours). Les configurations de hiérarchisation

peuvent être automatisées pour s'appliquer à toutes les sauvegardes ou cibler des ressources spécifiques. Lorsque les données de sauvegarde atteignent le seuil d'âge spécifié, elles passent au niveau de stockage le moins coûteux tout en conservant des capacités de restauration identiques.

Ce document décrit les étapes à suivre pour créer des configurations de hiérarchisation, gérer les données de sauvegarde hiérarchisées, surveiller les économies de coûts et résoudre les problèmes liés à la fonction de hiérarchisation intégrée. AWS Backup

Important

Considérations financières relatives à la hiérarchisation des sauvegardes :

- La hiérarchisation des sauvegardes comporte trois éléments de coût : le niveau de stockage à chaud, le niveau de stockage à froid à faible coût et les coûts de transition. Lorsque les données de sauvegarde passent au niveau le moins coûteux, vous devrez payer des frais de transition uniques par objet, basés sur le nombre d'objets éligibles à la hiérarchisation.
- Pour les ensembles de données volumineux contenant de nombreux objets, les coûts de transition peuvent être importants au départ, mais ils sont généralement compensés par des économies de stockage continues pour les données conservées au-delà du seuil minimum de 60 jours.

Configurations de hiérarchisation

La hiérarchisation des sauvegardes S3 implique la création d'une configuration de hiérarchisation qui spécifie quelles ressources doivent être hiérarchisées et le nombre de jours avant la transition (minimum 60 jours) vers le niveau le moins coûteux. Pour permettre l'optimisation des coûts, les données de sauvegarde doivent être couvertes par une configuration hiérarchisée.

La création de configurations de hiérarchisation peut être configurée pour s'appliquer largement aux sauvegardes de toutes les ressources S3 de votre compte, ou ciblée sur des coffres-forts et des ressources spécifiques. Vous pouvez créer plusieurs configurations pour répondre aux différentes exigences en matière de conservation des données et d'optimisation des coûts.

Les configurations de hiérarchisation s'appliquent à la fois aux données de sauvegarde existantes dans les coffres-forts et aux nouvelles sauvegardes créées après l'établissement de la configuration.

Les configurations de hiérarchisation des sauvegardes S3 spécifient :

- Étendue des ressources : Toutes les ressources de tous les coffres, toutes les ressources d'un coffre spécifique ou des ressources individuelles sélectionnées. Une configuration hiérarchisée qui s'applique à tous les coffres-forts et à toutes les ressources est considérée comme la configuration par défaut.
- Délai de transition : 60 jours minimum avant le transfert des données vers le niveau le moins coûteux
- Affectation du coffre-fort : à quels coffres-forts de sauvegarde s'applique la configuration (pour tous les coffres-forts ou pour un nom de coffre-fort spécifique)
- Sélection des ressources : jusqu'à 5 règles de sélection de ressources différentes par configuration

Contraintes de configuration :

- Une configuration par coffre : chaque coffre ne peut avoir qu'une seule configuration hiérarchique en dehors de la configuration par défaut
- Maximum de 5 sélections de ressources : la configuration spécifique au coffre-fort prend en charge jusqu'à 5 groupes de ressources différents et les paramètres de hiérarchisation correspondants
- 100 ressources maximum : jusqu'à 100 ressources spécifiques dans tous les groupes de ressources peuvent être sélectionnées par configuration
- Priorité du coffre : s'il existe à la fois « tous les coffres-forts » et des configurations de coffres-forts spécifiques, c'est la configuration du coffre spécifique qui est prioritaire

Création de configurations de hiérarchisation

Création de configurations de hiérarchisation

Console

Pour créer une configuration hiérarchisée de tous les coffres-forts (par défaut)

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez S3 backup tiering.
3. Choisissez Create configuration (Créer une configuration).
4. Pour le nom de configuration, entrez un nom descriptif unique.
5. Choisissez Toutes les ressources S3 dans tous les coffres-forts.

6. Pour échelonner les paramètres en jours, entrez le nombre de jours (minimum 60) avant la transition des données vers le niveau le moins coûteux.
7. (Facultatif) Ajoutez des balises.
8. Choisissez Create configuration (Créer une configuration).

Pour créer une configuration de hiérarchisation de coffre-fort spécifique

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez S3 backup tiering.
3. Choisissez Create configuration (Créer une configuration).
4. Pour le nom de configuration, entrez un nom descriptif unique.
5. Choisissez les ressources S3 dans un coffre spécifique.
6. Pour sélectionner un coffre-fort, sélectionnez un coffre-fort de sauvegarde spécifique dans la liste déroulante.
7. Pour la sélection des ressources, choisissez l'une des options suivantes :
 - a. Toutes les ressources S3 de ce coffre-fort doivent s'appliquer à toutes les ressources S3 du coffre-fort
 - b. Ressources S3 spécifiques dans ce coffre pour sélectionner des compartiments S3 individuels
8. Si vous sélectionnez des ressources spécifiques :
 - a. Choisissez des ressources S3 individuelles (jusqu'à 100 au total pour tous les groupes de ressources d'une configuration)
 - b. Définissez les paramètres de hiérarchisation en jours pour chaque groupe de ressources
 - c. Choisissez Ajouter un paramètre de hiérarchisation pour créer des règles supplémentaires (jusqu'à 5 au total)
9. (Facultatif) Ajoutez des balises.
10. Choisissez Create configuration (Créer une configuration).

AWS CLI

Pour créer une configuration hiérarchisée de tous les coffres-forts (par défaut) à l'aide du AWS CLI

```
aws backup create-tiering-configuration \
--tiering-configuration '{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [{
    "Resources": ["*"],
    "TieringDownSettingsInDays": 60,
    "ResourceType": "S3"
  }]
}'
```

Gestion des configurations de hiérarchisation

Affichage des configurations de hiérarchisation

Vous pouvez consulter les configurations de hiérarchisation existantes via la AWS Backup console ou AWS CLI l'API REST.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez S3 backup tiering.
3. Consultez la liste des configurations avec leur étendue, leurs paramètres de transition et leur état.

AWS CLI

Pour répertorier toutes les configurations de hiérarchisation à l'aide du AWS CLI

```
aws backup list-tiering-configurations --max-results 50
```

Pour obtenir des informations spécifiques sur la configuration de la hiérarchisation

```
aws backup get-tiering-configuration --tiering-configuration-name "MyTieringConfig"
```

Modification des configurations de hiérarchisation

Vous pouvez mettre à jour les configurations de hiérarchisation existantes pour modifier le calendrier de transition, la sélection des ressources ou les affectations des coffres-forts.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez S3 backup tiering.
3. Sélectionnez la configuration à modifier.
4. Choisissez Modifier.
5. Mettez à jour les paramètres souhaités.
6. Pour les paramètres de hiérarchisation en jours, entrez le nombre de jours (minimum 60) avant la transition des données vers le niveau le moins coûteux.
7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour une configuration de hiérarchisation à l'aide du AWS CLI

```
aws backup update-tiering-configuration \  
--tiering-configuration-name "MyTieringConfig" \  
--tiering-configuration '{  
  "BackupVaultName": "*",  
  "ResourceSelection": [{  
    "Resources": ["*"],  
    "TieringDownSettingsInDays": 60,  
    "ResourceType": "S3"  
  }]  
'
```

Supprimer des configurations de hiérarchisation

Vous pouvez supprimer les configurations de hiérarchisation lorsqu'elles ne sont plus nécessaires.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez S3 backup tiering.
3. Sélectionnez la configuration à supprimer.

4. Sélectionnez Delete (Supprimer).
5. Entrez le nom de la configuration de hiérarchisation pour confirmer la suppression.
6. Choisissez Supprimer la configuration de hiérarchisation.

AWS CLI

Pour supprimer une configuration de hiérarchisation à l'aide du AWS CLI

```
aws backup delete-tiering-configuration \  
--tiering-configuration-name "MyTieringConfig"
```

Remarque : la suppression d'une configuration de hiérarchisation permet de conserver les données existantes dans le niveau le moins coûteux, mais empêche la hiérarchisation des nouvelles données.

Comment s'appliquent les configurations de hiérarchisation des sauvegardes S3

AWS Backup évalue les objets contenus dans les sauvegardes afin de hiérarchiser leur éligibilité en fonction de leur âge. Le service vérifie quotidiennement l'âge des objets et fait passer les objets éligibles au niveau le moins coûteux en fonction de vos paramètres de configuration. L'évaluation de la hiérarchisation s'effectue automatiquement en arrière-plan. Lorsque les objets d'une sauvegarde atteignent le seuil d'âge spécifié (minimum 60 jours), ils sont éligibles à la transition lors du cycle d'évaluation suivant.

Les objets des sauvegardes existantes et les objets de sauvegarde nouvellement créés sont soumis à des configurations de hiérarchisation. Si plusieurs configurations peuvent s'appliquer aux mêmes objets de sauvegarde, les paramètres spécifiques au coffre ont priorité sur les configurations applicables à tous les coffres-forts. Le processus de hiérarchisation est irréversible : une fois que les objets sont déplacés vers le niveau le moins coûteux, ils y restent jusqu'à ce que la sauvegarde soit supprimée conformément à vos politiques de rétention.

Structure des coûts et surveillance

Modèle de tarification

La hiérarchisation des sauvegardes S3 utilise une structure tarifaire optimisée en termes de coûts :

- Coût de stockage : coût inférieur par Go par mois par rapport au niveau chaud standard

- Frais de transition : frais uniques par objet lors du passage au niveau inférieur
- Coût de restauration : /Go de charge lors de la restauration des données, identique à celui de la restauration à chaud
- Pas de frais de récupération : Il n'y a pas de frais de récupération supplémentaires

Suivi des coûts

Surveillez les économies que vous avez réalisées sur les coûts de hiérarchisation grâce à :

- AWS Cost Explorer : types d'utilisation distincts pour chaque niveau de stockage
- AWS Rapports sur les coûts et l'utilisation : ventilation détaillée avec balises de répartition des coûts
- AWS Console de sauvegarde : informations de configuration

Exemple de réduction des coûts

Pour un compartiment S3 de 500 To contenant 1 milliard d'objets dont 60 % sont éligibles à la hiérarchisation :

- Avant l'échelonnement : 25 600 \$/mois
- Après la hiérarchisation : 21 000 \$/mois
- Économies mensuelles : 4 600\$ par mois (réduction de 18 %)
- Frais de transition uniques : 6 000\$

Exemples de configuration

Exemple 1 : hiérarchisation à l'échelle du compte

Appliquez la hiérarchisation à toutes les ressources S3 dans tous les coffres-forts de sauvegarde :

```
{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [
    {
      "Resources": ["*"],
      "TieringDownSettingsInDays": 60,

```

```

    "ResourceType": "S3"
  }
]
}

```

Exemple 2 :

Répartissez toutes les ressources dans un coffre à MyBackupVault 4 places :

```

{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "MyBackupVault4",
  "ResourceSelection": [
    {
      "Resources": ["*"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    }
  ]
}

```

Exemple 3 :

Des compartiments spécifiques à un niveau avec des règles différentes :

```

{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "MyBackupVault",
  "ResourceSelection": [
    {
      "Resources": ["arn:aws:s3:::mybucket1", "arn:aws:s3:::mybucket2"],
      "TieringDownSettingsInDays": 60,
      "ResourceType": "S3"
    },
    {
      "Resources": ["arn:aws:s3:::mybucket3"],
      "TieringDownSettingsInDays": 120,
      "ResourceType": "S3"
    }
  ]
}

```

Exemple 4 :

Définissez la règle pour ne pas hiérarchiser un bucket (définissez la hiérarchisation sur 36500) :

```
{
  "TieringConfigurationName": "MyTieringConfig",
  "BackupVaultName": "*",
  "ResourceSelection": [
    {
      "Resources": ["arn:aws:s3:::mybucket7", "arn:aws:s3:::mybucket8"],
      "TieringDownSettingsInDays": 36500,
      "ResourceType": "S3"
    }
  ]
}
```

Fonctions prises en charge et limitations

Fonctionnalités prises en charge

- Types de sauvegarde : sauvegardes continues et périodiques
- Types de coffres-forts : coffres-forts de sauvegarde standard et coffres-forts à espacement logique
- Vault lock : compatibilité totale avec les coffres-forts de sauvegarde verrouillés
- Entre régions/comptes : copie de données hiérarchisées (les copies atterrissent dans le niveau standard à destination)
- Capacités de restauration : Point-in-time restauration et restaurations au niveau des éléments
- Recherche et indexation : compatibilité totale avec la fonctionnalité de recherche de sauvegarde
- Conformité : Maintient toutes les capacités de conformité et d'audit

Limites

- Durée de transition minimale : 60 jours avant que les données puissent être déplacées vers un niveau moins coûteux
- Limite de ressources : jusqu'à 100 ressources spécifiques par configuration
- Limite de configuration : jusqu'à 5 règles de sélection de ressources différentes par configuration
- Une configuration par coffre-fort : chaque coffre-fort ne peut avoir qu'une seule configuration de hiérarchisation spécifique au coffre-fort, en plus de la configuration par défaut
- Transition unidirectionnelle : les données transférées vers un niveau moins coûteux y restent jusqu'à leur suppression

Résolution des problèmes

Problèmes courants

La configuration ne s'applique pas aux sauvegardes existantes

- Vérifiez que la configuration est correctement attribuée aux coffres-forts appropriés
- Vérifiez que les ressources sont correctement sélectionnées dans les configurations ciblées
- Assurez-vous que les données de sauvegarde répondent à l'âge minimum requis (60 jours)

`AlreadyExistsException` lors de la création de la configuration

- Assurez-vous que le nom de la configuration de hiérarchisation est unique dans votre compte
- Vérifiez si le coffre cible possède déjà une configuration de hiérarchisation active

Erreurs liées à `LimitExceededException`

- Vérifiez que vous n'avez pas dépassé le maximum de 5 groupes de sélection de ressources par configuration
- Vérifiez que vous n'avez pas sélectionné plus de 100 ressources spécifiques

Coûts de transition plus élevés que prévu

- Vérifiez le nombre d'objets en cours de transition
- Tenez compte de l'impact des frais de transition liés aux données qui changent fréquemment
- Évaluez si les paramètres de seuil minimum sont adaptés à votre cas d'utilisation

Restaurer une sauvegarde par type de ressource

Comment restaurer

Pour les instructions de restauration de la console et les liens vers la documentation pour chaque type de ressource AWS Backup pris en charge, consultez les liens au bas de cette page.

Pour restaurer une sauvegarde par programmation, utilisez l'opération d'API [StartRestoreJob](#).

Les valeurs de configuration (« restaurer des métadonnées ») dont vous avez besoin pour restaurer votre ressource varient en fonction de la ressource que vous souhaitez restaurer. Pour obtenir les métadonnées de configuration avec lesquelles votre sauvegarde a été créée, vous pouvez appeler [GetRecoveryPointRestoreMetadata](#). Les exemples de restauration de métadonnées sont également disponibles dans les liens au bas de cette page.

La restauration depuis le stockage à froid prend généralement 4 heures de plus que la restauration depuis un stockage à chaud.

Pour chaque restauration, une tâche de restauration est créée avec un ID de tâche unique, par exemple 1323657E-2AA4-1D94-2C48-5D7A423E7394.

Note

AWS Backup ne fournit aucun accord de niveau de service (SLAs) pour une durée de restauration. Les temps de restauration peuvent varier en fonction de la charge et de la capacité du système, même pour les restaurations contenant les mêmes ressources.

Restaurations non destructives

Lorsque vous AWS Backup restaurez une sauvegarde, une nouvelle ressource est créée avec la sauvegarde que vous restaurez. Cela permet d'empêcher votre activité de restauration de détruire vos ressources existantes.

Tests de restauration

Vous pouvez effectuer des tests sur vos ressources pour simuler une expérience de restauration. Cela permet de déterminer si vous atteignez l'objectif de durée de récupération (RTO) de votre organisation et de vous préparer aux futurs besoins de restauration.

Pour plus d'informations, consultez [Tests de restauration](#).

Copie de balises lors d'une restauration

Note

Cette fonctionnalité n'est actuellement pas disponible pour les restaurations d'Amazon DynamoDB, Amazon S3, SAP HANA sur les instances EC2 Amazon, les machines virtuelles et les ressources Amazon Timestream.

Introduction

Vous pouvez copier des balises lorsque vous restaurez une ressource si les balises appartenaient à la ressource protégée au moment de la sauvegarde. Les balises, qui sont des étiquettes contenant une paire clé-valeur, peuvent vous aider à identifier et à rechercher des ressources. Lorsque vous lancez une tâche de restauration, des balises appartenant aux ressources sauvegardées d'origine peuvent être ajoutées à la ressource en cours de restauration.

Le fait de choisir d'inclure des balises lors d'une tâche de restauration permet de réduire les frais et le travail liés à l'application manuelle de balises aux ressources une fois la tâche de restauration terminée. Notez que cela est différent de l'ajout de nouvelles balises aux ressources restaurées.

Lorsque vous restaurez une sauvegarde dans le flux de console, vos balises source sont copiées par défaut. Dans la console, décochez la case si vous ne souhaitez pas copier les balises vers une ressource restaurée.

Dans l'opération d'API `StartRestoreJob`, le paramètre `CopySourceTagsToRestoredResource` est défini sur `false` par défaut, ce qui exclut les balises source d'origine de la ressource que vous restaurez. Si vous souhaitez inclure des balises provenant de la source d'origine, définissez ce paramètre sur `True`.

Considérations

- Une ressource peut avoir jusqu'à 50 balises, y compris les ressources restaurées. Pour plus d'informations sur les limites des balises, consultez [Balisage de vos ressources AWS](#).
- Assurez-vous que les autorisations appropriées sont présentes dans le rôle utilisé pour les restaurations afin de copier des balises. Le rôle par défaut pour les restaurations contient les autorisations nécessaires. Un rôle personnalisé doit inclure des autorisations supplémentaires pour baliser les ressources.

- Les ressources suivantes ne sont actuellement pas prises en charge pour l'inclusion de balises de restauration : VMware Cloud™ on AWS, VMware Cloud™ on AWS Outposts, systèmes sur site, EC2 instances SAP HANA sur Amazon, Timestream, DynamoDB, Advanced DynamoDB et Amazon S3.
- Pour les sauvegardes continues, les balises de la ressource d'origine telles que celles de la sauvegarde la plus récente seront copiées sur la ressource restaurée.
- Les balises ne seront pas copiées pour les restaurations au niveau des éléments.
- Les balises qui ont été ajoutées à une sauvegarde une fois la tâche de sauvegarde terminée mais qui n'étaient pas présentes sur la ressource d'origine avant la sauvegarde ne seront pas copiées sur la ressource restaurée. Seules les sauvegardes créées après le 22 mai 2023 sont éligibles à la copie de balises lors de la restauration.

Interaction de balises avec des ressources spécifiques

- Amazon EC2
 - Les balises appliquées aux EC2 instances Amazon restaurées sont également appliquées aux volumes Amazon EBS restaurés joints.
 - Les balises appliquées aux volumes EBS attachés aux instances source ne sont pas copiées sur les volumes attachés aux instances restaurées. Si vous avez des politiques IAM qui autorisent ou refusent aux utilisateurs l'accès aux volumes EBS en fonction de leurs balises, vous devez réattribuer manuellement les balises requises aux volumes restaurés pour garantir que vos politiques restent en vigueur.
- Lorsque vous restaurez une ressource Amazon EFS, elle doit être copiée dans un nouveau système de fichiers. Les restaurations d'un système de fichiers existant ne peuvent pas contenir de balises copiées sur celui-ci.
- Amazon RDS
 - Si le cluster RDS qui a été sauvegardé est toujours actif, les balises de ce cluster seront copiées.
 - Si le cluster d'origine n'est plus actif, les balises de l'instantané du cluster seront copiées à la place.
 - Les balises présentes sur la ressource au moment de la sauvegarde seront copiées lors de la restauration, que le paramètre booléen pour `CopySourceTagsToRestoredResource` soit défini sur `True` ou `False`. Toutefois, si l'instantané ne contient pas de balises, le paramètre booléen ci-dessus sera utilisé.

- Par défaut, les clusters Amazon Redshift incluent toujours des balises lors d'une tâche de restauration.

Copie des balises via la console

1. Ouvrez la [console AWS Backup](#).
2. Dans le volet de navigation, choisissez Ressources protégées et sélectionnez l'ID de ressource Amazon S3 que vous voulez restaurer.
3. Sur la page Détails de la ressource, vous verrez une liste des points de récupération pour l'ID de ressource sélectionné. Pour restaurer une ressource :
 - a. Dans le volet Sauvegarde, choisissez l'ID du point de récupération de la ressource.
 - b. Dans le coin supérieur droit du volet, choisissez Restaurer (vous pouvez également accéder au coffre-fort de sauvegarde, rechercher le point de récupération, puis cliquer sur Actions, puis sur Restaurer).
4. Sur la page Restaurer la sauvegarde, recherchez le panneau intitulé Restaurer avec des balises. Pour inclure toutes les balises de la ressource d'origine, maintenez la case cochée (notez que cette case est cochée par défaut dans la console).
5. Cliquez sur Restaurer la sauvegarde après avoir sélectionné tous vos paramètres et rôles préférés.

Pour inclure des balises par programmation

Utilisez l'opération d'API `StartRestoreJob`. Assurez-vous que le paramètre booléen suivant est défini sur `True` :

```
CopySourceTagsToRestoredResource = true
```

Si le paramètre booléen est `CopySourceTagsToRestoredResource = True`, la tâche de restauration copiera les balises de la ou des ressources d'origine vers le matériel restauré.

Important

La tâche de restauration échouera si ce paramètre est inclus pour une ressource non prise en charge (systèmes sur site VMware AWS Outposts, SAP HANA sur les EC2 instances, Timestream, DynamoDB, Advanced DynamoDB et Amazon S3).


```
{
  "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
  "Metadata": {
    "InstanceInitiatedShutdownBehavior": "stop",
    "DisableApiTermination": "false",
    "EbsOptimized": "false",
    "InstanceType": "t1.micro",
    "SubnetId": "subnet-123ab456cd7efgh89",
    "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
    "Placement": "{\"GroupName\":null,\"Tenancy\": \"default\"}",
    "HibernationOptions": "{\"Configured\":false}",
    "IamInstanceProfileName": "UseBackedUpValue",
    "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
  },
  "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
  "ResourceType": "EC2",
  "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
  "CopySourceTagsToRestoredResource": true
}
```

Résolution des problèmes de restauration des balises

ERREUR : autorisations insuffisantes

SOLUTION : assurez-vous de disposer des autorisations nécessaires dans votre rôle de restauration afin de pouvoir inclure des balises sur votre ressource restaurée. La politique de rôle de service [AWS géré](#) par défaut pour [AWSBackupServiceRolePolicyForRestores](#) les restaurations contient les autorisations nécessaires pour cette tâche.

Si vous choisissez d'utiliser un rôle personnalisé, assurez-vous que les autorisations suivantes sont présentes :

- elasticfilesystem:TagResource
- storagegateway:AddTagsToResource
- rds:AddTagsToResource
- ec2:CreateTags
- cloudformation:TagResource

Pour plus d'informations, consultez [Autorisations d'API](#).

Statuts de la tâche de restauration

Vous pouvez afficher le statut d'une tâche de restauration sur la page Tâches de la console AWS Backup . Les statuts d'une tâche de restauration peuvent être en attente, en cours d'exécution, terminée, abandonnée et échec.

Rubriques

- [Restauration d'un cluster Amazon Aurora](#)
- [Restauration Amazon Aurora DSQL](#)
- [Restaurer les CloudFormation piles](#)
- [Restauration d'un cluster DocumentDB](#)
- [Restaurer une table Amazon DynamoDB](#)
- [Restaurer un volume Amazon EBS](#)
- [Restaurer une EC2 instance Amazon](#)
- [Restaurer un système de fichiers Amazon EFS](#)
- [Restaurer un cluster Amazon EKS](#)
- [Restaurer un système FSx de fichiers](#)
- [Restaurer un cluster Neptune](#)
- [Restaurer une base de données RDS](#)
- [Restauration d'un cluster Amazon Redshift](#)
- [Restauration sans serveur Amazon Redshift](#)
- [Restaurer une base de données SAP HANA sur une instance Amazon EC2](#)
- [Restaurez les données S3 à l'aide de AWS Backup](#)
- [Restaurer un volume Storage Gateway](#)
- [Restauration d'une table Amazon Timestream](#)
- [Restaurez une machine virtuelle à l'aide de AWS Backup](#)

Restauration d'un cluster Amazon Aurora

Utiliser la AWS Backup console pour restaurer les points de restauration Aurora

AWS Backup restaure votre cluster Aurora ; il ne crée ni n'attache d'instance Amazon RDS à votre cluster. Au cours des étapes suivantes, vous allez créer et associer une instance Amazon RDS à votre cluster Aurora restauré à l'aide de l'interface de ligne de commande.

Pour restaurer un cluster Aurora, vous devez spécifier plusieurs options de restauration. Pour plus d'informations sur ces options, consultez [Présentation de la sauvegarde et de la restauration d'un cluster de bases de données Aurora](#) dans le Guide de l'utilisateur Amazon Aurora. Les spécifications relatives aux options de restauration se trouvent dans le guide de l'API pour [RestoreDBClusterFromSnapshot](#).

Pour restaurer un cluster Amazon Aurora

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Aurora que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications d'instance, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Moteur de base de données, Version du moteur de base de données et Type de capacité.

Note

Si le type de capacité Sans serveur est sélectionné, un volet Paramètres de capacité apparaît. Spécifiez les valeurs des paramètres Unité de capacité Aurora minimale et Unité de capacité Aurora maximale ou choisissez des options différentes dans la section Configuration de dimensionnement supplémentaire.

5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de cluster de base de données que vous Compte AWS possédez dans la région actuelle.
6. Dans le volet Réseau et sécurité, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Cloud privé virtuel (VPC), Groupe de sous-réseaux et Zone de disponibilité.

7. Dans le volet Options de base de données, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Port de base de données, Groupe de paramètres de cluster DB et Authentification IAM DB activée.
8. Dans le volet Sauvegarde, acceptez la valeur par défaut ou spécifiez la valeur du paramètre Copier les balises dans les instantanés.
9. Dans le volet Retour sur trace, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le retour sur trace ou Désactiver le retour sur trace.
10. Dans le volet Chiffrement, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le chiffrement ou Désactiver le chiffrement.
11. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.
12. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
13. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

14. Une fois votre restauration terminée, attachez votre cluster Aurora restauré à une instance Amazon RDS.

À l'aide de la AWS CLI :

- Pour Linux, macOS ou Unix :

```
aws rds create-db-instance --db-instance-identifiant sample-instance \  
                           --db-cluster-identifiant sample-cluster --engine aurora-mysql --db-  
instance-class db.r4.large
```

- Pour Windows :

```
aws rds create-db-instance --db-instance-identifiant sample-instance ^  
                           --db-cluster-identifiant sample-cluster --engine aurora-mysql --db-  
instance-class db.r4.large
```

Consultez la section [Sauvegardes et point-in-time restaurations continues \(PITR\)](#) pour obtenir des informations sur les sauvegardes continues et la restauration à un moment donné.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon Aurora

Utilisez [StartRestoreJob](#). Les métadonnées que vous pouvez inclure pour une tâche de restauration dépendent du fait que vous restaurez une sauvegarde continue à un moment donné (PITR) ou que vous restaurez un instantané.

Restaurer un cluster à partir d'un instantané

Vous pouvez spécifier les métadonnées suivantes pour une tâche de restauration de snapshots Aurora. Consultez [RestoreDBClusterFromSnapshot](#) le manuel Amazon Relational Database Service API Reference pour obtenir des informations supplémentaires et des valeurs acceptées.

```
// Required metadata:
dbClusterIdentifier // string
engine // string

// Optional metadata:
availabilityZones // array of strings
backtrackWindow // long
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // array of strings
enableIAMDatabaseAuthentication // Boolean
engineMode // string
engineVersion // string
kmsKeyId // string
optionGroupName // string
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings
```

Exemple :

```
"restoreMetadata":{"EngineVersion":"5.6.10a","KmsKeyId":"arn:aws:kms:us-east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7","EngineMode":"serverless","AvailabilityZones":["us-east-1b","us-east-1e","us-east-1c"],"Port":3306,"DatabaseName":"","DBSubnetGroupName":"default-vpc-05a3b07cf6e193e1g","VpcSecurityGroupIds":["sg-012d52c68c6e88f00"],"ScalingConfiguration":{"MinCapacity":2,"MaxCapacity":64,
```

```
\\\\"AutoPause\\\\":true,\\\\"SecondsUntilAutoPause\\\\":300,\\\\"TimeoutAction\\\\":
\\\\"RollbackCapacityChange\\\\"}\\",\\\\"EnableIAMDatabaseAuthentication\\\\":\\\\"false\\",
\\\\"DBClusterParameterGroupName\\\\":\\\\"default.aurora5.6\\",\\\\"CopyTagsToSnapshot\\\\":\\\\"true\\",
\\\\"Engine\\\\":\\\\"aurora\\",\\\\"EnableCloudwatchLogsExports\\\\":\\\\"[]\\\"}"
```

Restaurer un cluster à un point dans le temps (PITR)

Vous pouvez spécifier les métadonnées suivantes lorsque vous souhaitez restaurer une sauvegarde continue Aurora (point de restauration) à un moment précis (PITR). Consultez [RestoreDBClusterToPointInTime](#) le manuel Amazon Relational Database Service API Reference pour obtenir des informations supplémentaires et des valeurs acceptées.

```
// Required metadata:
dbClusterIdentifier // string
engine // string
restoreToTime // timestamp; must be specified if UseLatestRestorableTime parameter
isn't provided

// Optional metadata:
backtrackWindow // long
copyTagsToSnapshot // Boolean
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // array of strings
enableIAMDatabaseAuthentication // Boolean
engineMode // string
engineVersion // string
kmsKeyId // string
optionGroupName // string
port // integer
scalingConfiguration // object
vpcSecurityGroupIds // array of strings
```

Restauration Amazon Aurora DSQL

Rubriques

- [Aperçu](#)
- [Restaurer un cluster de région unique Aurora DSQL](#)
- [Restaurer un cluster multirégional Aurora DSQL](#)
- [Résoudre les problèmes de restauration d'Aurora SQL](#)

- [Questions fréquemment posées sur la restauration d'Aurora DSQL](#)

Aperçu

Pour restaurer un cluster Amazon Aurora DSQL à région unique, utilisez la AWS Backup console ou la CLI pour sélectionner le point de restauration (sauvegarde) que vous souhaitez restaurer. Pour restaurer un cluster multirégional Aurora DSQL, vous pouvez désormais utiliser la AWS Backup console ou la CLI.

Pour une restauration à région unique, incluez le nom, le chiffrement du cluster et la protection contre la suppression, puis lancez la restauration sur un cluster nouvellement créé.

Pour une restauration multirégionale, vous devez spécifier des paramètres supplémentaires, notamment une région témoin, une ou plusieurs régions homologues et des paramètres de configuration régionaux. La restauration multirégionale crée un cluster qui s'étend sur plusieurs régions AWS, offrant ainsi une disponibilité améliorée et des capacités de reprise après sinistre.

Restaurer un cluster de région unique Aurora DSQL

Vous pouvez restaurer un cluster Aurora DSQL dans une seule région à l'aide de la AWS Backup console ou AWS CLI.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez le bouton « Restaurer » à côté du point de récupération que vous souhaitez restaurer.
3. Configurez les paramètres du nouveau cluster sur lequel votre point de récupération sera restauré.
 - a. Par défaut, l'AMK (clé AWS gérée) sera utilisée pour chiffrer les données restaurées. Vous pouvez également spécifier une autre clé.
 - b. [La protection contre la suppression](#) de vos clusters Aurora est activée par défaut, mais décochez la case pour désactiver cette option.
4. Vérifiez les paramètres ; lorsqu'ils sont satisfaisants, cliquez sur le bouton Restaurer la sauvegarde.

AWS Backup créera un nouveau cluster Aurora DSQL.

AWS CLI

Restauration d'une seule région

1. Utilisez la commande CLI `aws backup start-restore-job` pour restaurer un cluster Aurora à partir du point de restauration spécifié.
2. Incluez les métadonnées nécessaires à la tâche de restauration. Exemple :

Exemple

```
aws backup start-restore-job \
  --recovery-point-arn "arn:aws:dsql:us-east-1:123456789012:cluster/example-
cluster/backup/example-backup" \
  --iam-role-arn "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole" \
  --metadata '{"regionalConfig":[{"region\":\"us-east-1\",
\"isDeletionProtectionEnabled\":true,\"kmsKeyId\":\"my_key\"}]}' \
  --copy-source-tags-to-restored-resource
```

Restaurer un cluster multirégional Aurora DSQL

La restauration d'un cluster multirégional Aurora DSQL s'effectue au sein d'un triplet de régions fermé, qui est un groupe de trois homologues. Régions AWS La restauration multirégionale nécessite que les régions que vous spécifiez dans l'opération soient contenues dans un triplet. Pour plus d'informations sur les clusters multirégionaux, voir [Configuration des clusters multirégionaux](#).

Les triplets des groupes suivants sont pris en charge. Lorsqu'il y a plus de régions, choisissez-en trois dans le même groupe.

- USA Est (Virginie du Nord) ; USA Est (Ohio) ; USA Ouest (Californie du Nord)
- Europe (Irlande) ; Europe (Londres) ; Europe (Paris) ; Europe (Francfort)
- Asie-Pacifique (Tokyo) ; Asie-Pacifique (Séoul) ; Asie-Pacifique (Osaka)

Pour terminer la restauration multirégionale, assurez-vous de disposer des autorisations suivantes :

- `backup:StartRestoreJob`
- `dsql:UpdateCluster`

- `dsql:AddPeerCluster`
- `dsql:RemovePeerCluster`

Vous pouvez restaurer une sauvegarde d'un cluster Aurora DSQL dans plusieurs régions à l'aide de la AWS Backup console ou des commandes de la CLI.

 Tip

Si vous disposez d'un plan de sauvegarde avec une règle qui crée automatiquement une copie interrégionale vers l'une des régions indiquées, la copie créée peut être utilisée pour cette restauration multirégionale.

La restauration multirégionale commence par votre région actuelle. Vous aurez également besoin d'un :

- Région homologue avec une copie interrégionale identique du point de récupération de votre région actuelle
- Région témoin, une région désignée Région AWS qui participe aux configurations de clusters multirégionaux en prenant en charge les écritures dans le journal des transactions uniquement sans consommer de stockage pour les données réelles. Pour plus d'informations sur les régions témoins, consultez la section [Création d'un cluster multirégional](#).

Les différentes étapes sont indiquées ci-dessous :

Console

La AWS Backup console prend désormais en charge la restauration multirégionale pour les clusters Aurora DSQL, fournissant ainsi un processus rationalisé pour créer des clusters couvrant plusieurs régions. Pour plus d'informations sur les clusters multirégionaux, voir [Configuration des clusters multirégionaux](#).

1. Connectez-vous à la console de AWS gestion et ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez le coffre de sauvegarde qui contient le point de restauration Aurora DSQL que vous souhaitez restaurer.

4. Sélectionnez le point de récupération que vous souhaitez restaurer, puis choisissez Restaurer.
5. Sur la page de restauration, sous Options de restauration, sélectionnez Ajouter des régions homologues pour activer la restauration multirégionale.
6. Sélectionnez une région de cluster homologue dans le menu déroulant. Cette région doit se trouver dans le même triplet que votre région actuelle et doit également contenir une copie interrégionale à partir du point de récupération de la (première) région actuelle.
7. Sélectionnez une région témoin dans le menu déroulant. Cette région doit également se trouver dans le même triplet.
8. Configurez les paramètres du cluster pour les clusters de région principaux et homologues :
 - a. Pour le cluster principal, configurez :
 - Chiffrement du cluster (facultatif) : sélectionnez une clé KMS pour le chiffrement.
 - Protection contre la suppression : active ou désactive la protection contre la suppression.
 - b. Pour le cluster de régions homologue, configurez :
 - Chiffrement du cluster par région homologue (facultatif) : sélectionnez une clé KMS pour le chiffrement.
 - Protection contre la suppression des clusters dans les régions homologues : activez ou désactivez la protection contre la suppression.
9. Vérifiez vos paramètres et choisissez Restaurer la sauvegarde.
10. La console lancera le processus de restauration multirégional, qui crée des clusters dans les deux régions et les lie automatiquement entre eux.

AWS CLI

La restauration multirégionale peut désormais être réalisée à l'aide des nouvelles métadonnées de restauration orchestrées à l'aide des commandes AWS Backup CLI. Cette approche simplifie le processus en gérant automatiquement la liaison des clusters. Pour plus d'informations sur la création de clusters multirégionaux par programmation, consultez la [section Configuration de clusters multirégionaux dans](#) le guide de l'utilisateur d'Aurora DSQL.

⚠ Important

Le cluster principal et le cluster homologue doivent tous deux se trouver dans des régions du même groupe. L'opération échouera si les clusters se trouvent dans des régions extérieures au groupe. Les groupes pris en charge incluent :

- USA Est (Virginie du Nord) ; USA Est (Ohio) ; USA Ouest (Californie du Nord)
- Europe (Irlande) ; Europe (Londres) ; Europe (Paris) ; Europe (Francfort)
- Asie-Pacifique (Tokyo) ; Asie-Pacifique (Séoul) ; Asie-Pacifique (Osaka)

Restauration multirégionale à AWS CLI l'aide de métadonnées de restauration orchestrées

1. Créez une tâche de restauration à l'aide de la commande CLI `aws backup start-restore-job` avec les nouvelles métadonnées d'orchestration multirégionales :

Exemple

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-
point:abcd1234" \
--iam-role-arn "arn:aws:iam::123456789012:role/service-role/
AWSBackupDefaultServiceRole" \
--metadata '{
  "witnessRegion":"us-west-1",
  "useMultiRegionOrchestration":"true",
  "peerRegion":["us-east-2"],
  "regionalConfig":[{"region":"us-east-1","isDeletionProtectionEnabled
":true,"kmsKeyId":"arn:aws:kms:us-east-1:123456789012:key/
ba4b3773-4bb8-4a7a-994c-46ede70202f5"}, {"region":"us-west-2",
"isDeletionProtectionEnabled":true,"kmsKeyId":"arn:aws:kms:us-
west-2:123456789012:key/ba4b3773-4bb8-4a7a-994c-46ede70202f5"}]
}' \
--copy-source-tags-to-restored-resource
```

La structure des métadonnées inclut :

- `witnessRegion`: La région qui servira de témoin au cluster multirégional. Pour plus d'informations, consultez [Resilience dans Amazon Aurora DSQL](#).

- `useMultiRegionOrchestration`: défini sur `true` pour activer l'orchestration multirégionale.
- `peerRegion`: un tableau contenant la ou les régions avec des clusters homologues dans le cluster multirégional. Pour plus d'informations, consultez le [MultiRegionProperties](#) manuel Aurora DSQL API Reference.
- `regionalConfig`: un tableau contenant la configuration pour chaque région :
 - `region`: L' Région AWS identifiant.
 - `isDeletionProtectionEnabled`: indicateur booléen pour la protection contre la enable/disable suppression. Pour plus d'informations, consultez le [CreateCluster](#) manuel Aurora DSQL API Reference.
 - `kmsKeyId`: l'ARN de la clé KMS pour le chiffrement (facultatif).

Si `regionalConfig` aucune propriété n'est spécifiée, les valeurs par défaut seront appliquées : chiffrement par défaut et `isDeletionProtectionEnabled = TRUE`.

2. Surveillez l'état de la tâche de restauration à l'aide de la `aws backup describe-restore-job` commande :

```
aws backup describe-restore-job --restore-job-id job-12345678
```

3. Une fois la tâche de restauration terminée, vous pouvez vérifier la configuration du cluster multirégional à l'aide de la CLI Aurora DSQL :

```
aws dsq1 describe-cluster --cluster-identifier your-cluster-id
```

Pour plus d'informations sur les opérations de clusters multirégionaux, consultez [UpdateCluster](#) le manuel Aurora DSQL API Reference.

Résoudre les problèmes de restauration d'Aurora SQL

Erreur : autorisations insuffisantes

Cause possible : si vous essayez de copier un point de restauration Aurora DSQL dans un compte (copie entre comptes) qui n'a jamais interagi avec l'API DSQL, vous risquez de recevoir une erreur d'autorisation car le rôle lié au service DSQL n'est pas configuré dans le compte de destination.

Solution : associez la [politique gérée SQL](#) qui inclut le rôle lié à un service SQL à un rôle dans le compte de destination. [AuroraDsqlServiceLinkedRolePolicy](#)

Si vous rencontrez d'autres problèmes lors du processus de sauvegarde ou de restauration, vous pouvez vérifier l'état de vos tâches de sauvegarde et de restauration dans la AWS Backup console ou à l'aide du AWS CLI. En outre, vous pouvez consulter les AWS CloudTrail journaux pour détecter tout message d'erreur ou événement pertinent lié à vos AWS Backup opérations.

Questions fréquemment posées sur la restauration d'Aurora DSQL

1. « Puis-je utiliser Aurora AWS Backup DSQL depuis la console Aurora DSQL ? »

Non, vous pouvez uniquement effectuer des sauvegardes et des restaurations, ainsi que gérer des sauvegardes, à partir de AWS Backup la console, du SDK ou de la CLI.

2. « Quelle est la granularité de sauvegarde disponible pour Aurora DSQL ? Puis-je sauvegarder des tables ou des bases de données spécifiques dans mon cluster ? »

Vous pouvez uniquement sauvegarder et restaurer l'intégralité d'un cluster Aurora DSQL.

3. « Les sauvegardes d'Aurora DSQL sont-elles des sauvegardes complètes ou des sauvegardes incrémentielles ? »

Les points de restauration des clusters Aurora DSQL (sauvegardes) sont des sauvegardes complètes de vos clusters.

4. « Puis-je créer des sauvegardes pour mes clusters multirégionaux Aurora DSQL ? »

Oui, vous pouvez créer des sauvegardes pour chaque cluster dans des clusters multirégionaux en suivant les mêmes étapes que lorsque vous créez une sauvegarde d'un seul cluster dans une seule région.

AWS Backup recommande comme bonne pratique de créer une copie interrégionale de votre sauvegarde dans l'autre région à partir de laquelle vous prévoyez de restaurer le cluster multirégional, car la restauration multirégionale nécessite une copie identique du même point de récupération [identique dans cette opération signifie que les points de restauration ont le même nom de ressource et la même heure de création].

5. « Mon cluster restauré remplacera-t-il mon cluster existant ? »

Non Lorsque vous restaurez vos données Aurora DSQL, vous AWS Backup créez un nouveau cluster à partir de vos instantanés ; le cluster restauré ne remplacera pas le cluster source.

Restaurer les CloudFormation piles

Une sauvegarde CloudFormation composite est une combinaison d'un CloudFormation modèle et de tous les points de restauration imbriqués associés. N'importe quel nombre de points de récupération imbriqués peut être restauré, mais le point de récupération composite (qui est le point de récupération de niveau supérieur) ne peut pas être restauré.

Lorsque vous restaurez un CloudFormation modèle de point de restauration, vous créez une nouvelle pile dont les modifications sont définies pour représenter la sauvegarde.

Restaurer CloudFormation à l'aide de la AWS Backup console

Depuis la [CloudFormation console](#), vous pouvez voir la nouvelle pile et le nouvel ensemble de modifications. Pour en savoir plus sur les jeux de modifications, consultez [Mise à jour des piles à l'aide de jeux de modifications](#) dans le Guide de l'utilisateur CloudFormation .

Déterminez les points de restauration imbriqués à partir desquels vous souhaitez effectuer la restauration avec votre CloudFormation pile, puis restaurez-les à l'aide de la AWS Backup console.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez aux Coffres de sauvegarde, sélectionnez le coffre-fort de sauvegarde contenant le point de récupération souhaité, puis cliquez sur Points de récupération.
3. Restaurez le point CloudFormation de récupération du modèle.
 - a. Cliquez sur le point de récupération composite contenant les points de récupération imbriqués que vous souhaitez restaurer pour afficher la page Détails du point de récupération composite.
 - b. Sous Points de récupération imbriqués, les points de récupération imbriqués seront affichés. Chaque point de récupération aura un ID de point de récupération, un statut, un ID de ressource, un type de ressource, un type de sauvegarde et l'heure à laquelle le point de récupération a été créé. Cliquez sur le bouton radio situé à côté du point CloudFormation de récupération, puis sur Restaurer. Assurez-vous de sélectionner le point de récupération dont le type de ressource est : CloudFormation et le type de sauvegarde : sauvegarde.
4. Une fois le travail de restauration du CloudFormation modèle terminé, votre CloudFormation modèle restauré sera visible dans la [CloudFormation console](#) sous Stacks.
5. Sous Noms des piles, vous devriez trouver le modèle restauré avec le statut REVIEW_IN_PROGRESS.
6. Cliquez sur le nom de la pile pour voir les détails de la pile.

7. Il y a des onglets sous le nom de la pile. Cliquez sur Jeux de modifications.
8. Exécutez le jeu de modification.
9. Après ce processus, les ressources de la pile d'origine seront recréées dans la nouvelle pile. Les ressources avec état seront recréées vides. Pour récupérer les ressources dynamiques, revenez à la liste des points de récupération de la AWS Backup console, sélectionnez le point de récupération dont vous avez besoin et lancez une restauration.

Restaurer CloudFormation avec AWS CLI

Dans l'interface de ligne de commande, vous [start-restore-job](#) permet de restaurer une CloudFormation pile.

La liste suivante répertorie les métadonnées acceptées pour restaurer une CloudFormation ressource.

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

Restauration d'un cluster DocumentDB

Utiliser la AWS Backup console pour restaurer les points de restauration Amazon DocumentDB

Pour restaurer un cluster Amazon DocumentDB, vous devez spécifier plusieurs options de restauration. Pour plus d'informations sur ces options, consultez [Restauration à partir d'un instantané de cluster](#) dans le Guide du développeur Amazon DocumentDB.

Pour restaurer un cluster Amazon DocumentDB

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon DocumentDB que vous voulez restaurer.

3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Assurez-vous d'être sur la page de console Restaurer les instantanés du cluster Amazon DocumentDB.
5. Dans le volet Spécifications de l'instance, sélectionnez un moteur de base de données pour l'instance.
6. Dans le volet Paramètres, entrez un nom unique pour l'identifiant de votre cluster de base de données.

Vous pouvez utiliser des lettres, des chiffres et des traits d'union, mais vous ne pouvez pas avoir deux traits d'union consécutifs ou terminer le nom par un tiret. Le nom final sera entièrement en minuscules.

7. Dans le volet Réseau et sécurité, sélectionnez une zone de disponibilité ou laissez-nous en choisir une pour vous.
8. Dans le volet des options de base de données, sélectionnez le port de base de données.

Il s'agit du TCP/IP port que l'instance ou le cluster de base de données utilisera pour les connexions aux applications. La chaîne de connexion de toute application se connectant à l'instance de base de données ou au cluster doit spécifier son numéro de port. Le groupe de sécurité appliqué à l'instance ou au cluster de base de données et les pare-feux de votre organisation doivent autoriser les connexions au port. Toutes les instances de base de données d'un cluster de base de données utilisent le même port.

9. Dans le volet des options de base de données, sélectionnez également le groupe de paramètres du cluster de base de données.

Il s'agit du groupe de paramètres associé au cluster de base de données de cette instance. Un groupe de paramètres de cluster de bases de données sert de conteneur pour les valeurs de configuration du moteur qui sont appliquées à chaque instance de base de données dans le cluster.

10. Dans le volet Chiffrement, sélectionnez la clé qui sera utilisée pour chiffrer ce volume de base de données. La valeur par défaut est `aws/rds`. Vous pouvez également utiliser une clé gérée par le client (CMK).
11. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.

12. Dans le volet Restaurer le rôle, choisissez le rôle IAM par défaut pour la tâche de restauration ou un autre rôle IAM.
13. Dans le volet Balises de ressources protégées, vous pouvez éventuellement choisir de copier les balises de la sauvegarde vers le cluster de base de données restauré.
14. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

15. Une fois votre restauration terminée, attachez votre cluster Amazon DocumentDB restauré à une instance Amazon RDS.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon DocumentDB

Restaurez d'abord votre cluster. Utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon DocumentDB :

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
scalingConfiguration
vpcSecurityGroupIds // string
```

Ensuite, attachez votre cluster Amazon DocumentDB restauré à une instance Amazon RDS à l'aide de `create-db-instance`

- Pour Linux, macOS ou Unix :

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                             --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Pour Windows :

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                             --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Restaurer une table Amazon DynamoDB

Utiliser la AWS Backup console pour restaurer les points de restauration DynamoDB

Pour restaurer une table DynamoDB

- Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
- Dans le volet de navigation, choisissez Ressources protégées et l>ID de ressource DynamoDB que vous voulez restaurer.
- Sur la page Détails de la ressource, une liste des points de récupération pour l>ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l>ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
- Pour Paramètres, Nom nouvelle table, entrez un nouveau nom de table.
- Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.
- Pour Paramètres de chiffrement :
 - Si votre sauvegarde est gérée par DynamoDB (son ARN commence par) AWS Backup , chiffre votre table restaurée à l'`arn:aws:dynamodb:` d'une clé appartenant à DynamoDB. AWS

Pour choisir une autre clé pour chiffrer votre table restaurée, vous pouvez soit utiliser l'AWS Backup [StartRestoreJob](#)opération, soit effectuer la restauration depuis la console [DynamoDB](#).

- b. Si votre sauvegarde prend en charge AWS Backup la gestion complète (son ARN commence par `arn:aws:backup`), vous pouvez choisir l'une des options de chiffrement suivantes pour protéger votre table restaurée :
- (Par défaut) Clé KMS appartenant à DynamoDB (sans frais supplémentaires pour le chiffrement)
 - Clé KMS gérée par DynamoDB (des frais KMS s'appliquent)
 - Clé KMS gérée par le client (des frais KMS s'appliquent)

Les clés « détenues par DynamoDB » et « gérées par DynamoDB » sont identiques aux clés « détenues par AWS » et « gérées par AWS », respectivement. Pour plus de précisions, consultez [Fonctionnement du chiffrement au repos](#) dans le Guide du développeur Amazon DynamoDB.

Pour plus d'informations sur AWS Backup la gestion complète, consultez [Sauvegarde DynamoDB avancée](#).

 Note

Les instructions suivantes s'appliquent uniquement si vous restaurez une sauvegarde copiée ET que vous souhaitez chiffrer la table restaurée avec la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine.

Lors de la restauration d'une sauvegarde interrégionale, pour chiffrer votre table restaurée à l'aide de la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine, votre clé doit être une clé multirégionale. AWS Les clés -owned et AWS-managed ne sont pas des clés multirégionales. Pour plus d'informations, consultez [Clés multi-régions](#) dans le Manuel du développeur AWS Key Management Service .

Lorsque vous restaurez une sauvegarde entre comptes, pour chiffrer votre table restaurée à l'aide de la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine, vous devez partager la clé de votre compte source avec votre compte de destination. AWS Les clés -owned et AWS-managed ne peuvent pas être partagées entre les comptes. Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Manuel du développeur AWS Key Management Service .

7. Choisissez Restore backup.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration DynamoDB

Utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors des restaurations DynamoDB. Les métadonnées ne sont pas sensibles à la casse.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Voici un exemple d'argument `restoreMetadata` pour une opération `StartRestoreJob` dans l'interface de ligne de commande :

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,kmsMasterKeyArn=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://endpointurl.com
```

L'exemple précédent chiffre la table restaurée à l'aide d'une clé AWS appartenant à l'utilisateur. La partie des métadonnées de restauration qui spécifie le chiffrement à l'aide de la clé AWS-owned est : `"encryptionType\":"Default\","kmsMasterKeyArn\":"Not Applicable\"`.

Pour chiffrer votre table restaurée à l'aide d'une clé AWS gérée, spécifiez les métadonnées de restauration suivantes : `"encryptionType\":"KMS\","kmsMasterKeyArn\":"Not Applicable\"`

Pour chiffrer votre table restaurée à l'aide d'une clé gérée par le client, spécifiez les métadonnées de restauration suivantes : `"encryptionType\":"KMS\","kmsMasterKeyArn\":"arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab\"`.

Restaurer un volume Amazon EBS

Lorsque vous restaurez un instantané Amazon Elastic Block Store (EBS), vous pouvez choisir de le restaurer en tant que volume EBS, de le restaurer sur un AWS Storage Gateway volume ou de restaurer certains éléments de celui-ci dans un compartiment Amazon S3.

Restaurer sur un volume EBS

Lorsque vous restaurez un instantané (sauvegarde périodique des données EBS) sur un nouveau volume, vous spécifiez le type de volume, sa taille en GiB et une zone de disponibilité. Vous pouvez éventuellement choisir de chiffrer le nouveau volume avec une clé existante ou une nouvelle AWS KMS clé.

Restaurer sur un volume de passerelle

Lorsque vous effectuez une restauration sur un volume de passerelle, vous devez spécifier une passerelle accessible, choisir le nom de votre cible iSCSI et choisir un ID de disque si votre passerelle est stockée en volume ou une capacité égale ou supérieure à celle de votre instantané si votre passerelle est mise en cache en volume.

Restauration au niveau des fichiers dans un compartiment Amazon S3

Avant de démarrer une tâche de restauration des ressources EBS dans un compartiment Amazon S3, vérifiez les [autorisations EBS et les exigences](#) [Autorisations de restauration Amazon S3](#) d'accès. Les autorisations nécessaires sont contenues dans la politique gérée [AWSBackupServiceRolePolicyForItemRestores](#) et doivent être incluses dans le [rôle IAM](#) utilisé pour l'opération de restauration.

Tous les nouveaux téléchargements d'objets, y compris les données restaurées, vers un compartiment S3 sont automatiquement chiffrés. Lorsque vous choisissez ce type de restauration, spécifiez SSE-S3 (clé gérée côté serveur Amazon S3) ou SSE-KMS (clé gérée côté serveur). AWS KMS SSE-S3 est la valeur par défaut.

Vous pouvez saisir jusqu'à cinq chemins lors de la restauration à partir de la AWS Backup console ; vous pouvez spécifier plusieurs chemins via la ligne de commande. Un chemin doit avoir une longueur inférieure à 1024 octets dans les chaînes codées en UTF-8, y compris les préfixes désignés et désignés par l'utilisateur AWS Backup

Si votre instantané contient plusieurs partitions, spécifiez l'identifiant du système de fichiers de la partition contenant les données que vous souhaitez restaurer. Cet identifiant peut être trouvé en

utilisant [Recherche de sauvegardes](#) et est identique à l'UUID ou à l'ID de disque du système de fichiers.

	Vers le nouveau volume EBS	Vers la passerelle	Restauration au niveau des fichiers dans le compartiment S3
Chiffrement	Facultatif. Vous pouvez choisir une AWS KMS clé existante ou créer une nouvelle clé KMS.		Obligatoire. Choisissez entre SSE-S3, SSE-KMS ou le chiffrement du compartiment de destination par défaut 1.
Autorisations et rôles	Choisissez un rôle existant ; s'il n'en existe aucun, le rôle par défaut avec les autorisations appropriées est créé.	Choisissez un rôle existant ; s'il n'en existe aucun, le rôle par défaut avec les autorisations appropriées est créé	Le choix du rôle doit avoir un EBS suffisant et. Autorisations de restauration Amazon S3
Restauration depuis un stockage à froid (EBS Archive Tier)	Available	Unavailable	Unavailable
Réglages à spécifier	Type de volume ; taille (GiB) ; zone de disponibilité ; débit	Passerelle (dans un état accessible) ; nom de la cible iSCSI ; identifiant du disque (pour les passerelles stockées en volume) ; capacité (pour les passerelles mises en cache par volume)	Type de restauration, y compris : nom du compartiment de destination ; chemin(s) à restaurer ; type de cryptage ; identifiant de clé KMS de restauration au niveau du fichier si SSE-KMS est défini comme type de chiffrement

¹ Dans la AWS Backup console, vous sélectionnez l'une des trois options de chiffrement ; si vous utilisez la CLI pour effectuer la restauration, omettez de `encryptionType` rétablir le chiffrement du bucket de destination par défaut.

Restaurer un instantané EBS avec la console AWS Backup

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis l'ID de ressource EBS que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les paramètres de restauration de votre ressource. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

Pour Type de ressource, choisissez la AWS ressource à créer lors de la restauration de cette sauvegarde.

5. Si vous choisissez Volume EBS, indiquez les valeurs Type de volume, Taille (Gio), et choisissez une Zone de disponibilité. Après Débit, il y aura une case à cocher facultative Chiffrer ce volume. Cette option restera active si le point de restauration EBS est crypté. . Vous pouvez spécifier une clé KMS ou créer une AWS KMS clé.

Si vous choisissez Volume Storage Gateway, choisissez une Passerelle accessible. Choisissez également votre Nom de cible iSCSI. Pour les passerelles Volume stocké, choisissez un ID de disque. Pour les passerelles Volume mis en cache, choisissez une capacité au moins égale à votre ressource protégée.

Si vous choisissez la restauration au niveau du fichier, vous pouvez inclure jusqu'à 5 objets ou dossiers à partir de l'instantané. Vous pouvez [effectuer une recherche dans vos sauvegardes indexées](#) pour trouver le nom ou le chemin du fichier.

- Entrez les chemins des fichiers.
- Choisissez d'utiliser un compartiment Amazon S3 existant ou de créer un nouveau compartiment pour la destination où les objets ou les dossiers seront restaurés.

- Définissez le chiffrement du ou des objets restaurés. Vous pouvez choisir le chiffrement du compartiment de destination par défaut, SSE-S3 ou SSE-KMS. Pour plus de détails, voir [Restaurez les données S3 à l'aide de AWS Backup](#).
6. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration. Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.
 7. Choisissez Restaurer la sauvegarde (les éléments de restauration s'affichent pour la restauration au niveau du fichier).

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Restaurer à partir de snapshots EBS archivés

La restauration d'un instantané EBS archivé le déplace temporairement d'un stockage à froid vers un stockage à chaud afin de créer un nouveau volume EBS. Ce type de restauration entraîne des frais de récupération uniques. Les frais de stockage pour le stockage à chaud et à froid sont facturés pendant cette période de restauration.

Tip

Les volumes EBS stockés à froid ne peuvent pas être restaurés sur un volume de passerelle ou restaurés au niveau des fichiers.

Vous pouvez restaurer un instantané EBS archivé dans un stockage à froid à l'aide de la [console AWS Backup](#) ou de la ligne de commande. Une restauration à partir d'un stockage à froid peut prendre jusqu'à 72 heures. Pour plus d'informations, consultez la section [Archiver les instantanés Amazon EBS](#) dans le Guide de l'utilisateur Amazon EBS.

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Accédez à Backup Vaults > *Vault* > Restaurer le snapshot EBS archivé.
3. Dans la section Paramètres, entrez une valeur comprise entre 0 et 180 inclus, qui indique le nombre de jours nécessaires pour restaurer temporairement un instantané archivé.

4. Entrez d'autres paramètres : type de volume, taille, IOPS, zone de disponibilité, débit et chiffrement.
5. Choisissez votre rôle de restauration.
6. Sélectionnez Restaurer la sauvegarde. Dans la fenêtre contextuelle de confirmation, confirmez les instantanés et le type de restauration. Sélectionnez ensuite Restaurer l'instantané.

AWS CLI

1. Utilisation des [start-restore-job](#)
2. Incluez les paramètres requis pour la restauration des instantanés EBS archivés :

```
--recovery-point-arn arn:aws:backup:region:account-id:recovery-point:recovery-  
point-id  
--metadata  
'{"temporaryRestoreDays":"value","volumeType":"value","volumeSize":"value","availabilityZone":"value"}'  
--iam-role-arn arn:aws:iam::account-id:role/service-role/  
AWSBackupDefaultServiceRole  
--resource-type EBS
```

3. Spécifiez la durée de restauration temporaire (0 à 180 jours) dans le `temporaryRestoreDays` paramètre. Cela détermine la durée pendant laquelle l'instantané archivé sera disponible dans un espace de stockage à chaud.
4. Configurez les nouveaux paramètres de volume EBS, y compris `volumeType` (gp2, gp3, io1, io2, st1, sc1), en GiB et cible. `volumeSize` `availabilityZone`
5. Surveillez l'état de la tâche de restauration à l'[describe-restore-job](#) aide de l'ID de tâche de restauration renvoyé. La restauration des archives peut prendre jusqu'à 72 heures.

Restaurez un instantané EBS en AWS CLI

Pour restaurer Amazon EBS à l'aide de l'API ou de l'interface de ligne de commande, utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors d'une restauration Amazon EBS :

```
aws:backup:request-id  
availabilityZone  
encrypted // if set to true, encryption will be enabled as volume is restored  
iops
```

```
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
of default KMS Key Id
restoreType // include for file level restore - see details below
throughput
temporaryRestoreDays
volumeType
volumeSize
```

Exemple :

```
"restoreMetadata": "{\"encrypted\": \"false\", \"volumeId\": \"vol-04cc95f3490b5ceea\",
\"availabilityZone\": null}"
```

Spécifications de restauration au niveau des fichiers

`restoreType` est nécessaire pour la restauration au niveau des fichiers. Pour ce type de restauration, les métadonnées uniques suivantes sont requises :

```
destinationBucketName //
pathsToRestore //
encryptionType // You can specify SSE-S3 or SSE-KMS; do not include if you want to
restore to default encryption
kmsKeyId //
```

L'identifiant du système de fichiers est facultatif pour les instantanés à partition unique. Si ces informations ne sont pas transmises, seul le chemin absolu sans le séparateur « : » (tel que `"/data/process/abc.txt"`, `"/data/departement/xyz.txt"`) sera accepté.

Restaurer une EC2 instance Amazon

Lorsque vous restaurez une EC2 instance, vous AWS Backup créez une Amazon Machine Image (AMI), une instance, le volume racine Amazon EBS, les volumes de données Amazon EBS (si la ressource protégée contenait des volumes de données) et des instantanés Amazon EBS. Vous pouvez personnaliser certains paramètres d'instance à l'aide de la AWS Backup console, ou un plus grand nombre de paramètres à l'aide du AWS CLI ou d'un AWS SDK.

Les considérations suivantes s'appliquent à la restauration EC2 des instances :

- AWS Backup configure l'instance restaurée pour qu'elle utilise la même paire de clés que celle utilisée à l'origine par la ressource protégée. Vous ne pouvez pas spécifier une paire de clés différente pour l'instance restaurée pendant le processus de restauration.

- AWS Backup ne sauvegarde ni ne restaure les données utilisateur utilisées lors du lancement d'une EC2 instance Amazon.
- Lors de la configuration de l'instance restaurée, vous pouvez choisir d'utiliser le même profil d'instance que celui utilisé initialement par la ressource protégée ou de le lancer sans profil d'instance. Cela permet d'éviter une escalade possible des privilèges. Vous pouvez mettre à jour le profil d'instance pour l'instance restaurée à l'aide de la EC2 console Amazon.

Si vous utilisez le profil d'instance d'origine, vous devez accorder AWS Backup les autorisations suivantes, l'ARN de la ressource étant l'ARN du rôle IAM associé au profil d'instance.

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Remplacez *role-name* par le nom du rôle de profil d' EC2 instance qui sera attaché à l' EC2 instance restaurée. Il ne s'agit pas du rôle de AWS Backup service, mais du rôle IAM qui fournit des autorisations aux applications exécutées sur l' EC2 instance.

- Lors d'une restauration, tous les EC2 quotas et restrictions de configuration d'Amazon s'appliquent.
- Si le coffre-fort contenant vos points de EC2 récupération Amazon est verrouillé, consultez [Considérations supplémentaires en matière de sécurité](#) pour plus d'informations.

Utiliser la AWS Backup console pour restaurer les points EC2 de récupération Amazon

Vous pouvez restaurer une EC2 instance Amazon complète à partir d'un point de récupération unique, y compris le volume racine, les volumes de données et certains paramètres de configuration de l'instance, tels que le type d'instance et la paire de clés.

Pour restaurer les EC2 ressources Amazon à l'aide de la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de la EC2 ressource Amazon pour ouvrir la page de détails de la ressource.
3. Dans le volet Points de restauration, cliquez sur le bouton radio situé à côté de l'ID du point de récupération à restaurer. Dans le coin supérieur droit du volet, choisissez Restaurer.

4. Dans le volet Paramètres réseau, nous utilisons les paramètres de l'instance protégée pour sélectionner les valeurs par défaut pour le type d'instance, le VPC, le sous-réseau, le groupe de sécurité et le rôle IAM de l'instance. Vous pouvez utiliser ces valeurs par défaut ou les modifier selon vos besoins.
5. Dans le volet Restaurer le rôle, utilisez le rôle par défaut ou choisissez un rôle IAM pour spécifier un rôle IAM qui AWS Backup autorise la restauration de la sauvegarde.
6. Dans le volet Balises de ressources protégées, nous sélectionnons par défaut Copier les balises de la ressource protégée vers la ressource restaurée. Si vous ne souhaitez pas copier ces balises, décochez la case.
7. Dans le volet Paramètres avancés, acceptez les valeurs par défaut des paramètres de l'instance ou modifiez-les selon vos besoins. Pour plus d'informations sur ces paramètres, choisissez Info pour le paramètre afin d'ouvrir son volet d'aide.
8. Lorsque vous avez terminé de configurer l'instance, choisissez Restaurer la sauvegarde.

Restaurez Amazon EC2 avec AWS CLI

Dans l'interface de ligne de commande [start-restore-job](#), vous pouvez effectuer une restauration avec un maximum de 32 paramètres (y compris certains paramètres qui ne sont pas personnalisables via la AWS Backup console).

La liste suivante répertorie les métadonnées acceptées que vous pouvez transmettre pour restaurer un point de EC2 récupération Amazon.

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
```

```
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
BlockDeviceMappings
aws:backup:request-id
```

AWS Backup accepte les attributs suivants fournis uniquement à titre informatif. Cependant, leur inclusion n'affectera pas la restauration :

```
vpcId
```

[BlockDeviceMappings](#) est un paramètre facultatif que vous pouvez inclure. AWS Backup prend en charge les BlockDeviceMappings attributs suivants.

 Note

SnapshotId et OutpostArn ne sont pas prises en charge.

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName" : string,
      "NoDevice" : string,
      "VirtualName" : string,
      "Ebs": {
        "DeleteOnTermination": boolean,
        "Iops": number,
        "VolumeSize": number,
        "VolumeType": string,
        "Throughput": number,
        "Encrypted": boolean,
        "KmsKeyId": string
      }
    }
  ]
}
```

```

    }
  }
}

```

Par exemple :

```

{
  "BlockDeviceMappings": [
    {
      "DeviceName": "/def/tuvw",
      "Ebs": {
        "DeleteOnTermination": true,
        "Iops": 3000,
        "VolumeSize": 16,
        "VolumeType": "gp3",
        "Throughput": 125,
        "Encrypted": true,
        "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/ab3cde45-67f8-9g01-
hi2j-3456klmno7p8"
      }
    },
    {
      "DeviceName": "/abc/xyz",
      "Ebs": {
        "DeleteOnTermination": false,
        "Iops": 3000,
        "VolumeSize": 16,
        "VolumeType": "gp3",
        "Throughput": 125,
        "Encrypted": false
      }
    }
  ]
}

```

Vous pouvez également restaurer une EC2 instance Amazon sans inclure de paramètres enregistrés. Cette option est disponible dans l'onglet Ressource protégée de la AWS Backup console.

Important

Si vous ne remplacez pas la AWS KMS clé contenue dans le `BlockDeviceMappings` lors de la restauration à partir de sauvegardes entre comptes ou entre régions, votre

restauration risque d'échouer. Pour de plus amples informations, veuillez consulter [Résoudre les problèmes de restauration des EC2 instances Amazon](#).

Résoudre les problèmes de restauration des EC2 instances Amazon

Résolution des problèmes

- [Défaillances de restauration entre comptes](#)
- [Défaillances de restauration entre régions](#)

Défaillances de restauration entre comptes

Description : la restauration de l' EC2 instance Amazon échoue lorsque vous tentez de restaurer à partir d'une sauvegarde partagée avec votre compte.

Problèmes possibles : votre compte n'a peut-être pas accès aux AWS KMS clés utilisées pour chiffrer les volumes sources dans le compte de partage. Les clés KMS ne sont peut-être pas partagées avec votre compte.

Ou bien, les volumes attachés à l'instance source ne sont pas chiffrés.

Solution : pour résoudre ce problème, définissez l'encryptedattribut sur true, puis effectuez l'une des opérations suivantes :

- Remplacez les clés KMS dans le BlockDeviceMappings et spécifiez une clé KMS que vous possédez dans votre compte.
- Demandez au compte propriétaire de vous accorder l'accès aux clés KMS utilisées pour chiffrer les volumes en mettant à jour la politique des clés KMS. Pour plus d'informations, voir [Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS](#).

Défaillances de restauration entre régions

Description : la restauration de l' EC2 instance Amazon échoue lors d'une tentative de restauration à partir d'une sauvegarde interrégionale.

Problème : Les volumes de la sauvegarde sont peut-être chiffrés à l'aide de AWS KMS clés d'une seule région qui ne sont pas disponibles dans la région de destination. Ou bien, les volumes attachés à l'instance source ne sont pas chiffrés.

Solution : pour résoudre ce problème, définissez l'attribut `encrypted` sur `true` et remplacez la clé KMS dans le `BlockDeviceMappings` par une clé KMS dans la région de destination.

Restaurer un système de fichiers Amazon EFS

Si vous restaurez une instance Amazon Elastic File System (Amazon EFS), vous pouvez effectuer une restauration complète ou une restauration au niveau des éléments.

Restauration complète

Lorsque vous effectuez une restauration complète, l'ensemble du système de fichiers est restauré.

AWS Backup ne prend pas en charge les restaurations destructives avec Amazon EFS. Une restauration destructive se produit lorsqu'un système de fichiers restauré supprime ou remplace le système de fichiers source ou existant. AWS Backup restaure plutôt votre système de fichiers dans un répertoire de restauration situé hors du répertoire racine.

Restauration au niveau des éléments

Lorsque vous effectuez une restauration au niveau de l'élément, AWS Backup restaure un fichier ou un répertoire spécifique. Vous devez spécifier le chemin relatif à la racine du système de fichiers. Par exemple, si le système de fichiers est monté sur `user/home/myname/efs/file1` et que le chemin d'accès à ce dernier est `/file1`, saisissez `/user/home/myname/efs`. Les chemins sont sensibles à la casse. Les caractères génériques et les chaînes regex ne sont pas pris en charge. Votre chemin peut être différent de celui de l'hôte si le système de fichiers est monté à l'aide d'un point d'accès.

Vous pouvez sélectionner jusqu'à 10 éléments lorsque vous utilisez la console pour exécuter une restauration EFS. Il n'y a aucune limite d'éléments lorsque vous utilisez l'interface de ligne de commande pour effectuer une restauration ; toutefois, la longueur des métadonnées de restauration pouvant être transmises est limitée à 200 Ko.

Vous pouvez restaurer ces éléments dans un système de fichiers nouveau ou existant. Dans tous les cas, AWS Backup crée un nouveau répertoire Amazon EFS (`aws-backup-restore_datetime`) à partir du répertoire racine pour contenir les éléments. La hiérarchie complète des éléments spécifiés est conservée dans le répertoire de récupération. Par exemple, si le répertoire A contient des sous-répertoires B, C et D, AWS Backup conserve la structure hiérarchique lorsque A, B, C et D sont restaurés. Vous pouvez effectuer une restauration Amazon EFS au niveau des éléments dans un système de fichiers existant ou sur un nouveau système de fichiers, mais chaque tentative de restauration crée un nouveau répertoire de récupération hors du répertoire racine pour contenir les

fichiers restaurés. Si vous tentez plusieurs restaurations pour le même chemin d'accès, plusieurs répertoires contenant les éléments restaurés peuvent exister.

 Note

Si vous ne conservez qu'une sauvegarde hebdomadaire, vous pouvez uniquement restaurer vers le statut du système de fichiers au moment où vous avez effectué cette sauvegarde. Vous ne pouvez pas restaurer vers des sauvegardes incrémentielles antérieures.

Utiliser la AWS Backup console pour restaurer un point de récupération Amazon EFS

Pour restaurer un système de fichiers Amazon EFS

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Votre coffre-fort de sauvegarde EFS reçoit la stratégie d'accès Deny backup:StartRestoreJob lors de sa création. Si vous restaurez votre coffre-fort de sauvegarde pour la première fois, vous devez modifier votre stratégie d'accès comme suit.
 - a. Choisissez Coffres-forts de sauvegarde.
 - b. Choisissez le coffre-fort de sauvegarde contenant le point de récupération que vous souhaitez restaurer.
 - c. Faites défiler jusqu'à la Stratégie d'accès du coffre
 - d. Le cas échéant, supprimez backup:StartRestoreJob de la Statement. Pour ce faire, choisissez Modifier, supprimez backup:StartRestoreJob, puis choisissez Enregistrer la stratégie.
3. Dans le volet de navigation, choisissez Ressources protégées et l'ID du système de fichiers EFS que vous voulez restaurer.
4. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID du système de fichiers sélectionné s'affiche. Pour restaurer un système de fichiers, dans le volet Sauvegardes, cliquez sur la case d'option en regard de l'ID du point de récupération du système de fichiers. Dans le coin supérieur droit du volet, choisissez Restaurer.
5. Spécifiez les paramètres de restauration de votre système de fichiers. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

Vous pouvez effectuer une Restauration complète, qui restaure l'ensemble du système de fichiers. Vous pouvez également restaurer des fichiers et des répertoires spécifiques à l'aide d'une Restauration au niveau des éléments.

- Choisissez l'option Restauration complète pour restaurer le système de fichiers dans son intégralité, y compris tous les dossiers et fichiers de niveau racine.
- Choisissez l'option de restauration au niveau des éléments pour restaurer un fichier ou un répertoire spécifique. Vous pouvez sélectionner et restaurer jusqu'à cinq éléments dans votre Amazon EFS.

Pour restaurer un fichier ou un répertoire spécifique, vous devez spécifier le chemin relatif lié au point de montage. Par exemple, si le système de fichiers est monté sur **/file1** et que le chemin d'accès au fichier est `/user/home/myname/efs`, saisissez `user/home/myname/efs/file1`. Les chemins sont sensibles à la casse et ne peuvent pas contenir de caractères spéciaux, de caractères génériques et de chaînes regex.

1. Dans la zone de texte Chemin d'accès de l'élément, saisissez le chemin d'accès de votre fichier ou dossier.
2. Choisissez Ajouter un élément pour ajouter des fichiers ou des répertoires supplémentaires. Vous pouvez sélectionner et restaurer jusqu'à cinq éléments dans votre système de fichiers EFS.

6. Pour Emplacement de restauration

- Choisissez Restaurer dans le répertoire du système de fichiers source si vous souhaitez restaurer dans le système de fichiers source.
- Choisissez Restaurer dans un nouveau système de fichiers si vous souhaitez restaurer dans un autre système de fichiers.

7. Pour Type de système de fichiers

- (Recommandé) Choisissez Régional si vous souhaitez restaurer votre système de fichiers dans plusieurs zones de AWS disponibilité.
- Choisissez Unizone si vous souhaitez restaurer votre système de fichiers dans une seule zone de disponibilité. Ensuite, dans le menu déroulant Zone de disponibilité, choisissez la destination de votre restauration.

Pour plus d'informations, consultez [Gestion de classes de stockage Amazon EFS](#) dans le Guide de l'utilisateur Amazon EFS.

8. Pour Performances

- Si vous avez choisi d'effectuer une restauration Régionale, choisissez Usage général (recommandé), ou E/S max..
- Si vous avez choisi d'effectuer une restauration Unizone, vous devez choisir Usage général (recommandé). Les restaurations Unizone ne prennent pas en charge E/S max.

9. Pour Activer le chiffrement

- Choisissez Activer le chiffrement, si vous souhaitez chiffrer votre système de fichiers. La clé KMS IDs et les alias apparaissent dans la liste une fois qu'ils ont été créés à l'aide de la console AWS Key Management Service (AWS KMS).
- Dans la zone de texte Clé KMS, choisissez la clé à utiliser dans la liste.

10. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.

Note

Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.

11. Choisissez Restore backup.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Note

Si vous ne conservez qu'une sauvegarde hebdomadaire, vous pouvez uniquement restaurer vers le statut du système de fichiers au moment où vous avez effectué cette sauvegarde. Vous ne pouvez pas restaurer vers des sauvegardes incrémentielles antérieures.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon EFS

Utilisez [StartRestoreJob](#). Lors de la restauration d'une instance Amazon EFS, vous pouvez restaurer un système de fichiers entier ou des fichiers ou répertoires spécifiques. Vous avez besoin des informations suivantes pour restaurer des ressources Amazon EFS :

- `file-system-id`— L'ID du système de fichiers Amazon EFS sauvegardé par AWS Backup. Renvoyé dans `GetRecoveryPointRestoreMetadata`. Cela n'est pas obligatoire lors de la restauration d'un nouveau système de fichiers (cette valeur est ignorée si le paramètre `newFileSystem` est `True`).
- `Encrypted` : valeur booléenne qui, si la valeur est `true`, spécifie que le système de fichiers est chiffré. Si `KmsKeyId` est spécifié, `Encrypted` doit être défini sur `true`.
- `KmsKeyId`— Spécifie la AWS KMS clé utilisée pour chiffrer le système de fichiers restauré.
- `PerformanceMode` : spécifie le mode de débit du système de fichiers. Les valeurs valides sont `generalPurpose` (par défaut) et `maxIO`. Ce `generalPurpose` mode fournit la latence la plus faible par opération et peut atteindre 7 000 opérations de fichiers par seconde. Le `maxIO` mode peut évoluer vers des niveaux plus élevés de débit agrégé et d'opérations par seconde, avec une latence légèrement plus élevée pour les opérations sur les fichiers.
- `CreationToken` : valeur fournie par l'utilisateur qui garantit que le caractère unique (idempotence) de la demande.
- `newFileSystem` : valeur booléenne qui, si la valeur est `true`, spécifie que le point de récupération est restauré à un nouveau système de fichiers Amazon EFS.
- `ItemsToRestore` : tableau de cinq chaînes au maximum, chaque chaîne étant un chemin d'accès au fichier. Utilisez `ItemsToRestore` pour restaurer des fichiers ou des répertoires spécifiques, plutôt que la totalité du système de fichiers. Ce paramètre est facultatif.

Vous pouvez également inclure `aws:backup:request-id`.

Les restaurations One Zone peuvent être effectuées en incluant les paramètres suivants :

```
"singleAzFilesystem": "true"  
"availabilityZoneName": "ap-northeast-3"
```

Pour plus d'informations sur les valeurs de configuration Amazon EFS, consultez [create-file-system](#).

Désactivation des sauvegardes automatiques dans Amazon EFS

Par défaut, [Amazon EFS crée automatiquement des sauvegardes de données](#). Ces sauvegardes sont représentées sous forme de points de restauration dans AWS Backup. Les tentatives de suppression du point de récupération entraîneront un message d'erreur indiquant que les privilèges sont insuffisants pour effectuer l'action.

Il est recommandé de maintenir cette sauvegarde automatique active. Notamment en cas de suppression accidentelle de données, cette sauvegarde permet de restaurer le contenu du système de fichiers à la date du dernier point de récupération créé.

Dans le cas peu probable où vous souhaiteriez les désactiver, la stratégie d'accès doit être modifiée de "Effect": "Deny" à "Effect": "Allow". Consultez le Guide de l'utilisateur Amazon EFS pour plus d'informations sur l'activation ou la désactivation [des sauvegardes automatiques](#).

Restaurer un cluster Amazon EKS

Vous pouvez restaurer les sauvegardes du cluster EKS à l'aide de la AWS Backup console ou de la CLI. Les sauvegardes EKS sont des points de restauration composites qui incluent à la fois des sauvegardes de l'état du cluster EKS et des sauvegardes de volumes persistants.

AWS Backup prend en charge plusieurs expériences de restauration, y compris les restaurations granulaires au niveau de l'espace de noms. Les restaurations ne sont pas destructives et ne remplaceront aucun objet Kubernetes existant dans votre cluster EKS cible. Les restaurations ne remplaceront pas non plus les versions Kubernetes du cluster EKS cible.

Les sauvegardes EKS doivent être restaurées sur un cluster EKS cible, c'est-à-dire un cluster Amazon EKS préprovisionné. Dans le cadre du processus de restauration, vous pouvez choisir de créer un nouveau cluster EKS qui AWS Backup sera créé en votre nom.

Note

AWS Backup fournira un ensemble limité d'options pour créer un nouveau cluster EKS dans le cadre d'une restauration. Pour toutes les fonctionnalités de création de clusters EKS, les clients peuvent créer un nouveau cluster [EKS à l'aide de la console EKS](#) ou APIs le sélectionner comme cible de restauration.

Fonctionnalités de restauration pour Amazon EKS

Type de restauration	Restaurer la cible	Restaurer le comportement
Restauration d'un cluster existant	Restaurer sur le cluster EKS source ou sur le cluster EKS existant	Restaure toutes les ressources Kubernetes et les volumes persistants dans les clusters EKS existants. Toutes les restaurations sont non destructives et les objets existants ne sont pas remplacés. Pour les objets ignorés, vous pouvez vous abonner aux notifications SNS
Restauration d'un nouveau cluster	Crée un nouveau cluster Amazon EKS dans le cadre de votre restauration EKS	Restore crée un nouveau cluster EKS et restaure toutes les ressources Kubernetes et les volumes persistants dans le cluster nouvellement créé
Restauration de l'espace de noms	Cluster Amazon EKS existant	Les restaurations portant uniquement sur les espaces de noms spécifiés, leurs ressources Kubernetes et les restaurations de stockage persistantes correspondantes ne sont pas destructives et les objets existants ne sont pas remplacés. Pour les objets ignorés, vous pouvez vous abonner aux notifications SNS
Restauration permanente du stockage	Dépendant du stockage persistant	Restaurez le stockage persistant individuel sous forme de restaurations autonomes. Consultez Comportement de restauration

Type de restauration	Restaurer la cible	Restaurer le comportement
		d' Amazon EBS , Amazon S3 , Amazon EFS .

Autorisations

Les autorisations requises dépendent du type de restauration et de la destination cible.

- AWS Backup [AWSBackupServiceRolePolicyForRestores](#) contient les autorisations requises pour restaurer votre cluster Amazon EKS et votre stockage persistant EBS et EFS.
- Si votre cluster EKS contient un compartiment S3, ou si vous restaurez le point de récupération S3 enfant seul, vous devrez vous assurer que les politiques ou autorisations suivantes sont attribuées à votre rôle [AWSBackupServiceRolePolicyForS3Restore](#).

Considérations avant la restauration

Avant de commencer une tâche de restauration EKS, passez en revue les points suivants. Si vous restaurez une sauvegarde EKS qui a été copiée sur un compte ou une région, assurez-vous de prendre en compte ces considérations avant les restaurations afin d'éviter les échecs de restauration.

1. Rôles IAM : lors de la restauration sur un autre cluster, les rôles IAM utilisés dans le cluster source (tels que Pod identity, IRSA). Le fournisseur OIDC (configurations, etc.) doit être présent dans le compte/la région en tant que cluster de destination.
2. Vérifiez la version et la compatibilité d'EKS : les versions d'API des objets que vous souhaitez restaurer doivent être identiques (ou aussi proches que possible) et prises en charge dans le nouveau cluster. AWS Backup effectuera au mieux une restauration entre les versions d'EKS, bien que des problèmes de compatibilité puissent survenir lors de la restauration entre des versions très différentes.
3. Classes de stockage correspondantes : pour les restaurations d'un cluster EKS existant, assurez-vous que les modules complémentaires du pilote de stockage CSI appropriés sont installés avant la restauration
4. Compartiments S3 : lors de la restauration d'un cluster EKS avec des compartiments S3, assurez-vous que votre compartiment S3 est versionné et accessible dans le compte ou la région de destination.

5. **Référentiel d'images** : lors de la restauration d'un cluster EKS, assurez-vous que le compte ou la région du cluster EKS de destination a accès aux images référencées dans le cadre de la restauration. Vérifiez que votre registre dispose des autorisations nécessaires pour toutes les régions/politiques relatives aux comptes.
6. **Groupe de sécurité** : les groupes de sécurité doivent être pré-crées pour ALB, Pod Identities, EKS Node Groups, etc. dans le compte et la région cibles si vous créez un nouveau cluster EKS dans le cadre de votre restauration
7. **Zones de disponibilité et nœuds EBS** : les zones de disponibilité dans lesquelles vous restaurez vos volumes EBS doivent être mappées à la zone de disponibilité d'un nœud EKS existant
8. **Restaurations non destructives** : toutes les restaurations EKS seront non destructives et ne remplaceront pas les objets Kubernetes de la restauration cible.
9. **Activer les journaux d'audit EKS** : activez les journaux d'audit EKS pour une journalisation et un dépannage supplémentaires avant la restauration. Vous pouvez également vous abonner aux [notifications SNS](#) pour signaler les objets ignorés ou défaillants lors de la restauration.

Configurations EKS

Lorsque vous restaurez l'Amazon composite AWS Backup, vous choisissez le type de restauration et la destination cible. Vous pouvez choisir de restaurer sur le cluster EKS source, sur un cluster EKS existant ou de créer un nouveau cluster EKS comme cible de restauration. Pour les nouveaux clusters EKS, vous pouvez choisir d'utiliser les mêmes paramètres d'infrastructure existants (par exemple, VPC, sous-réseaux) que le cluster sauvegardé ou d'en configurer de nouveaux. AWS Backup effectuera toujours une restauration non destructive qui ne remplacera pas les ressources existantes.

Pour les restaurations d'espaces de noms, vous pouvez spécifier jusqu'à 5 espaces de noms à restaurer de manière sélective. Seules les ressources délimitées par un espace de noms sont restaurées, tandis que les ressources étendues par cluster sont exclues, à l'exception des volumes persistants associés.

En tant que paramètre avancé, vous pouvez choisir de modifier l'ordre de restauration des objets Kubernetes. Par défaut, tous les objets Kubernetes AWS Backup seront restaurés dans l'ordre suivant :

Ressources Kubernetes étendues au cluster

1. Définitions de ressources personnalisées

2. Espaces de noms (l'espace de noms lui-même, et non les ressources de cet espace de noms)
3. StorageClasses
4. PersistentVolumes

Ressources Kubernetes limitées à l'espace de nommage

1. PersistentVolumeClaims
2. Secrets
3. ConfigMaps
4. ServiceAccounts
5. LimitRanges
6. Capsules
7. ReplicaSets

Configurations de stockage persistantes

Dans le cadre de la restauration de sauvegarde composite Amazon EKS, la deuxième étape consistera à configurer vos configurations de stockage persistant. Cela varie en fonction du stockage persistant sauvegardé dans le cadre de votre cluster EKS.

Pour les instantanés Amazon EBS, vous devez fournir une zone de disponibilité dans laquelle le volume Amazon EBS sera restauré et créé. AWS Backup tentera ensuite de créer le pod EKS dans la même zone de disponibilité que celle sélectionnée afin que votre volume puisse être remonté sur votre cluster EKS dans le cadre de la restauration.

Dans le cadre de la restauration, vos volumes Amazon EBS et vos compartiments Amazon S3 AWS Backup seront remontés sur votre cluster EKS restauré. Les systèmes de fichiers Amazon EFS sont restaurés selon des préfixes aléatoires et nécessitent la création manuelle de points d'accès après la restauration pour être remontés sur votre cluster EKS. AWS Backup ne crée pas de points d'accès ni ne monte de cibles en votre nom. Consultez les instructions ici pour les [points d'accès](#) et les [cibles de montage](#).

Procédure de restauration Amazon EKS

Suivez ces étapes pour restaurer les sauvegardes Amazon EKS à l'aide de la AWS Backup console ou AWS CLI :

Console

Pour restaurer votre cluster Amazon EKS

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez le coffre de sauvegarde qui contient votre sauvegarde Amazon EKS, puis sélectionnez le point de récupération pour votre sauvegarde Amazon EKS.
4. Choisissez Restore (Restaurer).
5. Dans le volet des options de restauration, choisissez votre type de restauration :
 - Restaurer le cluster EKS complet : restaure l'intégralité du point de récupération composite Amazon EKS
 - Sélectionnez les espaces de noms à restaurer : restaure jusqu'à cinq espaces de noms spécifiques
6. Configurez la destination cible :
 - Pour la restauration du cluster, choisissez de créer un nouveau cluster ou d'utiliser un cluster existant
 - Pour les nouveaux clusters, spécifiez le nom du cluster, la version de Kubernetes, la configuration VPC, les rôles IAM, les sous-réseaux, les groupes de sécurité supplémentaires, les paramètres des groupes de nœuds, les profils fargate et les rôles IAM d'identité du pod
 - Pour les clusters existants, sélectionnez le cluster cible dans la liste déroulante
 - Pour la restauration des espaces de noms, spécifiez le cluster cible et les noms des espaces de noms
7. Configurez éventuellement les paramètres avancés pour un ordre de restauration personnalisé pour les ressources Kubernetes.
8. Choisissez le rôle de restauration IAM pour la tâche. Si vous n'utilisez pas le rôle par défaut, assurez-vous que le rôle sélectionné inclut l'PassRole autorisation iam :.
9. Choisissez Restore backup.

AWS CLI

Utilisez la `aws backup start-restore-job` commande avec les métadonnées spécifiques à Amazon EKS.

Les métadonnées requises dépendent du type de restauration. Toutes les opérations de restauration nécessitent `clusterName` ce paramètre.

Restaurez les points de récupération Amazon EKS via AWS CLI

Utiliser `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon EKS :

Métadonnées obligatoires :

- `clusterName`- Nom du cluster vers lequel effectuer la restauration

Métadonnées facultatives :

- `newCluster`- (vrai/faux) Si nous devons créer un nouveau cluster EKS pendant la restauration
 - Si `NewCluster` est « vrai », les champs de métadonnées suivants s'appliquent :
 - `eksClusterVersion`- Version K8s du cluster souhaitée si vous souhaitez augmenter la version du cluster lors de la restauration
 - `clusterRole`- L'ARN du rôle IAM à associer au cluster EKS créé
 - `clusterVpcConfig`- VPC/Networking configuration pour le cluster EKS créé. Ce champ contient les champs imbriqués suivants :
 - `vpcId`- Le VPC associé à votre cluster
 - `subnetIds`- Les sous-réseaux associés à votre cluster
 - `securityGroupIds`- Les groupes de sécurité supplémentaires associés à votre cluster
 - `nodeGroups`- Les groupes de nœuds gérés à créer sur le cluster EKS. La restauration `NodeGroups` doit avoir tous les mêmes groupes de nœuds depuis la sauvegarde et correspondre `nodeGroupId`.
 - `nodeGroupId`- L'ID du groupe de nœuds
 - `subnetIds`- Les sous-réseaux spécifiés pour le groupe Auto Scaling associé à votre groupe de nœuds
 - `instanceTypes`- Si le groupe de nœuds n'a pas été déployé avec un modèle de lancement, il s'agit du type d'instance associé au groupe de nœuds
 - `nodeRole`- Le rôle IAM associé à votre groupe de nœuds
 - `securityGroupIds`- Le groupe IDs de sécurité autorisé à accéder aux nœuds par SSH

- `remoteAccessEc2SshKey`- Le nom de la clé Amazon EC2 SSH qui permet d'accéder aux communications SSH avec les nœuds du groupe de nœuds gérés
- `fargateProfiles`- Les profils Fargate à créer sur le cluster EKS. Les profils Fargate à restaurer doivent avoir tous les mêmes profils Fargate au moment de la sauvegarde et avoir le même nom.
 - `name`- Le nom du profil Fargate
 - `subnetIds`- Le nombre IDs de sous-réseaux dans lesquels lancer un pod
 - `podExecutionRoleArn`- L'ARN du rôle IAM du rôle d'exécution du Pod à utiliser pour un Pod qui correspond aux sélecteurs du profil Fargate
- `podIdentityAssociations`- Les associations d'identité des pods à créer sur le cluster EKS
 - `associationId`- L'identifiant de l'association Pod Identity
 - `roleArn`- L'ARN du rôle IAM pour la Pod Identity Association
- `kubernetesRestoreOrder`- Remplacez l'ordre dans lequel les manifestes Kubernetes sont restaurés. Cet ordre aura la priorité sur l'ordre de restauration du service par défaut. Cela suit le format suivant `group/version/kind` or `version/kind` :

[« `v1/volumes persistants` », « `v1/pods` », » «] `customresource/v2/custom`

- `namespaceLevelRestore`- (vrai/faux) Si vous souhaitez effectuer une restauration au niveau de l'espace de noms
- `namespaces`- Une liste d'espaces de noms à restaurer si elle `namespaceLevelRestore` est « vraie ». Peut fournir jusqu'à 5 espaces de noms à restaurer
- `restoreKubernetesManifestsOnly`- (vrai/faux) Si vous souhaitez uniquement restaurer les fichiers manifestes Kubernetes et aucun système de stockage persistant (EBS, S3, EFS, etc.)
- `nestedRestoreJobs`- Restaurez la configuration des métadonnées de tous les points de restauration imbriqués pour les systèmes `PersistentVolume` de stockage dans le point de restauration composite. Voici une carte de `RecoveryPointArn` : `RestoreMetadata` de ce point de récupération

Restaurer dans un cluster existant

```
aws backup start-restore-job \
    --recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
```

```
--iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
--metadata '{"clusterName":"existing-
cluster","newCluster":false}' \
--resource-type "EKS"
```

Restaurer vers un nouveau cluster

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-
west-2:123456789012:recovery-point:composite:eks/my-cluster-20240115" \
--iam-role-arn "arn:aws:iam::123456789012:role/
AWSBackupServiceRolePolicyForEKSRestore" \
--metadata '{"clusterName":"new-
cluster","newCluster":true,"clusterRole":"arn:aws:iam::123456789012:role/
EKSClusterRole","eksClusterVersion":"1.33","clusterVpcConfig":{"vpcId
":"vpc-1234","subnetIds":["subnet-1","subnet-2","subnet-3"],
"securityGroupIds":["sg-123"]},"nodeGroups":[{"nodeGroupId":
"nodegroup-1","subnetIds":["subnet-1","subnet-2","subnet-3"],
"nodeRole":"arn:aws:iam::123456789012:role/EKSNodeGroupRole","instanceTypes
":["t3.small"]},"fargateProfiles":[{"name":"fargate-profile-1",
"subnetIds":["subnet-1","subnet-2","subnet-3"],"podExecutionRoleArn":
"arn:aws:iam::123456789012:role/EKSFargateProfileRole"}]}' \
--resource-type "EKS"
```

Après avoir démarré la tâche de restauration, utilisez `describe-restore-job` pour suivre la progression :

```
aws backup describe-restore-job --restore-job-id restore-job-id
```

Vous pouvez vous abonner aux événements de notification pour les objets défaillants ou ignorés à des fins de restauration. Pour plus d'informations, consultez la section [Options de notification avec AWS Backup](#).

Restaurer un système FSx de fichiers

Les options de restauration disponibles lorsque vous les utilisez AWS Backup pour restaurer les systèmes de FSx fichiers Amazon sont les mêmes que lorsque vous utilisez la FSx sauvegarde Amazon native. Vous pouvez utiliser le point de restauration d'une sauvegarde pour créer un nouveau système de fichiers et restaurer un point-in-time instantané d'un autre système de fichiers.

AWS Backup prend en charge la restauration des systèmes de fichiers qui utilisent le stockage par hiérarchisation intelligente FSx pour les systèmes de fichiers Lustre et FSx OpenZFS. Les systèmes de fichiers de hiérarchisation intelligente ont des exigences de configuration spécifiques lors des opérations de restauration.

Lors de la restauration des systèmes de FSx fichiers Amazon, AWS Backup crée un nouveau système de fichiers et le remplit avec les données (Amazon FSx for NetApp ONTAP permet de restaurer un volume dans un système de fichiers existant). Cela est similaire à la façon dont Amazon natif FSx sauvegarde et restaure les systèmes de fichiers. La restauration d'une sauvegarde sur un nouveau système de fichiers prend le même temps que la création d'un nouveau système de fichiers. Les données restaurées à partir de la sauvegarde sont chargées de façon différée dans le système de fichiers. Il se peut donc que vous rencontriez une latence légèrement plus élevée au cours du processus.

Note

Vous ne pouvez pas effectuer de restauration sur un système de FSx fichiers Amazon existant, ni restaurer des fichiers ou des dossiers individuels.

FSx for ONTAP ne prend pas en charge la sauvegarde de certains types de volumes, notamment les volumes DP (protection des données), les volumes LS (partage de charge), les volumes complets ou les volumes situés sur des systèmes de fichiers pleins. Pour plus d'informations, consultez [FSx ONTAP Working with backups](#).

AWS Backup les coffres-forts contenant les points de récupération des systèmes de FSx fichiers Amazon sont visibles à l'extérieur de AWS Backup. Vous pouvez restaurer les points de récupération à l'aide d'Amazon FSx , mais vous ne pouvez pas les supprimer.

Vous pouvez voir les sauvegardes créées par la fonctionnalité de sauvegarde FSx automatique intégrée d'Amazon depuis la AWS Backup console. Vous pouvez également récupérer ces sauvegardes à l'aide de AWS Backup. Cependant, vous ne pouvez pas supprimer ces sauvegardes ni modifier les plannings de sauvegarde automatiques de vos systèmes de FSx fichiers Amazon à l'aide de AWS Backup.

Utiliser la AWS Backup console pour restaurer les points FSx de récupération Amazon

Vous pouvez restaurer la plupart des FSx sauvegardes Amazon créées AWS Backup à l'aide de la AWS Backup console, de l'API ou AWS CLI.

Cette section explique comment utiliser la AWS Backup console pour restaurer les systèmes de FSx fichiers Amazon.

Restauration d'un système de fichiers FSx pour Windows File Server

Pour restaurer un système de fichiers FSx pour Windows File Server

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de FSx ressource Amazon que vous souhaitez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde.
5. Dans la section Informations sur le système de fichiers, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Vous pouvez effectuer une restauration à la fois FSx pour le serveur de fichiers Windows et FSx pour les systèmes de fichiers Lustre.
6. Pour Type de déploiement, acceptez le choix par défaut. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers lors de la restauration.
7. Choisissez le Type de stockage à utiliser. Si la capacité de stockage de votre système de fichiers est inférieure à 2 000 GiO, vous ne pouvez pas utiliser le type de stockage HDD.
8. Pour la capacité de débit, choisissez Capacité de débit recommandée pour utiliser le débit recommandé de 16 Mo par seconde (MBps), ou choisissez Spécifier la capacité de débit et entrez un nouveau débit.
9. Dans la section Réseau et sécurité, fournissez les informations requises.
10. Si vous restaurez un système de fichiers FSx pour serveur de fichiers Windows, fournissez les informations d'authentification Windows utilisées pour accéder au système de fichiers, ou vous pouvez en créer un nouveau.

Note

Lorsque vous restaurez une sauvegarde, vous ne pouvez pas modifier le type d'Active Directory sur le système de fichiers.

Pour plus d'informations sur Microsoft Active Directory, consultez la section [Utilisation d'Active Directory dans le serveur de fichiers Amazon FSx pour Windows](#) dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

11. (Facultatif) Dans la section Sauvegarde et maintenance, fournissez les informations permettant de définir vos préférences de sauvegarde.
12. Dans la section Rôle de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également fournir votre propre rôle IAM.
13. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration d'un système de fichiers Amazon FSx for Lustre

AWS Backup prend en charge les systèmes de fichiers Amazon FSx for Lustre dotés d'un type de déploiement de stockage persistant et qui ne sont pas liés à un référentiel de données tel qu'Amazon S3.

Note

Vous ne pouvez restaurer votre sauvegarde que sur un système de fichiers ayant le même type de déploiement, la même classe de stockage, la même capacité de débit, la même capacité de stockage, le même type de compression de données et AWS la même région que le système d'origine. Vous pouvez augmenter la capacité de stockage de votre système de fichiers restauré une fois qu'il sera disponible.

Pour restaurer un système de fichiers Amazon FSx for Lustre

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de FSx ressource Amazon que vous souhaitez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde vers un nouveau système de fichiers.

5. Dans la section Paramètres, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Le Type de système de fichiers doit être Lustre.
6. Choisissez un type de déploiement. AWS Backup prend uniquement en charge le type de déploiement persistant. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers lors de la restauration.

Le type de déploiement persistant est destiné au stockage à long terme. Pour obtenir des informations détaillées sur FSx les options de déploiement de Lustre, consultez la section [Utilisation des options de déploiement disponibles pour les systèmes de fichiers Amazon FSx pour Lustre](#) dans le guide de l'utilisateur d'Amazon FSx pour Lustre.

7. Choisissez le Débit par unité de stockage que vous souhaitez utiliser.

 Note

Le débit par unité de stockage ne peut pas être configuré pour les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering.

8. (Facultatif) Pour les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering, choisissez le mode et la capacité de dimensionnement du cache de lecture SSD. Pour plus d'informations, consultez la FSx documentation relative à la [gestion du cache de lecture SSD provisionné](#).
9. (Optional) For file systems using Intelligent-Tiering storage class, choose whether to enable EFA (Elastic Fabric Adapter). To enable EFA, make sure that your security group allows all inbound and outbound traffic within the security group.
10. Spécifiez la Capacité de stockage à utiliser. Entrez une capacité comprise entre 32 GiO et 64 436 GiO.

 Note

Pour les systèmes de fichiers Intelligent Tiering, la capacité de stockage est élastique et ne peut pas être spécifiée lors de la restauration. La capacité s'adapte automatiquement en fonction de votre consommation de données.

11. Dans la section Réseau et sécurité, fournissez les informations requises.
12. (Facultatif) Dans la section Sauvegarde et maintenance, fournissez les informations permettant de définir vos préférences de sauvegarde.

13. Dans la section Rôle de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également fournir votre rôle IAM.
14. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration des volumes Amazon FSx pour NetApp ONTAP

Pour restaurer les volumes Amazon FSx for NetApp ONTAP, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de FSx ressource Amazon que vous souhaitez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer.

La première section, Informations sur le système de fichiers, affiche l'ID du point de récupération, l'ID du système de fichiers et le type de système de fichiers.

5. Sous Options de restauration, plusieurs sections s'offrent à vous. Choisissez d'abord le Système de fichiers dans le menu déroulant.
6. Choisissez ensuite la Machine virtuelle de stockage préférée dans le menu déroulant.
7. Entrez un nom pour votre volume.
8. Spécifiez le Chemin de jonction, c'est-à-dire l'emplacement dans votre système de fichiers où votre volume sera monté.
9. Spécifiez la Taille du volume en mégaoctets (Mo) que vous créez.
10. (Facultatif) Vous pouvez choisir Activer l'efficacité de stockage en cochant la case. Cela permettra la déduplication, la compression et le compactage.
11. Dans le menu déroulant Politique de hiérarchisation des groupes de capacité, sélectionnez la préférence de hiérarchisation.
12. Dans Autorisations de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour restaurer les sauvegardes.
13. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration d'un système de fichiers Amazon FSx pour OpenZFS

Note

La restauration depuis une sauvegarde avec une classe de stockage donnée vers un système de fichiers avec une classe de stockage différente n'est pas prise en charge.

Pour restaurer un système FSx de fichiers OpenZFS

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de FSx ressource Amazon que vous souhaitez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde.

Dans la section Informations sur le système de fichiers, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Le type de système de fichiers doit être FSx pour OpenZFS.

5. Sous Options de restauration, vous pouvez sélectionner Restauration rapide ou Restauration standard. La restauration rapide utilisera les paramètres par défaut du système de fichiers source. Si vous effectuez une restauration rapide, passez à l'étape 7.

Si vous choisissez la restauration standard, spécifiez les configurations supplémentaires suivantes :

- a. IOPS SSD provisionnées : vous pouvez choisir la case d'option Automatique ou choisir l'option Provisionné par l'utilisateur si disponible.

Note

Les IOPS des SSD ne peuvent pas être définies pour les systèmes de fichiers utilisant la classe de stockage Intelling-Tiering

- b. Capacité de débit : vous pouvez choisir la capacité de débit recommandée de 64 MB/sec (pour la classe de stockage SSD) et 160 MB/sec (pour la classe de stockage à hiérarchisation intelligente), ou vous pouvez choisir de spécifier la capacité de débit.

- c. (Facultatif) Groupes de sécurité VPC : vous pouvez spécifier des groupes de sécurité VPC à associer à l'interface réseau de votre système de fichiers.
 - d. Clé de chiffrement : Spécifiez la AWS Key Management Service clé pour protéger les données du système de fichiers restaurées au repos.
 - e. (Facultatif) Configuration du volume racine : cette configuration est réduite par défaut. Vous pouvez l'agrandir en cliquant sur le carat pointant vers le bas (flèche). La création d'un système de fichiers à partir d'une sauvegarde créera un nouveau système de fichiers ; les volumes et les instantanés conserveront leurs configurations source.
 - f. (Facultatif) Sauvegarde et maintenance : pour définir une sauvegarde planifiée, cliquez sur le carat pointant vers le bas (flèche) pour développer la section. Vous pouvez choisir la fenêtre de sauvegarde, l'heure et les minutes, la période de rétention et la fenêtre de maintenance hebdomadaire.
6. La Capacité de stockage SDD affichera la capacité de stockage du système de fichiers.

 Note

Pour les systèmes de fichiers Intelligent Tiering, la capacité de stockage est élastique et ne peut pas être spécifiée lors de la restauration. La capacité s'adaptera automatiquement en fonction de votre consommation de données.

7. (Facultatif) Pour les systèmes de fichiers utilisant la classe de stockage Intelligent-Tiering, choisissez le mode et la capacité de dimensionnement du cache de lecture SSD. Pour plus d'informations, consultez la FSx documentation relative à la [gestion du cache de lecture SSD provisionné](#).
8. Choisissez le Cloud privé virtuel (VPC) à partir duquel votre système de fichiers est accessible.
9. Dans le menu déroulant Sous-réseau, choisissez le sous-réseau dans lequel réside l'interface réseau de votre système de fichiers.
10. Dans la section Rôle de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également choisir un rôle IAM.
11. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de FSx restauration Amazon

Pour restaurer Amazon à FSx l'aide de l'API ou de la CLI, utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors d'une FSx restauration Amazon :

```
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

Note

La capacité de stockage ne peut pas être spécifiée pour les systèmes de fichiers à hiérarchisation intelligente, car ils utilisent un stockage élastique qui évolue automatiquement en fonction de l'utilisation des données.

FSx pour restaurer les métadonnées du serveur de fichiers Windows

Vous pouvez spécifier les métadonnées suivantes lors d'une restauration FSx pour Windows File Server :

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx pour les métadonnées de restauration Lustre

Vous pouvez spécifier les sous-champs suivants `LustreConfiguration` dans les métadonnées lors d'une restauration FSx pour Lustre :

- `PerUnitStorageThroughput`- Spécifie la capacité de débit par unité de stockage provisionnée, mesurée par MB/s TiB de stockage.
- `DriveCacheType`- Type de cache de disque utilisé par les systèmes de `PERSISTENT_1` fichiers équipés de périphériques de stockage sur disque dur. Ce paramètre est obligatoire quand `StorageType` est défini sur `HDD`.
- `DataReadCacheConfiguration`- Spécifie le cache de lecture SSD provisionné pour les systèmes de fichiers Intelligent Tiering. Obligatoire lorsque `StorageType` est défini sur `INTELLIGENT_TIERING`. Voir [LustreReadCacheConfiguration](#) pour plus de détails.
- `EfaEnabled`- Spécifie si le support Elastic Fabric Adapter (EFA) GPUDirect et Storage (GDS) est activé pour FSx le système de fichiers for Lustre.

Pour obtenir des informations complètes sur tous les paramètres disponibles dans `LustreConfiguration`, consultez [CreateFileSystemLustreConfiguration](#) le Amazon FSx API Reference.

FSx pour les métadonnées de restauration ONTAP

Vous pouvez spécifier les métadonnées suivantes lors d'une restauration FSx pour ONTAP :

- Nom `#name` du volume à créer
- `OntapConfiguration`: # configuration ontap
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx pour les métadonnées de restauration OpenZFS

Vous pouvez spécifier les sous-champs suivants `OpenZFSConfiguration` dans les métadonnées lors d'une restauration FSx pour OpenZFS :

- **ThroughputCapacity**- Spécifie la capacité de débit du système de fichiers restauré, mesurée en Mo/s.
- **DiskIopsConfiguration**- Lorsque vous spécifiez des lops pour la classe de stockage SSD, utilisez une valeur comprise entre 0 et 160 000. N'incluez pas le mode lorsque lops est spécifié.
- **ReadCacheConfiguration**- Spécifie le cache de lecture SSD provisionné pour les systèmes de fichiers Intelligent Tiering. Obligatoire lorsque **StorageType** est défini sur **INTELLIGENT_TIERING**. Voir [Ouvrir ZFSRead CacheConfiguration](#) pour plus de détails.

Pour obtenir des informations complètes sur tous les paramètres disponibles dans **OpenZFSConfiguration**, consultez [CreateFileSystemOpenZFSConfiguration](#) le Amazon FSx API Reference.

Exemple de commande de restauration d'une interface de ligne de commande :

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-type "FSx" --region us-west-2 --metadata 'SubnetIds=["subnet-1234","subnet-5678"]',StorageType=HDD,SecurityGroupIds=["sg-bb5efdc4","sg-0faa52"]',WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\", \"PreferredSubnetId\": \"subnet-1234\", \"ThroughputCapacity\": \"32\"}"'
```

Exemple de métadonnées de restauration :

```
"restoreMetadata": "{ \"StorageType\": \"SSD\", \"KmsKeyId\": \"arn:aws:kms:us-east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\", \"StorageCapacity\": \"1200\", \"VpcId\": \"vpc-0ab0979fa431ad326\", \"FileSystemType\": \"LUSTRE\", \"LustreConfiguration\": \"{ \\\"WeeklyMaintenanceStartTime\\\": \\\"4:10:30\\\", \\\"DeploymentType\\\": \\\"PERSISTENT_1\\\", \\\"PerUnitStorageThroughput\\\": 50, \\\"CopyTagsToBackups\\\": true }\", \"FileSystemId\": \"fs-0ca11fb3d218a35c2\", \"SubnetIds\": [ \\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Restaurer un cluster Neptune

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon Neptune

La restauration d'une base de données Amazon Neptune nécessite la spécification de plusieurs options de restauration. Pour plus d'informations sur ces options, consultez [Restauration à partir d'un instantané de cluster de bases de données](#) dans le Guide du développeur Amazon DocumentDB.

Pour restaurer une base de données Neptune

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Neptune que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications d'instance, acceptez les valeurs par défaut ou spécifiez le Moteur de base de données et la Version.
5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de cluster de base de données que vous Compte AWS possédez dans la région actuelle. L'identifiant de cluster de base de données n'est pas sensible à la casse, mais il est stocké intégralement en minuscules, comme dans `mydbclusterinstance`. Ce champ est obligatoire.
6. Dans le volet Options de base de données, acceptez les valeurs par défaut ou spécifiez les options pour Port de la base de données et Groupe de paramètres de cluster de base de données.
7. Dans le volet Chiffrement, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le chiffrement ou Désactiver le chiffrement.
8. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.
9. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
10. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

11. Une fois votre restauration terminée, attachez votre cluster Neptune restauré à une instance Amazon RDS.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Neptune

Restaurez d'abord votre cluster. Utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon DocumentDB :

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
scalingConfiguration
vpcSecurityGroupIds // string
```

Ensuite, attachez votre cluster Neptune restauré à une instance Amazon RDS à l'aide de `create-db-instance`

- Pour Linux, macOS ou Unix :

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                               --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Pour Windows :

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                               --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

Pour plus d'informations, consultez [RestoreDBClusterFromSnapshot](#) dans la Référence de l'API de gestion Neptune et [restore-db-cluster-from-snapshot](#) dans le Guide de l'interface de ligne de commande Neptune.

Restaurer une base de données RDS

La restauration d'une base de données Amazon RDS nécessite la spécification de plusieurs options de restauration. Pour plus d'informations sur ces options, consultez [Sauvegarde et restauration d'une instance de base de données Amazon RDS](#) dans le Guide de l'utilisateur Amazon RDS.

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon RDS

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon RDS que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications de l'instance, acceptez les valeurs par défaut ou spécifiez les options dont vous avez besoin.
5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de base de données et les clusters que vous Compte AWS possédez dans la région actuelle. L'identifiant d'instance de base de données n'est pas sensible à la casse, mais il est stocké intégralement en minuscules, comme dans mydbinstance. Ce champ est obligatoire.
6. Dans le volet Réseau et sécurité, acceptez les valeurs par défaut ou spécifiez les options dont vous avez besoin.
7. Dans le volet des options de base de données, acceptez les valeurs par défaut ou spécifiez les options dont vous avez besoin.
8. Dans le volet Chiffrement, utilisez les paramètres par défaut. Si l'instance de base de données source de l'instantané a été chiffrée, l'instance de base de données restaurée est également chiffrée. Ce chiffrement ne peut pas être supprimé.
9. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.

10. Dans le volet Maintenance, acceptez la valeur par défaut ou spécifiez la valeur du paramètre Mise à niveau automatique des versions mineures.
11. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
12. Choisissez Restore backup.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon RDS

Utilisez [StartRestoreJob](#). Pour plus d'informations sur les métadonnées et les valeurs acceptées, consultez [RestoreDBInstanceFromDBSnapshot](#) et [RestoreDBInstanceToPointInTime](#) dans le manuel Amazon RDS API Reference. AWS Backup Accepte en outre les attributs informatifs suivants. Cependant, leur inclusion n'affectera pas la restauration :

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Restauration d'un cluster Amazon Redshift

Vous pouvez restaurer des instantanés automatisés et manuels dans la AWS Backup console ou via la CLI.

Lorsque vous restaurez un cluster Amazon Redshift, les paramètres du cluster d'origine sont saisis par défaut dans la console. Vous pouvez définir différents paramètres pour les configurations ci-dessous. Lors de la restauration d'une table, vous devez spécifier les bases de données source et cible. Pour plus d'informations sur ces configurations, consultez [Restauration d'un cluster à partir d'un instantané](#) dans le Guide de gestion Amazon Redshift.

- Table unique ou cluster : vous pouvez choisir de restaurer un cluster entier ou une seule table. Si vous choisissez de restaurer une seule table, la base de données source, le schéma source et le nom de la table source sont nécessaires, ainsi que le cluster cible, le schéma et le nouveau nom de table.

- Type de nœud : chaque cluster Amazon Redshift est composé d'un nœud principal et d'au moins un nœud de calcul. Lorsque vous restaurez un cluster, vous devez spécifier le type de nœud qui répond à vos exigences en matière de processeur, de RAM, de capacité de stockage et de type de lecteur.
- Nombre de nœuds : lorsque vous restaurez un cluster, vous devez spécifier le nombre de nœuds nécessaires.
- Récapitulatif de configuration
- Autorisations du cluster

Pour restaurer un cluster ou une table Amazon Redshift à l'aide de la console AWS Backup

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Paramètres et l'ID de ressource Amazon Redshift que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Points de récupération, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Options de restauration
 - a. Restaurez un cluster à partir d'un instantané, ou
 - b. Restaurez une table unique dans un instantané sur un nouveau cluster. Si vous choisissez cette option, vous devez configurer les éléments suivants :
 - i. Activez ou désactivez les noms sensibles à la casse.
 - ii. Entrez les valeurs de la table source, y compris la base de données, le schéma et la table. Les informations de la table source se trouvent dans la console [Amazon Redshift](#).
 - iii. Entrez les valeurs de la table cible, y compris la base de données, le schéma et le nouveau nom de la table.
5. Spécifiez les nouveaux paramètres de configuration de votre cluster.
 - a. Pour la restauration du cluster : choisissez l'identifiant du cluster, le type de nœud et le nombre de nœuds.
 - b. Spécifiez la zone de disponibilité et les fenêtres de maintenance.

- c. Vous pouvez associer des rôles supplémentaires en cliquant sur Associer des rôles IAM.
6. Facultatif : configurations supplémentaires :
- a. L'option Utiliser la valeur par défaut est activée par défaut.
 - b. Utilisez les menus déroulants pour sélectionner les paramètres de mise en réseau et de sécurité, les groupes de sécurité VPC, le groupe de sous-réseaux du cluster et la zone de disponibilité.
 - c. Activez ou désactivez Routage VPC amélioré.
 - d. Déterminez si vous souhaitez rendre le point de terminaison de votre cluster accessible au public. Si tel est le cas, les instances et les appareils extérieurs au VPC peuvent se connecter à votre base de données via le point de terminaison du cluster. Si cette option est activée, entrez l'adresse IP élastique.
7. Facultatif : configuration de la base de données. Vous pouvez choisir de saisir
- a. Port de base de données (en tapant dans le champ de texte)
 - b. Groupes de paramètres
8. Maintenance : vous pouvez choisir
- a. Fenêtre de maintenance
 - b. Suivi de la maintenance, que ce soit en cours, finie ou en aperçu. Cela contrôle la version du cluster qui est appliquée au cours d'une fenêtre de maintenance.
9. L'instantané automatique est défini par défaut.
- a. Période de rétention de l'instantané automatique. La période de rétention doit être comprise entre 0 et 35 jours. Choisissez 0 pour ne pas créer d'instantanés automatiques.
 - b. La période de rétention manuelle des instantanés est de 1 à 3 653 jours.
 - c. Il existe une case à cocher facultative pour la relocalisation du cluster. Si cette case est cochée, cela permet de relocaliser votre cluster dans une autre zone de disponibilité. Une fois que vous avez activé la relocalisation, vous pouvez utiliser le point de terminaison d'un VPC.
10. Surveillance : après la restauration d'un cluster, vous pouvez configurer la surveillance via Amazon Redshift CloudWatch ou Amazon Redshift.
11. Choisissez le rôle IAM à transmettre pour effectuer des restaurations. Vous pouvez utiliser le rôle par défaut ou en spécifier un autre.

Vos tâches de restauration seront visibles sous Tâches. Vous pouvez consulter le statut actuel de votre tâche de restauration en cliquant sur le bouton d'actualisation ou sur CTRL-R.

Restauration d'un cluster Amazon Redshift à l'aide d'une API, d'une interface de ligne de commande ou d'un kit SDK

Utilisez [StartRestoreJob](#) pour restaurer un cluster Amazon Redshift.

Pour restaurer un Amazon Redshift à l'aide de AWS CLI, utilisez la commande `start-restore-job` et spécifiez les métadonnées suivantes :

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
```

```
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE or TABLE_RESTORE or NAMESPACE_RESTORE
```

Pour plus d'informations, consultez [RestoreFromClusterSnapshot](#) dans la Référence de l'API Amazon Redshift et [restore-from-cluster-snapshot](#) dans le Guide de l'AWS CLI .

Voici un exemple de modèle :

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name" \
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region Région AWS
-\-endpoint-url URL
```

Voici un exemple :

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

Vous pouvez également utiliser [DescribeRestoreJob](#) pour vous aider à obtenir des informations de restauration.

Dans le AWS CLI, utilisez l'opération `describe-restore-job` et utilisez les métadonnées suivantes :

Region

Voici un exemple de modèle :

```
aws backup describe-restore-job --restore-job-id restore job ID
-\-region Région AWS
```

Voici un exemple :

```
aws backup describe-restore-job --restore-job-id BEA3B353-576C-22C0-9E99-09632F262620 \
--region us-west-2 \
```

Restauration sans serveur Amazon Redshift

Vous pouvez restaurer des instantanés manuels de bases de données ou de tables à l'aide de la AWS Backup console ou AWS CLI.

Redshift Serverless prend en AWS Backup charge la restauration interchangeable pour les instantanés d'entrepôts de données. Cela signifie que vous pouvez restaurer des sauvegardes Redshift Serverless sur des [clusters provisionnés par Amazon Redshift ou restaurer des sauvegardes provisionnées](#) sur des espaces de noms Redshift Serverless. Cela s'applique uniquement à la restauration complète de la base de données, et non à la restauration d'une seule table.

Capacités de restauration pour Redshift Serverless

Capacités de restauration	Namespace	Table individuelle
Type de cliché	Manuelle	Manuelle
Informations nécessaires	- Aperçu de la source - Espace de noms cible - WorkGroup	- Aperçu de la source - Base de données source - Nom de la table source - Base de données cible - Nouveau nom de table
Restaurer l'effet cible	Restaure un espace de noms existant par le biais d'une restauration destructive qui remplace les données existantes	Restaure une nouvelle table
Restauration interchangeable ?	Oui. Les sauvegardes Redshift Serverless peuvent être	Non pris en charge.

Capacités de restauration	Namespace	Table individuelle
	restaurées sur des clusters provisionnés par Amazon Redshift. • Les sauvegardes provisionnées par Amazon Redshift peuvent être restaurées sur des clusters Redshift Serverless.	

Pour plus d'informations sur les configurations, consultez la section [Snapshots and recovery points](#) dans le guide de gestion Amazon Redshift.

Considérations avant la restauration

Avant de commencer une tâche de restauration, passez en revue les points suivants :

Configurations

Lorsque vous restaurez un instantané Redshift Serverless, vous choisissez l'espace de noms cible dans lequel vous souhaitez restaurer toutes les bases de données ou une seule table.

Lorsque vous restaurez les bases de données d'un instantané dans un espace de noms sans serveur, il s'agit d'une restauration destructive. Cela signifie que toutes les données existantes dans l'espace de noms de restauration cible sont remplacées lorsque vous effectuez une restauration dans cet espace de noms.

Lorsque vous restaurez une seule table, il ne s'agit pas d'une restauration destructive. Pour restaurer une table, spécifiez le groupe de travail, le snapshot, la base de données source, la table source, l'espace de noms de restauration cible et le nom de la nouvelle table.

Autorisations

Les autorisations requises sont déterminées par l'entrepôt de données cible (c'est-à-dire l'espace de noms ou le cluster provisionné dans lequel vous allez restaurer les bases de données ou les tables). Le tableau suivant peut vous aider à déterminer les autorisations, le rôle et la politique à utiliser. Pour plus d'informations sur la gestion des politiques IAM, consultez la section [Gestion des identités et des accès dans Amazon Redshift](#).

Autorisations et rôles requis pour les opérations de restauration

Restaurer la cible	Autorisations nécessaires	Rôle et politique de l'IAM
Cluster provisionné Amazon Redshift	<code>redshift:RestoreFromClusterSnapshot</code>	<code>AWSBackupServiceRolePolicyForRestores</code> contient cette autorisation ; elle peut être utilisée pour <code>aws backup start-restore-job</code> .
Espace de noms Redshift Serverless	<code>redshift-serverless:RestoreFromSnapshot</code>	Vous devez ajouter cette autorisation au rôle et à la politique que vous utiliserez pour appeler <code>aws backup start-restore-job</code>. Comme il s'agit d'une tâche de restauration destructrice, la politique de rôle de service pour les restaurations ne peut pas être utilisée.

Procédure de restauration Redshift Serverless

Suivez ces étapes pour restaurer les sauvegardes Redshift Serverless à l'aide de la AWS Backup console ou : AWS CLI

Console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Paramètres et sélectionnez l'ID de ressource Redshift Serverless à restaurer.
3. Sur la page Détails de la ressource, sélectionnez l'ID du point de récupération dans le volet Points de restauration, puis choisissez Restaurer.
4. Dans le volet des options de restauration, choisissez de restaurer l'intégralité de l'entrepôt de données ou une seule table.
5. Sélectionnez la cible de destination dans le volet de configuration de l'entrepôt de données cible.
 - Pour une restauration complète de l'entrepôt de données, choisissez entre le cluster provisionné Amazon Redshift ou l'espace de noms Redshift Serverless.

- Pour la restauration d'une seule table, spécifiez l'instantané source, la base de données, le schéma, le nom de la table et les détails de la cible.
6. Choisissez le rôle de restauration IAM pour la tâche. Si vous n'utilisez pas le rôle par défaut, assurez-vous que le rôle sélectionné inclut l'`iam:PassRole` autorisation.

AWS CLI

Utilisez la commande `aws backup start-restore-job`.

AWS Backup fonctionne avec Redshift Serverless pour orchestrer la tâche de restauration. La commande CLI sera précédée par des métadonnées pertinentes pour Redshift Serverless ou Amazon Redshift, `aws backup` mais elle contiendra également ces métadonnées.

Les métadonnées obligatoires et facultatives varient selon que vous restaurez un entrepôt de données complet ou une seule table.

- Pour la restauration d'une seule table, voir [restore-table-from-snapshot](#) la référence des AWS CLI commandes.
- Pour la restauration de l'espace de noms, voir [restore-from-snapshot](#) la référence des AWS CLI commandes.
- Pour effectuer une restauration sur un cluster provisionné par Amazon Redshift, consultez la AWS CLI référence des [restore-from-cluster-snapshot](#) commandes.

Exemple modèle pour **start-restore-job** effectuer une restauration dans un espace de noms sans serveur :

```
aws backup start-restore-job \  
--recovery-point-arn "arn:aws:backup:region:account:snapshot:name--iam-role-arn  
"arn:aws:iam:account:role/role-name" \  
--metadata \  
--resource-type Redshift Serverless \  
--region Region \  
--endpoint-url URL
```

Exemple Exemple de restauration **start-restore-job** vers un espace de noms sans serveur :

```
aws backup start-restore-job \  
--recovery-point-arn "arn:aws:redshift-serverless:us-east-1:123456789012:snapshot/  
a12bc34d-567e-890f-123g-h4ijk56l78m9" \  

```

```
--iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \  
--metadata 'RestoreType=NAMESPACE_RESTORE,NamespaceIdentifier=redshift-namespace-1-  
restore' \  
--resource-type "RedshiftServerless" \  
--region us-west-2
```

Après avoir démarré le travail de restauration, utilisez-le `describe-restore-job` pour suivre la progression.

Restaurer une base de données SAP HANA sur une instance Amazon EC2

Les bases de données SAP HANA sur EC2 les instances peuvent être restaurées à l'aide de la AWS Backup console, de l'API ou de. AWS CLI

Rubriques

- [Restaurer une base de données SAP HANA à l'aide de la console AWS Backup](#)
- [StartRestoreJob API pour SAP HANA sur EC2](#)
- [CLI pour SAP HANA sur EC2](#)
- [Restauration de la haute disponibilité \(HA\) de SAP HANA](#)
- [Résolution des problèmes](#)

Restaurer une base de données SAP HANA à l'aide de la console AWS Backup

Notez que les tâches de sauvegarde et de restauration impliquant la même base de données ne peuvent pas être exécutées simultanément. Lorsqu'une tâche de restauration de base de données SAP HANA est en cours, les tentatives de sauvegarde de la même base de données peuvent entraîner le message d'erreur suivant : « Impossible de sauvegarder la base de données tant qu'elle est arrêtée ».

1. Accédez à la AWS Backup console à l'aide des informations d'identification fournies dans les prérequis.
2. Dans le menu déroulant Emplacement de restauration cible, choisissez une base de données à remplacer par le point de récupération que vous utilisez pour la restauration (notez que l'instance hébergeant la base de données cible de restauration doit également disposer des autorisations des conditions préalables).

⚠ Important

Les restaurations de bases de données SAP HANA sont destructrices. La restauration d'une base de données remplacera la base de données à l'emplacement de restauration cible spécifié.

3. Suivez cette étape uniquement si vous effectuez une restauration de copie du système ; sinon, passez à l'étape 4.

Les restaurations de copies du système sont des tâches de restauration qui restaurent vers une base de données cible différente de la base de données source qui a généré le point de récupération. Pour les restaurations de copies du système, notez la commande `aws ssm-sap put-resource-permission` qui vous est fournie sur la console. Cette commande doit être copiée, collée et exécutée sur la machine qui a rempli les conditions préalables. Lorsque vous exécutez la commande, utilisez les informations d'identification du rôle dans les conditions préalables où vous configurez les autorisations requises pour l'enregistrement des applications.

```
// Example command
aws ssm-sap put-resource-permission \
--region us-east-1 \
--action-type RESTORE \
--source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
--resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
```

4. Une fois que vous avez choisi l'emplacement de restauration, vous pouvez voir l'ID de ressource de la base de données cible, le nom de l'application, le type de base de données et l'EC2instance.
5. Vous pouvez éventuellement étendre les paramètres de restauration avancés pour modifier l'option de restauration de votre catalogue. Les options disponibles varient en fonction des paramètres de restauration sélectionnés.
6. Cliquez sur Restaurer la sauvegarde.
7. L'emplacement cible sera remplacé lors de la restauration (« restauration destructive »). Vous devez donc confirmer que vous l'autorisez dans la boîte de dialogue contextuelle suivante.
 - a. Pour continuer, vous devez comprendre que la base de données existante sera remplacée par celle que vous restaurez.

- b. Une fois que cela est compris, vous devez reconnaître que les données existantes seront remplacées. Pour confirmer cela et continuer, tapez remplacer dans le champ de saisie de texte.
8. Cliquez sur Restaurer la sauvegarde.

Si la procédure est réussie, une bannière bleue s'affiche en haut de la console. Cela signifie que la tâche de restauration est en cours. Vous serez automatiquement redirigé vers la page Tâches où votre tâche de restauration apparaîtra dans la liste des tâches de restauration. Cette tâche la plus récente aura le statut Pending. Vous pouvez rechercher, puis cliquer sur l'ID de la tâche de restauration pour voir les détails de chaque tâche de restauration. Vous pouvez actualiser la liste des tâches de restauration en cliquant sur le bouton d'actualisation pour afficher les modifications apportées au statut des tâches de restauration.

[StartRestoreJob API](#) pour SAP HANA sur EC2

Cette action récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN).

Syntaxe de la demande

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
  "IdempotencyToken": "string",
  "Metadata": {
    "string" : "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

Paramètres de demande URI : la demande n'utilise pas de paramètres URI.

Corps de la requête : la demande accepte les données suivantes au format JSON :

IdempotencyTokenChaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques. StartRestoreJob Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Metadonnées

Un ensemble de paires clé-valeur de métadonnées. Contient des informations, telles que le nom de la ressource, nécessaires pour restaurer un point de récupération. Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Par exemple, vous devrez peut-être fournir un nouveau nom de ressource si l'original existe déjà.

Vous devez inclure des métadonnées spécifiques pour restaurer une EC2 instance SAP HANA sur Amazon. Consultez les [StartRestoreJob métadonnées des](#) éléments spécifiques à SAP HANA.

Pour récupérer les métadonnées pertinentes, vous pouvez utiliser l'appel [GetRecoveryPointRestoreMetadata](#).

Exemple de point de récupération de base de données SAP HANA standard :

```
"RestoreMetadata": {
  "BackupSize": "1660948480",
  "DatabaseName": "DATABASENAME",
  "DatabaseType": "SYSTEM",
  "HanaBackupEndTime": "1674838362",
  "HanaBackupId": "1234567890123",
  "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
  "HanaBackupStartTime": "1674838349",
  "HanaVersion": "2.00.040.00.1553674765",
  "IsCompressedBySap": "FALSE",
  "IsEncryptedBySap": "FALSE",
  "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/DB/DATABASENAME",
  "SystemDatabaseSid": "HDB",
  "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
}
```

Exemple de point de récupération d'une base de données SAP HANA en continu :

```
"RestoreMetadata": {
  "AvailableRestoreBases":
    "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
  "BackupSize": "1711284224",
}
```

```

    "DatabaseName": "DATABASENAME",
    "DatabaseType": "TENANT",
    "EarliestRestorablePitrTimestamp": "1674764799789",
    "HanaBackupEndTime": "1668032687",
    "HanaBackupId": "1234567890123",
    "HanaBackupPrefix": "1234567890123_HDB_FULL",
    "HanaBackupStartTime": "1668032667",
    "HanaVersion": "2.00.040.00.1553674765",
    "IsCompressedBySap": "FALSE",
    "IsEncryptedBySap": "FALSE",
    "LatestRestorablePitrTimestamp": "1674850299789",
    "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
    "SystemDatabaseSid": "HDB",
    "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
  }

```

CLI pour SAP HANA sur EC2

La commande `start-restore-job` récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN). L'interface de ligne de commande suivra les directives de l'API ci-dessus.

Résumé :

```

start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]

```



```
[--ca-bundle value]  
[--cli-read-timeout value]  
[--cli-connect-timeout value]
```

Options

`--recovery-point-arn` (chaîne) est une chaîne sous la forme d'un Amazon Resource Number (ARN) qui identifie de manière unique un point de récupération ; par exemple `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata` (map) : un ensemble de paires clé-valeur de métadonnées. Contient des informations, telles que le nom de la ressource, nécessaires pour restaurer un point de récupération. Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Vous devez spécifier des métadonnées spécifiques pour restaurer une EC2 instance SAP HANA sur Amazon :

- `aws:backup:request-id` : il s'agit de n'importe quelle chaîne UUID utilisée pour l'idempotence. Cela ne modifie en rien votre expérience de restauration.
- `aws:backup:TargetDatabaseArn` : spécifiez la base de données dans laquelle vous souhaitez effectuer la restauration. Il s'agit de l'ARN de la base de EC2 données SAP HANA sur Amazon.
- `CatalogRestoreOption` : spécifiez d'où vous souhaitez restaurer votre catalogue. Il doit s'agir de `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP` ou `CATALOG_FROM_LOCAL_PATH`.
- `LocalCatalogPath`: Si la valeur `CatalogRestoreOption` des métadonnées est `CATALOG_FROM_LOCAL_PATH`, spécifiez le chemin d'accès au catalogue local sur votre EC2 instance. Il doit s'agir d'un chemin de fichier valide dans votre EC2 instance.
- `RecoveryType` : actuellement, les types de récupération `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` et `MOST_RECENT_TIME_RECOVERY` sont pris en charge.

clé = (chaîne) ; valeur = (chaîne). Syntaxe raccourcie :

```
KeyName1=string,KeyName2=string
```

Syntaxe JSON :

```
{"string": "string"}
```

```
...}
```

--idempotency-token est une chaîne choisie par l'utilisateur que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartRestoreJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

--resource-type est une chaîne qui lance une tâche de restauration d'un point de restauration pour l'une des ressources suivantes : SAP HANA on Amazon EC2 pour SAP HANA sur Amazon EC2. Facultatif Les ressources SAP HANA peuvent être balisées à l'aide de la commande `aws ssm-sap tag-resource`

Sortie : `RestoreJobId` est une chaîne identifiant de manière unique la tâche qui restaure un point de récupération.

Restauration de la haute disponibilité (HA) de SAP HANA

Des considérations importantes et des étapes supplémentaires doivent être prises en compte lors de la restauration d'un système de haute disponibilité (HA) de SAP HANA. Développez la section ci-dessous qui correspond le mieux à votre cas d'utilisation.

Scénario de restauration :

Base de données système vers une cible SAP HANA HA

Avant de procéder à la restauration sur le système SAP HANA HA cible (de destination),

1. Si un cluster est installé, mettez toutes les notes du cluster en mode Maintenance.
2. Arrêtez la base de données SAP HANA sur tous les nœuds, y compris le nœud principal et le nœud secondaire.
3. (Recommandé) Désactivez tous les plans de sauvegarde pour vous assurer qu'ils n'interfèrent pas avec l'opération de restauration.

Une fois le travail de restauration terminé, accédez au système SAP HANA HA restauré, puis :

1. Démarrez la base de données SAP HANA en mode principal.
2. Démarrez manuellement toute base de données mutualisée dans laquelle la base de données système a été restaurée mais dont les locataires n'ont pas été restaurés.
3. Rétablissez la réplication du système SAP HANA (HSR) entre les nœuds principal et secondaire.

4. Démarrez la base de données SAP HANA sur le nœud secondaire.
5. Si un cluster est installé, assurez-vous que tous les nœuds du cluster sont en ligne.
6. Activez tous les plans de sauvegarde que vous avez désactivés avant l'opération de restauration.

(Facultatif) Vous pouvez synchroniser l'application sur [AWS Systems Manager for SAP](#) en appelant [StartApplicationRefresh](#), ou vous pouvez attendre l'actualisation planifiée de l'application qui fournira les dernières métadonnées SAP.

Base de données système vers une cible à nœud unique SAP HANA

Avant de commencer une tâche de restauration, accédez au système SAP HANA à nœud unique cible, puis :

1. Arrêtez la base de données SAP HANA sur le système SAP HANA cible.
2. (Recommandé) Désactivez tous les plans de sauvegarde pour vous assurer qu'ils n'interfèrent pas avec l'opération de restauration.

Une fois la tâche de restauration terminée, accédez au système SAP HANA à nœud unique cible, puis :

1. Démarrez SAP HANA sur le système SAP HANA cible.
2. Démarrez manuellement chaque base de données mutualisée sur le nœud cible.
3. Activez tous les plans de sauvegarde que vous avez désactivés avant l'opération de restauration.

(Facultatif) Vous pouvez synchroniser l'application sur [AWS Systems Manager for SAP](#) en appelant [StartApplicationRefresh](#), ou vous pouvez attendre l'actualisation planifiée de l'application qui fournira les dernières métadonnées SAP.

Base de données des locataires (sur place ou copie du système)

Avant de démarrer une tâche de restauration, accédez au système SAP HANA cible, puis :

1. (Facultatif, mais recommandé) Mettez tous les clusters installés en mode maintenance pour éviter une prise de contrôle inattendue lors de l'opération de restauration.
2. Assurez-vous que la base de données du système fonctionne sur le système SAP HANA cible.

3. (Recommandé) Désactivez tous les plans de sauvegarde pour vous assurer qu'ils n'interfèrent pas avec l'opération de restauration.

Une fois le travail de restauration terminé :

- Activez tous les plans de sauvegarde que vous avez désactivés avant l'opération de restauration.

Résolution des problèmes

Si l'une des erreurs suivantes se produit lors d'une tentative de sauvegarde, consultez la résolution associée.

- Erreur : erreur du journal de sauvegarde continue

Afin de conserver les points de récupération pour les sauvegardes continues, des journaux sont créés par SAP HANA pour toutes les modifications. Lorsque les journaux ne sont pas disponibles, le statut de chacun de ces points de récupération continue est STOPPED. Le dernier point de récupération viable pouvant être utilisé pour la restauration est celui dont le statut est AVAILABLE. Si les données du journal sont manquantes pour la période entre les points de récupération dotés d'un statut STOPPED et les points dotés d'un statut AVAILABLE, il n'est pas possible de garantir la réussite de la restauration. Si vous entrez une date et une heure comprises dans cette plage, il AWS Backup tentera de faire la sauvegarde, mais utilisera l'heure de restauration disponible la plus proche. Cette erreur sera affichée par le message "Encountered an issue with log backups. Please check SAP HANA for details."

Résolution : dans la console, l'heure de restauration la plus récente, basée sur les journaux, est affichée. Vous pouvez saisir une heure plus récente que l'heure indiquée. Toutefois, si les données relatives à cette période ne sont pas disponibles dans les journaux, AWS Backup nous utiliserons la date de restauration la plus récente.

- Erreur : Internal error

Solution : créez un dossier d'assistance depuis votre console ou contactez votre interlocuteur en Support fournissant les détails de votre restauration, tels que l'identifiant de la tâche de restauration.

- Erreur : The provided role arn:aws:iam::**ACCOUNT_ID**:role/ServiceLinkedRole cannot be assumed by AWS Backup

Résolution : assurez-vous que le rôle assumé lors de l'appel de restauration dispose des autorisations requises pour créer des rôles liés au service.

- Erreur : User: arn:aws:sts::**ACCOUNT_ID**:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:**ACCOUNT_ID**:...

Résolution : assurez-vous que le rôle assumé lors de l'appel des autorisations de restauration décrites dans les conditions préalables est correctement entré.

- Erreur : b* 449: recovery strategy could not be determined: [111014]
The backup with backup id '1660627536506' cannot be used for recovery
SQLSTATE: HY000\n

Résolution : assurez-vous que l'agent Backint a été correctement installé. Vérifiez tous les prérequis, en particulier [Installer AWS BackInt l'agent et AWS Systems Manager pour SAP](#) sur votre serveur d'applications SAP, puis réessayez d'installer l' BackInt agent.

- Erreur : IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED

Résolution : la tâche de restauration a été annulée par le flux de travail du service. Réessayez la tâche de restauration.

- Erreur : problème rencontré lors de la restauration d'une base de données client sur un système SAP HANA High Availability : b* -10709: Connection failed (RTE:[89006] System call 'connect' failed, rc=111:Connection refused ([::1]:40404 # localhost:30013))\n

Solution : Vérifiez SAP HANA pour vous assurer que le SYSTEMDB est opérationnel.

- Erreur : b'* 448: recovery could not be completed: [301102] exception 301153: Sending root key to secondary failed: connection refused. This may be caused by a stopped system replication secondary. Please keep the secondary online to receive the restored root key. Alternatively you could unregister the secondary site in case of an urgent recovery.\n SQLSTATE: HY000\n'

Solution : Sur un système SAP HANA High Availability, il est possible que SAP HANA ne soit pas exécuté sur le nœud secondaire pendant qu'une opération de restauration active est en

cours d'exécution. Démarrez SAP HANA sur le nœud secondaire, puis réessayez la tâche de restauration.

- Erreur: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out`

Résolution : une instabilité transitoire du réseau se produit sur l'instance. Réessayez la restauration. Si ce problème se produit régulièrement, essayez d'ajouter `ForceRetry: "true"` au fichier de configuration de l'agent à l'adresse `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Pour tout autre problème lié à l'agent AWS Backint, reportez-vous à la section [Résoudre les problèmes liés à AWS l'agent Backint](#) pour SAP HANA.

Restaurez les données S3 à l'aide de AWS Backup

Vous pouvez restaurer les données S3 que vous avez sauvegardées AWS Backup à l'aide de la classe de stockage S3 Standard. Vous pouvez restaurer tous les objets d'un compartiment ou des objets spécifiques. Vous pouvez les restaurer dans un compartiment existant ou nouveau.

Autorisations de restauration Amazon S3

Avant de commencer à restaurer les ressources, assurez-vous que le rôle que vous utilisez dispose des autorisations suffisantes.

Pour plus d'informations, consultez les entrées suivantes sur les politiques :

1. [AWSBackupServiceRolePolicyForS3Restore](#)
2. [AWSBackupServiceRolePolicyForRestores](#)
3. [Politiques gérées pour AWS Backup](#)

Considérations relatives à la restauration sur Amazon S3

- S' ACLs ils ont été activés pendant la sauvegarde, le compartiment de destination pour la restauration doit être ACLs activé ; sinon, la tâche de restauration échoue.
- Si le blocage de l'accès public est activé sur le compartiment de destination, le travail de restauration se termine correctement, mais les objets publics ne ACLs sont pas restaurés.

- Les restaurations d'objets sont ignorées si le compartiment de destination contient un objet portant le même nom ou le même ID de version.
- Lorsque vous effectuez une restauration dans le compartiment S3 d'origine,
 - AWS Backup n'effectue pas de restauration destructive, c'est-à-dire qu' AWS Backup il ne place pas un objet dans un bucket à la place d'un objet qui existe déjà, quelle que soit sa version.
 - Dans la version actuelle, un marqueur de suppression est considéré comme un objet inexistant, de sorte qu'une restauration peut avoir lieu.
 - AWS Backup ne supprime pas d'objets (sans marqueurs de suppression) d'un bucket lors d'une restauration (exemple : les clés actuellement présentes dans le bucket qui n'étaient pas présentes lors de la sauvegarde seront conservées).
- Restauration de copies interrégionales
 - Bien que les sauvegardes S3 puissent être copiées d'une région à l'autre, les tâches de restauration ne sont effectuées que dans la même région dans laquelle se trouve la sauvegarde ou la copie d'origine.

Exemple

Exemple : un compartiment S3 créé dans la région USA Est (Virginie du Nord) peut être copié dans la région Canada (Centre). La tâche de restauration peut être lancée à l'aide du compartiment d'origine dans la région USA Est (Virginie du Nord) et restaurée dans cette région, ou la tâche de restauration peut être lancée à l'aide de la copie dans la région du Canada (centre) et restaurée dans cette région.

- La méthode de chiffrement d'origine ne peut pas être utilisée pour restaurer un point de restauration (sauvegarde) copié depuis une autre région. AWS KMS Le chiffrement des copies entre régions n'est pas disponible pour les ressources Amazon S3 ; utilisez plutôt un type de chiffrement différent pour une tâche de restauration.

Restauration ACLs et balises d'objets

Lorsque vous restaurez des données Amazon S3, vous choisissez si ACLs vous participez à la restauration.

S' ACLs ils sont disponibles dans le point de restauration, vous pouvez choisir de les restaurer ou de les exclure à ACLs l'aide du ACLs paramètre Restaurer ; s'ils ne ACLs figurent pas dans la sauvegarde, ils ne peuvent pas être restaurés quel que soit le paramètre. Si vous essayez de créer une tâche de restauration avec ACLs cette option activée mais qu'elle ne faisait pas partie de

la sauvegarde, vous risquez de voir s'afficher un message d'erreur tel que `Unable to restore Access Control Lists (ACLs) for bucket because backup was created with the 'BackupACLs' option disabled. Please proceed with restoring without ACLs.`

Les balises d'objet sont automatiquement restaurées si elles ont été incluses dans la sauvegarde d'origine

Note

Restaurer les points de récupération sans ACLs

Si AWS CLI vous tentez ACLs de restaurer à partir d'une sauvegarde exclue ACLs, l'opération de restauration échouera avec un message d'erreur indiquant des paramètres de restauration non valides.

Restaurer plusieurs versions

Par défaut, AWS Backup restaure uniquement la dernière version de vos objets. Vous avez le choix de restaurer des versions supplémentaires ou toutes les versions des objets.

Reportez-vous à l'étape 6 de la section suivante pour savoir comment restaurer les 10 dernières versions ou toutes les versions à l'aide de la AWS Backup console.

Consultez [???](#) plus loin sur cette page les détails des métadonnées à inclure lors de la restauration par programmation.

Restaurer via la AWS Backup console

Pour restaurer vos données Amazon S3 à l'aide de la AWS Backup console :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et sélectionnez l'ID de ressource Amazon S3 que vous voulez restaurer.
3. Sur la page Détails de la ressource, vous verrez une liste des points de récupération pour l'ID de ressource sélectionné. Pour restaurer une ressource :
 - a. Dans le volet Sauvegarde, choisissez l'ID du point de récupération de la ressource.
 - b. Dans le coin supérieur droit du volet, choisissez Restaurer.

(Vous pouvez également accéder au coffre-fort de sauvegarde, trouver le point de récupération, puis cliquer sur Actions, puis sur Restaurer.)

4. Si vous restaurez une sauvegarde continue, dans le volet Heure de restauration, sélectionnez l'une des options suivantes :
 - a. Acceptez la valeur par défaut pour restaurer la Dernière heure de restauration.
 - b. Spécifiez la date et l'heure de restauration.
5. Dans le volet Paramètres, indiquez si vous souhaitez Restaurer le compartiment entier ou effectuer une Restauration au niveau des éléments.
 - a. Si vous choisissez la restauration au niveau de l'élément, vous restaurez jusqu'à 5 éléments (objets ou dossiers dans un compartiment) par tâche de restauration en spécifiant l'[URI S3](#) de chaque élément qui identifie de manière unique cet objet.

(Pour plus d'informations sur le compartiment S3 URIs, consultez la section [Méthodes d'accès à un compartiment](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.)
 - b. Choisissez Ajouter un élément pour spécifier un autre élément à restaurer.
6. Par défaut, seule la dernière version d'un objet est restaurée. Vous pouvez restaurer jusqu'aux 10 dernières versions ou restaurer toutes les versions des objets. Sélectionnez votre préférence dans le menu déroulant.
7. Choisissez votre Destination de restauration. Vous pouvez Restaurer vers le compartiment source, Utiliser un compartiment existant ou Créer un compartiment.

 Note

La gestion des versions doit être activée dans votre compartiment de destination de restauration. AWS Backup vous avertit si le bucket que vous sélectionnez ne répond pas à cette exigence.

- a. Si vous choisissez Utiliser un compartiment existant, sélectionnez le compartiment S3 de destination dans le menu qui affiche tous les compartiments existants dans votre AWS région actuelle.
- b. Si vous choisissez Créer un compartiment, saisissez le Nouveau nom de compartiment. Une fois le bucket créé, vous pouvez modifier les paramètres par défaut du BPA (Block Public Access) et du contrôle de version S3.

8. Pour le chiffrement des objets de votre compartiment S3, vous pouvez choisir le chiffrement des objets restauré. Utilisez les clés de chiffrement d'origine (par défaut), la Clé Amazon S3 (SSE-S3) ou la CléAWS Key Management Service (SSE-KMS).

Ces paramètres s'appliquent uniquement au chiffrement des objets du compartiment S3. Cela n'affecte pas le chiffrement du compartiment lui-même.

- a. Utiliser les clés de chiffrement d'origine (par défaut) restaure les objets avec les mêmes clés de chiffrement que celles utilisées par l'objet source. Si un objet source n'a pas été chiffré, cette méthode le restaure sans chiffrement.

Cette option de restauration vous permet de choisir éventuellement une clé de chiffrement de remplacement pour chiffrer le ou les objets de restauration si la clé d'origine n'est pas disponible.

- b. Si vous choisissez la Clé Amazon S3 (SSE-S3), vous n'avez pas besoin de spécifier d'autres options.
 - c. Si vous choisissez la AWS Key Management Service clé (SSE-KMS), vous pouvez effectuer les choix suivants : Clé gérée par AWS (aws/s3), Choisissez parmi vos AWS KMS clés ou Entrez l'ARN de la clé. AWS KMS
 - i. Si vous choisissez Clé gérée par AWS (aws/s3), vous n'avez pas besoin de spécifier d'autres options.
 - ii. Si vous choisissez parmi vos AWS KMS clés, sélectionnez une AWS KMS clé dans le menu déroulant. Vous pouvez également choisir Créer une clé.
 - iii. Si vous entrez l'ARN de la AWS KMS clé, saisissez l'ARN dans la zone de texte. Vous pouvez également choisir Créer une clé.
9. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
 10. Choisissez Restore backup. Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Restaurez les points de récupération Amazon S3 via AWS CLI

Utilisez [StartRestoreJob](#). Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon S3 :

```
// Mandatory metadata:
```

```

DestinationBucketName // The destination bucket for your restore.

// Optional metadata:
RestoreACLs // Boolean. If ACLs were part of the backup, include and set to TRUE. If
the backup
does not include ACLs and this parameter is included, set to FALSE.
EncryptionType // The type of encryption to encrypt your restored objects. Options
are original (same encryption as the original object), SSE-S3, or SSE-KMS).
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
required for item-level restore.
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
RestoreLatestVersionsUpTo // Include this optional parameter to multiple versions.
RestoreTime // The restore time (only valid for continuous recovery points where it is
required, in format 2021-11-27T03:30:27Z).

```

`RestoreLatestVersionsUpTo` est une paire clé-valeur de métadonnées facultative. Par défaut, ou si cela est omis, la dernière version est restaurée. Incluez ces métadonnées pour restaurer des versions supplémentaires de vos objets. Les valeurs acceptées sont :

- 1 (pour restaurer la dernière version)
- n , où n est un entier positif supérieur à 1. Les dernières versions de vos objets seront restaurées. Si le nombre de versions réel d'un objet est inférieur à n , ce nombre de versions sera restauré pour cet objet.
- all (pour restaurer toutes les versions)

Statut du point de récupération

Les points de récupération auront un statut indiquant leur état.

EXPIRED Le statut indique que le point de restauration a dépassé sa période de rétention, mais qu'il n'est AWS Backup pas autorisé ou qu'il est incapable de le supprimer pour une autre raison. Pour supprimer manuellement ces points de récupération, voir [Étape 3 : Supprimer les points de récupération](#) dans la section Nettoyage des ressources du guide Mise en route.

Le statut **STOPPED** apparaît lors d'une sauvegarde continue lorsqu'un utilisateur a effectué une action qui entraîne la désactivation de la sauvegarde continue. Cela peut être dû à la suppression des autorisations, à la désactivation de la gestion des versions, à la désactivation des événements envoyés à Amazon EventBridge ou à la désactivation des EventBridge règles mises en place par AWS Backup.

Pour résoudre le statut STOPPED, assurez-vous que toutes les autorisations demandées sont en place et que la gestion des versions est activée sur le compartiment S3. Une fois ces conditions remplies, la prochaine instance d'une règle de sauvegarde exécutée entraînera la création d'un nouveau point de récupération continue. Les points de récupération ayant le statut ARRÊTÉ n'ont pas besoin d'être supprimés.

Messages de restauration S3

Lorsqu'une tâche de restauration se termine ou échoue, le message suivant peut s'afficher. Le tableau suivant peut vous aider à déterminer la cause possible du message d'état.

Scénario	Statut de la tâche	Message	Exemple
Tous les objets n'ont pas pu être restaurés.	FAILED	« Aucun objet n'a été restauré de <i>RecoveryPointARN</i> à <i>bucket</i> . Pour être informé de ces défaillances, activez les notifications d'événements SNS. »	Le rôle utilisé pour démarrer la tâche de restauration n'est pas autorisé à placer des objets dans le compartiment de destination. Le rôle de restauration n'est pas autorisé à vérifier si la version de l'objet existe dans le compartiment de destination.
Un ou plusieurs objets (mais pas tous) n'ont pas pu être restaurés.	TERMINÉ	« Un ou plusieurs objets n'ont pas pu être restaurés de <i>RecoveryPointARN</i> à <i>bucket</i> . Pour être informé de ces défaillances, activez les notifications d'événements SNS. »	Le rôle utilisé pour démarrer la tâche de restauration n'a pas accès à la clé KMS utilisée par un ou plusieurs des objets d'origine.

Scénario	Statut de la tâche	Message	Exemple
Il n'y a aucun objet à restaurer.	TERMINÉ	« Aucun objet ne correspond à la demande de restauration pour <i>RecoveryPointARN</i> . »	Le point de récupération (sauvegarde) du compartiment source à restaurer ne comporte aucun objet. Le préfixe utilisé pour la tâche de restauration ne correspond à aucun objet.

Restaurer un volume Storage Gateway

Si vous restaurez un instantané de AWS Storage Gateway volume, vous pouvez choisir de le restaurer en tant que volume Storage Gateway ou en tant que volume Amazon EBS. Cela est dû au fait qu'il AWS Backup s'intègre aux deux services et que tout instantané de Storage Gateway peut être restauré sur un volume Storage Gateway ou sur un volume Amazon EBS.

Restaurez Storage Gateway via la AWS Backup console

Pour restaurer un volume Storage Gateway

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées, puis l'ID de ressource Storage Gateway que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les paramètres de restauration de votre ressource. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

Pour Type de ressource, choisissez la AWS ressource à créer lors de la restauration de cette sauvegarde.

5. Si vous choisissez Volume Storage Gateway, choisissez une Passerelle accessible. Choisissez également votre Nom de cible iSCSI.

1. Pour les passerelles « Volume stocké », choisissez un ID de disque.
2. Pour les passerelles « Volume mis en cache », choisissez une capacité au moins égale à votre ressource protégée.

Si vous choisissez Volume EBS, indiquez les valeurs Type de volume, Taille (Gio), et choisissez une Zone de disponibilité.

6. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.

 Note

Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.

7. Choisissez Restore backup.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Restaurez Storage Gateway avec AWS CLI

Dans l'interface de ligne de commande, [start-restore-job](#) vous permet de restaurer un volume Storage Gateway.

La liste suivante contient les métadonnées acceptées.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
            operation to return a list of gateways for your account and Région AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Restauration d'une table Amazon Timestream

Lorsque vous restaurez une table Amazon Timestream, plusieurs options doivent être configurées, notamment le nom de la nouvelle table, la base de données de destination, vos préférences d'allocation de stockage (mémoire et stockage magnétique) et le rôle que vous utiliserez pour terminer la tâche de restauration. Vous pouvez également choisir un compartiment Amazon S3 dans lequel stocker les journaux d'erreurs. Les écritures sur stockage magnétique étant asynchrones, vous souhaiterez peut-être journaliser les erreurs.

Le stockage de données Timestream comporte deux niveaux : un stockage en mémoire et un stockage magnétique. Le stockage en mémoire est requis, mais vous avez la possibilité de transférer votre table restaurée vers un stockage magnétique une fois la durée de mémoire spécifiée écoulée. La mémoire est optimisée pour les écritures de données à haut débit et les point-in-time requêtes rapides. Le stockage magnétique est optimisé pour les écritures de données à faible débit et arrivée tardive, le stockage de données à long terme et les requêtes analytiques rapides.

Lorsque vous restaurez une table Timestream, vous déterminez combien de temps vous souhaitez que la table reste dans chaque niveau de stockage. À l'aide de la console ou de l'API, vous pouvez définir la durée de stockage pour les deux. Notez que le stockage est linéaire et séquentiel. Timestream stockera d'abord votre table restaurée dans un stockage en mémoire, puis la transmettra automatiquement en stockage magnétique lorsque le temps de stockage en mémoire sera atteint.

Note

La période de rétention de la mémoire magnétique doit être égale ou supérieure à la période de rétention initiale (indiquée en haut à droite de la console), sinon les données seront perdues.

Exemple : vous définissez l'allocation de stockage en mémoire pour conserver les données pendant une semaine et l'allocation de mémoire magnétique pour conserver les mêmes données pendant un an. Lorsque les données du stockage en mémoire datent d'une semaine, elles sont automatiquement déplacées vers le stockage magnétique. Elles sont ensuite conservées dans le stockage magnétique pendant un an. À la fin de cette période, elles sont supprimées de Timestream et d' AWS Backup.

Pour restaurer une table Amazon Timestream à l'aide de la console AWS Backup

Vous pouvez restaurer les tables Timestream dans la AWS Backup console créée par. AWS Backup

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon Timestream que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les nouveaux paramètres de configuration de votre table, notamment :
 - a. Nom de la nouvelle table, composé de 2 à 256 caractères (lettres, chiffres, tirets, points et traits de soulignement).
 - b. Base de données de destination, choisie dans le menu déroulant.
5. Allocation de stockage : définissez la durée pendant laquelle la table restaurée restera pour la première fois dans le [stockage en mémoire](#) et définissez la durée pendant laquelle la table restaurée restera ensuite dans le [stockage magnétique](#). Le stockage en mémoire peut être défini en heures, jours, semaines ou mois. Le stockage magnétique peut être défini en jours, semaines, mois ou années.
6. (Facultatif) Activer les écritures de stockage magnétique : vous avez la possibilité d'autoriser les écritures sur stockage magnétique. Lorsque cette option est cochée, les données à arrivée tardive, c'est-à-dire les données horodatées en dehors de la période de rétention de la mémoire, seront écrites directement dans le stockage magnétique.
7. (Facultatif) Emplacement des journaux d'erreurs Amazon S3 : vous pouvez spécifier un emplacement S3 dans lequel vos journaux d'erreurs seront stockés. Parcourez vos fichiers S3 ou copiez-collez le chemin du fichier S3.

 Note

Si vous choisissez de spécifier l'emplacement du journal des erreurs S3, le rôle que vous utilisez pour cette restauration doit être autorisé à écrire dans un compartiment S3 ou doit contenir une politique avec cette autorisation.

8. Choisissez le rôle IAM à transmettre pour effectuer des restaurations. Vous pouvez utiliser le rôle IAM par défaut ou en spécifier un autre.
9. Cliquez sur Restaurer la sauvegarde.

Vos tâches de restauration seront visibles sous Ressources protégées. Vous pouvez consulter le statut actuel de votre tâche de restauration en cliquant sur le bouton d'actualisation ou sur CTRL-R.

Pour restaurer une table Amazon Timestream à l'aide d'une API, d'une interface de ligne de commande ou d'un kit SDK

Utilisez [StartRestoreJob](#) pour restaurer une table Timestream via l'API.

Pour restaurer un flux temporel à l'aide de AWS CLI, utilisez l'opération `start-restore-job`. et spécifiez les métadonnées suivantes :

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' | 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' | 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

Voici un exemple de modèle :

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStoreRetentionPeriodInHours=1,EnableMagneticStoreWrites=true,\
"MagneticStoreRejectedDataLocation\":{\\"S3Configuration\":{\\"BucketName\":"bucketname"},"EncryptionOption\":"SSE_S3\"},"'" \
--region us-west-2 \
--endpoint-url url
```

Vous pouvez également utiliser [DescribeRestoreJob](#) pour vous aider à obtenir des informations de restauration.

Dans le AWS CLI, utilisez l'opération `describe-restore-job` et utilisez les métadonnées suivantes :

```
TableName: string;
```

```
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
'years'
EnableMagneticStoreWrites?: boolean;
```

Voici un exemple de modèle :

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Restaurez une machine virtuelle à l'aide de AWS Backup

Vous pouvez restaurer une machine virtuelle sur VMware Cloud on AWS, VMware Cloud on AWS Outposts, un volume Amazon EBS ou [une EC2 instance Amazon](#). VMware La restauration (ou la migration) d'une machine virtuelle EC2 nécessite une licence. Par défaut, AWS inclura une licence (des frais s'appliquent). Pour plus d'informations, consultez la section [Options de licence](#) dans le Guide de l' Import/Export utilisateur de la machine virtuelle.

Vous pouvez restaurer une machine VMware virtuelle à l'aide de la AWS Backup console ou via le AWS CLI. Lorsqu'une machine virtuelle est restaurée, le dossier VMware Tools n'est pas inclus. Consultez VMware la documentation pour réinstaller VMware Tools.

AWS Backup les restaurations de machines virtuelles ne sont pas destructives, ce qui signifie AWS Backup qu'elles ne remplacent pas les machines virtuelles existantes lors d'une restauration. Au lieu de cela, la tâche de restauration déploie une nouvelle machine virtuelle.

Tâches

- [Considérations relatives à la restauration d'une machine virtuelle sur une EC2 instance Amazon](#)
- [Utiliser la AWS Backup console pour restaurer les points de restauration des machines virtuelles](#)
- [AWS CLI À utiliser pour restaurer les points de restauration des machines virtuelles](#)

Considérations relatives à la restauration d'une machine virtuelle sur une EC2 instance Amazon

- La restauration (ou la migration) d'une machine virtuelle EC2 nécessite une licence. Par défaut, un AWS testament inclut une licence (des frais s'appliquent). Pour plus d'informations, consultez la section [Options de licence](#) dans le Guide de l' Import/Export utilisateur de la machine virtuelle.
- Il existe une limite maximale de 5 To (téraoctets) pour chaque disque de machine virtuelle.
- Vous ne pouvez pas spécifier de paire de clés lorsque vous restaurez la machine virtuelle sur une instance. Vous pouvez ajouter une paire de clés `authorized_keys` pendant le lancement (via les données utilisateur de l'instance) ou après le lancement (comme décrit dans [cette section de résolution](#) des problèmes du guide de EC2 l'utilisateur Amazon).
- Vérifiez que votre [système d'exploitation est compatible](#) pour l'importation vers et l'exportation depuis Amazon EC2 dans le guide de l' Import/Export utilisateur de la machine virtuelle.
- Consultez les limites liées à [l'importation VMs vers Amazon EC2](#) dans le guide de l' Import/Export utilisateur de la machine virtuelle.
- Lorsque vous effectuez une restauration sur une EC2 instance Amazon à l'aide de AWS CLI, vous devez spécifier `"RestoreTo": "EC2Instance"`. Tous les autres attributs ont des valeurs par défaut.
- EC2 Offres Amazon [EC2 autorisées AMIs](#). Si ce paramètre est activé dans votre compte, ajoutez l'alias `aws-backup-vault` à votre liste d'autorisation. Dans le cas contraire, les opérations de restauration des points de restauration des machines virtuelles sur les EC2 instances échoueront avec un message d'erreur tel que « AMI source introuvable dans la région ».

Utiliser la AWS Backup console pour restaurer les points de restauration des machines virtuelles

Vous pouvez restaurer une machine virtuelle à partir de plusieurs emplacements dans le volet de navigation gauche de la AWS Backup console :

- Choisissez Hyperviseurs pour afficher les points de récupération des machines virtuelles gérées par un hyperviseur connecté à AWS Backup.
- Choisissez Machines virtuelles pour afficher les points de récupération des machines virtuelles sur tous les hyperviseurs connectés à AWS Backup.
- Choisissez Backup vaults pour afficher les points de restauration stockés dans un AWS Backup coffre-fort spécifique.

- Choisissez Ressources protégées pour afficher les points de restauration de toutes vos ressources AWS Backup protégées.

Si vous devez restaurer une machine virtuelle qui n'est plus connectée à Backup gateway, choisissez Coffres de sauvegarde ou Ressources protégées pour localiser votre point de récupération.

Options

- [Restaurer vers VMware](#)
- [Restaurer sur un volume Amazon EBS](#)
- [Restaurer sur une EC2 instance Amazon](#)

Pour restaurer une machine virtuelle sur VMware Cloud AWS on et VMware Cloud on VMware AWS Outposts

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.
 - a. La Restauration complète restaure tous les disques de la machine virtuelle.
 - b. La Restauration au niveau du disque restaure une sélection définie par l'utilisateur d'un ou de plusieurs disques. Utilisez le menu déroulant pour sélectionner les disques à restaurer.
5. Choisissez l'Emplacement de la restauration. Les options sont VMwareles suivantes : VMware Cloud AWS activé et VMware Cloud activé AWS Outposts.
6. Si vous effectuez une restauration complète, passez à la prochaine étape. Si vous effectuez une restauration au niveau du disque, un menu déroulant s'affichera sous Disques de machine virtuelle. Choisissez un ou plusieurs volumes de démarrage à restaurer.
7. Sélectionnez un hyperviseur dans le menu déroulant pour gérer la machine virtuelle restaurée
8. Pour la machine virtuelle restaurée, utilisez les bonnes pratiques de votre organisation en matière de machine virtuelle pour spécifier :
 - a. Nom

- b. Chemin (tel que /datacenter/vm)
- c. Nom de la ressource de calcul (tel que VMHost ou Cluster)

Si un hôte fait partie d'un cluster, vous ne pouvez pas effectuer de restauration sur l'hôte, mais uniquement sur le cluster donné.

- d. Entrepôt de données
9. Pour Restaurer le rôle, sélectionnez le Rôle par défaut (recommandé) ou Sélectionner un rôle IAM à l'aide du menu déroulant.
 10. Choisissez Restore backup.
 11. Facultatif : vérifiez que votre tâche de restauration a le statut Completed. Dans le menu de navigation de gauche, choisissez Tâches.

Pour restaurer une machine virtuelle sur un volume Amazon EBS

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.
 - La Restauration du disque restaure une sélection définie par l'utilisateur d'un disque. Utilisez le menu déroulant pour sélectionner le disque à restaurer.
5. Choisissez l'Emplacement de restauration comme Amazon EBS.
6. Dans le menu déroulant Disque de machine virtuelle, choisissez le volume de démarrage à restaurer.
7. Sous Type de volume EBS, choisissez le type de volume.
8. Choisissez votre Zone de disponibilité.
9. Chiffrement (facultatif). Cochez cette case si vous choisissez de chiffrer le volume EBS.
10. Sélectionnez votre clé KMS dans le menu.
11. Pour le rôle Restaurer, sélectionnez le rôle par défaut (recommandé) ou Choisissez un rôle IAM.
12. Choisissez Restore backup.

13. Facultatif : vérifiez que votre tâche de restauration a le statut Completed. Dans le menu de navigation de gauche, choisissez Tâches.
14. Facultatif : consultez [Comment utiliser LVM pour créer un volume logique sur la partition d'un volume Amazon EBS](#) ? pour en savoir plus sur la façon de monter des volumes gérés et d'accéder aux données sur le volume Amazon EBS restauré.

Pour restaurer une machine virtuelle sur une EC2 instance Amazon

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.
 - La Restauration complète restaure complètement le système de fichiers, y compris le dossier et les fichiers au niveau racine.
5. Choisissez l'emplacement de restauration comme Amazon EC2.
6. Pour Type d'instance, choisissez la combinaison de calcul et de mémoire requise pour exécuter votre application sur votre nouvelle instance.

 Tip

Choisissez un type d'instance qui correspond ou dépasse les spécifications de la machine virtuelle d'origine. Pour plus d'informations, consultez le [guide des types d' EC2 instances Amazon](#).

7. Pour Virtual Private Cloud (VPC), choisissez un cloud privé virtuel (VPC) qui définit l'environnement réseau de l'instance.
8. Pour Sous-réseau, choisissez l'un des sous-réseaux du VPC. Votre instance reçoit une adresse IP privée depuis la plage d'adresses de sous-réseau.
9. Pour les groupes de sécurité, choisissez un groupe de sécurité qui agit comme un pare-feu pour le trafic vers votre instance.
10. Pour le rôle Restaurer, sélectionnez le rôle par défaut (recommandé) ou Choisissez un rôle IAM.

11. Facultatif : pour exécuter un script sur votre instance au lancement, développez les paramètres avancés et entrez le script dans Données utilisateur.
12. Choisissez Restore backup.
13. Facultatif : vérifiez que votre tâche de restauration a le statut Completed. Dans le menu de navigation de gauche, choisissez Tâches.

AWS CLI À utiliser pour restaurer les points de restauration des machines virtuelles

Utilisez [StartRestoreJob](#).

Vous pouvez spécifier les métadonnées suivantes pour une restauration de machine virtuelle sur Amazon EC2 et Amazon EBS :

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
NetworkInterfaces
```

Vous pouvez spécifier les métadonnées suivantes pour la restauration d'une machine virtuelle vers VMware, VMware Cloud on AWS et VMware Cloud on AWS Outpost :

```
RestoreTo
```

```
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

Cet exemple montre comment effectuer une restauration complète pour VMware :

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":[{"DiskId":"2000","Label":"Hard disk 1"}],"vmId":"vm-101"}'
```

Tests de restauration

Les tests de restauration, une fonctionnalité proposée par AWS Backup, fournissent une évaluation automatique et périodique de la viabilité de la restauration, ainsi que la possibilité de surveiller la durée des tâches de restauration.

Table des matières

- [Aperçu](#)
- [Comparaison des tests de la restauration avec le processus de restauration](#)
- [Gestion des tests de la restauration](#)
- [Création d'un plan de test de la restauration](#)
- [Mise à jour d'un plan de test de la restauration](#)
- [Affichage des plans de test de la restauration existants](#)
- [Affichage des tâches de test de la restauration](#)
- [Suppression d'un plan de test de la restauration](#)
- [Tests de restauration Audit](#)
- [Restauration de quotas et de paramètres de test](#)
- [Résolution des problèmes liés aux tests de restauration](#)
- [Métadonnées déduites de tests de la restauration](#)
- [Restaurer la validation des tests](#)

Aperçu

Tout d'abord, vous créez un plan de test de la restauration dans lequel vous indiquez le nom de votre plan, la fréquence de vos tests de la restauration et l'heure de début cible. Ensuite, vous attribuez les ressources à inclure dans votre plan. Vous choisissez ensuite d'inclure des points de récupération spécifiques ou aléatoires dans votre test. AWS Backup backup [déduit intelligemment les métadonnées](#) qui seront nécessaires à la réussite de votre tâche de restauration.

Lorsque l'heure prévue dans votre plan arrive, AWS Backup démarre les tâches de restauration en fonction de votre plan et surveille le temps nécessaire pour terminer la restauration.

Une fois le plan de test de la restauration terminé, vous pouvez utiliser les résultats pour démontrer la conformité aux exigences organisationnelles ou de gouvernance, telles que la réussite des scénarios de test de la restauration ou le délai d'exécution des tâches de restauration.

Vous pouvez éventuellement l'utiliser [Restaurer la validation des tests](#) pour confirmer les résultats du test de restauration.

Une fois que la validation facultative est terminée ou que la AWS Backup fenêtre de validation se ferme, les ressources impliquées dans le test de restauration sont supprimées conformément au service SLAs.

À la fin du processus de test, vous pouvez afficher les résultats et le délai d'exécution des tests.

Comparaison des tests de la restauration avec le processus de restauration

Le test de la restauration exécute les tâches de restauration de la même manière que les restaurations à la demande et utilise les mêmes points de récupération (sauvegardes) qu'une restauration à la demande. Vous verrez des appels d'`StartRestoreJob` entrée CloudTrail (si vous avez activé cette option) pour chaque tâche démarrée par des tests de restauration

Il existe toutefois quelques différences entre le fonctionnement d'un test de la restauration planifié et celui d'une opération de restauration à la demande :

	Tests de restauration	Restaurer
Compte	La bonne pratique recommandée consiste à désigner un compte à utiliser pour les tests de la restauration	Vous pouvez restaurer des ressources à partir d'un compte

	Tests de restauration	Restaurer
AWS Backup Audit Manager	Peut activer une commande pour confirmer si un test de la restauration répond aux objectifs de restauration spécifiés	
Cadence	Périodiquement dans le cadre d'un plan planifié.	À la demande
Ressources	Les types de ressources que vous pouvez attribuer à votre plan de test incluent : Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon, Amazon EFS, EC2 Amazon (Lustre, ONTAP, FSx OpenZFS, Windows), Amazon Neptune, Amazon RDS et Amazon S3.	Toutes les ressources peuvent être restaurées.
Résultats	Une fois le test de restauration terminé, la ressource restaurée est supprimée à la fin de la Restaurer la validation des tests fenêtre.	Une fois la tâche de restauration terminée, la version restaurée de la ressource est conservée.
Balises	Pour les types de ressources qui prennent en charge les balises lors de la restauration, les tests appliquent des balises lors de la restauration.	Les balises sont facultatives pour les ressources prises en charge.

Gestion des tests de la restauration

Vous pouvez créer, afficher, mettre à jour ou supprimer un plan de test de la restauration dans la [console AWS Backup](#).

Vous pouvez utiliser [AWS CLI](#) pour exécuter par programmation des opérations pour les plans de test de la restauration. Chaque CLI est spécifique au AWS service dont elle provient. Les commandes doivent être précédées de `aws backup`.

Suppression de données

Lorsqu'un test de restauration est terminé, AWS Backup commence à supprimer les ressources impliquées dans le test. Cette suppression n'est pas instantanée. Chaque ressource possède une configuration sous-jacente qui détermine la manière dont ces ressources sont stockées et leur cycle de vie. Par exemple, si les compartiments Amazon S3 font partie du test de la restauration, des [règles de cycle de vie sont ajoutées au compartiment](#). L'exécution des règles et la suppression complète du compartiment et de ses objets peuvent prendre plusieurs jours, mais ces ressources ne seront facturées que jusqu'au jour où la règle de cycle de vie est lancée (par défaut, il s'agit d'un jour). La vitesse de suppression dépend du type de ressource.

Les ressources faisant partie d'un plan de test de la restauration contiennent une balise appelée `awsbackup-restore-test`. Si un utilisateur supprime cette balise, il AWS Backup ne peut pas supprimer la ressource à la fin de la période de test. L'utilisateur devra plutôt la supprimer manuellement.

Pour savoir pourquoi les ressources n'ont peut-être pas été supprimées comme prévu, vous pouvez rechercher les tâches ayant échoué dans la console ou utiliser l'interface de ligne de commande pour appeler la demande d'API `DescribeRestoreJob` afin de récupérer les messages du statut de suppression.

Les plans de sauvegarde (autres que les plans de test de restauration) ignorent les ressources créées par les tests de restauration (celles dont la balise `awsbackup-restore-test` ou le nom commence par `awsbackup-restore-test`).

Contrôle des coûts

Les tests de la restauration ont un coût par test de la restauration. Selon les ressources incluses dans votre plan de test de la restauration, les tâches de restauration incluses dans le plan peuvent également avoir un coût. Consultez [Tarification AWS Backup](#) pour plus d'informations.

Lorsque vous configurez un plan de test de la restauration pour la première fois, il peut être avantageux d'inclure un nombre minimum de types de ressources et de ressources protégées afin de vous familiariser avec la fonctionnalité, le processus et les coûts moyens impliqués. Vous pouvez mettre à jour un plan après sa création pour ajouter d'autres types de ressources et des ressources protégées.

Création d'un plan de test de la restauration

Un plan de test de la restauration comporte deux parties : la création du plan et l'attribution des ressources.

Lorsque vous utilisez la console, ces parties sont séquentielles. Dans la première partie, vous définissez le nom, la fréquence et les heures de début. Au cours de la deuxième partie, vous affectez des ressources à votre plan de test.

Lorsque vous utilisez AWS CLI une API, utilisez d'abord [create-restore-testing-plan](#). Une fois que vous avez reçu une réponse positive et que le plan a été créé [create-restore-testing-selection](#), utilisez-le pour chaque type de ressource à inclure dans votre plan.

Lorsque vous créez un plan de test de restauration, nous vous créons un rôle lié au service. Pour de plus amples informations, veuillez consulter [Utilisation des rôles pour les tests de la restauration](#).

Console

Partie I : Création d'un plan de test de la restauration à l'aide de la console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le menu de navigation de gauche, recherchez Tests de restauration et sélectionnez-le.
3. Choisissez Créer un plan de test de la restauration.
4. Général
 - a. Nom : tapez le nom de votre nouveau plan de test de la restauration. Le nom ne peut pas être modifié après la création. Le nom doit contenir uniquement des caractères alphanumériques et des traits de soulignement.
 - b. Fréquence des tests : choisissez la fréquence à laquelle les tests de la restauration seront exécutés.
 - c. Heure de début : définissez l'heure (en heures et minutes) à laquelle vous préférez que le test commence. Vous pouvez également définir le fuseau horaire local dans lequel vous souhaitez que le plan de test de la restauration fonctionne.

- d. Commencer dans les délais : cette valeur (en heures) correspond à la période pendant laquelle le test de restauration est censé commencer. AWS Backup fait de son mieux pour démarrer toutes les tâches de restauration désignées au cours du délai imparti et répartit les heures de début de manière aléatoire au cours de cette période.
5. Sélection des points de récupération : vous définissez ici les coffres-forts sources, la plage de points de récupération et les critères de sélection pour les points de récupération (sauvegardes) que vous souhaitez inclure dans le plan.
- a. Coffres-forts sources : choisissez d'inclure tous les coffres-forts disponibles ou uniquement des coffres-forts spécifiques pour vous aider à filtrer les points de récupération pouvant figurer dans votre plan. Si vous choisissez des coffres-forts spécifiques, dans le menu déroulant, sélectionnez les coffres-forts que vous souhaitez inclure.
 - b. Points de récupération éligibles : spécifiez la période à partir de laquelle les points de récupération seront sélectionnés. Vous pouvez sélectionner 1 à 365 jours, 1 à 52 semaines, 1 à 12 mois ou 1 an.
 - c. Critères de sélection : une fois que votre plage de dates de points de récupération est spécifiée, vous pouvez choisir d'inclure le dernier point ou un point au hasard dans votre plan. Vous pouvez choisir un point aléatoire pour évaluer l'état général des points de récupération à une fréquence plus régulière au cas où une restauration vers une ancienne version serait justifiée.
 - d. Point-in-time points de restauration : si votre plan inclut des ressources [dotées de points de sauvegarde continue \(point-in-time-restore/PITR\)](#), vous pouvez cocher cette case pour que votre plan de test inclue les sauvegardes continues en tant que points de restauration éligibles (voir [Disponibilité des fonctionnalités par ressource](#) pour lesquels les types de ressources disposent de cette fonctionnalité).
6. (facultatif) Balises ajoutées pour restaurer le plan de test : vous pouvez choisir d'ajouter jusqu'à 50 balises à votre plan de test de la restauration. Chaque balise doit être ajoutée séparément. Pour ajouter une nouvelle balise, sélectionnez Ajouter une nouvelle balise.

Partie II : Attribution de ressources au plan à l'aide de la console

Dans cette section, vous choisissez les ressources que vous avez sauvegardées à inclure dans votre plan de test de la restauration. Vous choisirez le nom de l'attribution de ressource, le rôle que vous utiliserez pour le test de la restauration et définirez la période de conservation

avant le nettoyage. Ensuite, vous allez sélectionner le type de ressource ainsi que l'étendue, et éventuellement affiner votre sélection à l'aide de balises.

 Tip

Pour revenir au plan de test de la restauration auquel vous souhaitez ajouter des ressources, vous pouvez accéder à la [console AWS Backup](#), sélectionner Tests de restauration, puis rechercher le plan de test de votre choix et le sélectionner.

1. Général

- a. Nom d'attribution de la ressource : entrez un nom pour cette attribution de ressource à l'aide d'une chaîne de caractères alphanumériques et de traits de soulignement, sans espaces blancs.
- b. Restaurer le rôle IAM : le test doit utiliser un rôle Identity and Access Management (IAM) que vous désignez. Vous pouvez choisir le rôle AWS Backup par défaut ou un rôle différent. Si la AWS Backup valeur par défaut n'existe pas encore à la fin de ce processus, elle AWS Backup sera créée automatiquement pour vous avec les autorisations nécessaires. Le rôle IAM que vous choisissiez pour les tests de la restauration doit contenir les autorisations trouvées dans [AWSBackupServiceRolePolicyForRestores](#).
- c. Période de conservation avant le nettoyage : lors d'un test de la restauration, les données de sauvegarde sont temporairement restaurées. Par défaut, ces données sont supprimées une fois le test terminé. Vous avez la possibilité de retarder la suppression de ces données si vous souhaitez exécuter la validation lors de la restauration.

Si vous prévoyez d'exécuter la validation, sélectionnez Conserver pendant un certain nombre d'heures et entrez une valeur comprise entre 1 et 168 heures incluses. Notez que la validation peut être exécutée par programmation, mais pas depuis la console AWS Backup .

2. Ressources protégées :

- a. Sélectionner un type de ressource : sélectionnez les types de ressources et l'étendue des sauvegardes de ces types à inclure dans le plan de test des ressources. Chaque plan peut contenir plusieurs types de ressources, mais chaque type de ressource doit être attribué au plan individuellement.

- b. Portée de la sélection des ressources : une fois le type choisi, indiquez si vous souhaitez inclure toutes les ressources protégées disponibles de ce type ou si vous souhaitez inclure uniquement des ressources protégées spécifiques.
- c. (facultatif) Affiner la sélection des ressources à l'aide de balises : si vos sauvegardes comportent des balises, vous pouvez filtrer par balises pour sélectionner des ressources protégées spécifiques. Entrez la clé de la balise, la condition pour que cette clé soit incluse ou non, et la valeur de la clé. Sélectionnez ensuite le bouton Ajouter des balises.

Les balises des ressources protégées sont évaluées en vérifiant les balises du dernier point de récupération dans le coffre-fort de sauvegarde contenant la ressource protégée.

3. Paramètres de restauration : certaines ressources nécessitent de spécifier des paramètres pour préparer une tâche de restauration. Dans la plupart des cas, AWS Backup déduira les valeurs en fonction de la sauvegarde stockée.

Il est recommandé dans la plupart des cas de conserver ces paramètres ; toutefois, vous pouvez modifier les valeurs en choisissant une autre sélection dans le menu déroulant. Parmi les exemples où la modification des valeurs peut être optimale, citons le remplacement des clés de chiffrement, les FSx paramètres Amazon où les données ne peuvent pas être déduites et la création de sous-réseaux.

Par exemple, si une base de données RDS est l'un des types de ressources que vous attribuez à votre plan de test de la restauration, des paramètres tels que la zone de disponibilité, le nom de la base de données, la classe d'instance de base de données et le groupe de sécurité VPC apparaîtront avec des valeurs déduites que vous pouvez modifier le cas échéant.

AWS CLI

La commande de l'interface de ligne de commande `CreateRestoreTestingPlan` est utilisée pour établir un plan de test de la restauration.

Le plan de test doit contenir :

- `RestoreTestingPlan`, qui doit contenir un `RestoreTestingPlanName` unique
- Expression cron [ScheduleExpression](#)
- [RecoveryPointSelection](#)

Bien que nommé de la même manière, ce n'est PAS le même que `RestoreTestingSelection`.

[RecoveryPointSelection](#) possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer `Algorithm` si vous voulez le dernier point de récupération dans votre répertoire `SelectionWindowDays` ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans `IncludeVaults` quels coffres-forts les points de récupération peuvent être choisis.

Une sélection peut comporter une ou plusieurs ressources protégées ARNs ou une ou plusieurs conditions, mais elle ne peut pas avoir les deux.

Vous pouvez également inclure :

- [ScheduleExpressionTimezone](#)
- [Tags](#)
- [CreatorRequestId](#)
- [StartWindowHours](#)

Utilisez la commande de l'interface de ligne de commande [create-restore-testing-plan](#).

Une fois le plan créé, vous devez lui attribuer des ressources à l'aide de [create-restore-testing-selection](#).

Cela comprend `RestoreTestingSelectionName`, `ProtectedResourceType` et l'un des éléments suivants :

 Note

`RestoreTestingSelectionName` exigences en matière de dénomination :

- Doit comporter de 1 à 256 caractères
- Peut contenir des lettres (a-z, A-Z), des chiffres (0-9), des traits d'union (-) et des traits de soulignement (_)
- Doit commencer par une lettre ou un chiffre

- Ne peut pas se terminer par un trait d'union ou un trait de soulignement
- Doit être unique dans le plan de test de restauration

- ProtectedResourceArns
- ProtectedResourceConditions

Chaque type de ressource protégée peut avoir une seule valeur. Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour ProtectedResourceArns avec ProtectedResourceConditions. Vous pouvez également inclure jusqu'à 30 ressources protégées spécifiques ARNs dans ProtectedResourceArns.

Détermination du point de récupération

Chaque fois qu'un plan de test est exécuté (selon la fréquence et l'heure de début que vous avez spécifiées), un point de récupération éligible par ressource protégée sélectionnée est restauré par le test de restauration. Si aucun point de récupération pour une ressource ne répond aux critères de sélection des points de récupération, cette ressource ne sera pas incluse dans le test.

Un point de récupération pour une ressource protégée dans une sélection de test est éligible s'il répond aux critères de la période spécifiée et s'il inclut des coffres-forts dans le plan de test de restauration.

Une ressource protégée est sélectionnée si la sélection du test inclut le type de ressource et si l'une des conditions suivantes est vraie :

- L'ARN de la ressource est spécifié dans cette sélection ; ou
- Les conditions des balises associées à cette sélection correspondent aux balises du dernier point de récupération de la ressource.

Mise à jour d'un plan de test de la restauration

Vous pouvez mettre à jour certaines parties de votre plan de test de la restauration et les sélections de ressources qu'il contient via la console ou AWS CLI.

Console

Mise à jour des plans de test de la restauration et des sélections dans la console

Lorsque vous consultez la page des détails du plan de test de la restauration dans la console, vous pouvez modifier (mettre à jour) de nombreux paramètres de votre plan. Pour ce faire,

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le menu de navigation de gauche, recherchez Tests de restauration et sélectionnez-le.
3. Sélectionnez le bouton Modifier.
4. Réglez la fréquence, l'heure de début et l'heure à laquelle le test débutera après l'heure de début choisie.
5. Enregistrez vos modifications.

AWS CLI

Mettez à jour les plans de test et les sélections de restauration via AWS CLI

Demande [UpdateRestoreTestingPlan](#) et [UpdateRestoreTestingSelection](#) peut être utilisé pour envoyer des mises à jour partielles d'un plan ou d'une sélection spécifique. Les noms ne peuvent pas être modifiés, mais vous pouvez mettre à jour d'autres paramètres. N'incluez que les paramètres que vous souhaitez modifier dans chaque demande.

Avant d'envoyer une demande de mise à jour, utilisez [GetRestoreTestingPlan](#) et [GetRestoreTestingSelection](#) pour déterminer si votre RestoreTestingSelection contenu est spécifique ARNs ou s'il utilise le caractère générique et les conditions.

Si votre sélection de test de restauration a spécifié ARNs (au lieu d'un caractère générique) et que vous souhaitez le remplacer par un caractère générique assorti de conditions, la demande de mise à jour doit inclure à la fois le caractère générique ARN et les conditions. Une sélection peut avoir une ressource protégée ARNs ou utiliser le caractère générique assorti de conditions, mais elle ne peut pas avoir les deux.

- [get-restore-testing-plan](#)
- [get-restore-testing-selection](#)
- [update-restore-testing-plan](#)
- [update-restore-testing-selection](#)

Affichage des plans de test de la restauration existants

Console

Affichage des détails d'un plan de test de la restauration existant et des ressources attribuées dans la console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Sélectionnez Tests de restauration dans le menu de navigation de gauche. L'écran affiche vos plans de test de la restauration. Les plans sont affichés par défaut dans l'ordre de dernière exécution.
3. Sélectionnez le lien dans un plan pour voir ses détails, y compris un résumé du plan, son nom, sa fréquence, son heure de début et le début au sein de la valeur.

Vous pouvez également consulter les ressources protégées dans le cadre de ce plan, les tâches de test de la restauration des 30 derniers jours incluses dans ce plan et toutes les balises que vous pouvez créer dans le cadre de ce plan de test.

AWS CLI

Obtention d'informations sur un plan de test de la restauration existant et sur une sélection de tests à l'aide de la ligne de commande

- [list-restore-testing-plan](#)
- [list-restore-testing-selections](#)
- [get-restore-testing-plan](#)
- [get-restore-testing-selection](#)

Affichage des tâches de test de la restauration

Console

Affichage des tâches de test de la restauration existantes dans la console

Les tâches de test de la restauration sont incluses sur la page des tâches de restauration.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.

2. Accédez à la page Tâches.

Vous pouvez également sélectionner Tests de restauration, puis sélectionner un plan de test de la restauration pour voir ses détails et les tâches associées au plan.

3. Sélectionnez l'onglet Tâches de restauration.

Sur cette page, vous pouvez consulter le statut, l'heure de restauration, le type de restauration, l'ID de ressource, le type de ressource, le plan de test de la restauration auquel appartient la tâche, l'heure de création et l'ID du point de récupération de la tâche de restauration.

Les tâches incluses dans un plan de test de la restauration ont le type de restauration Test.

Les tâches de test de la restauration comportent plusieurs catégories de statut :

- Un type de statut nécessitant une attention particulière est souligné ; passez le curseur sur le statut pour voir des informations supplémentaires si elles sont disponibles.
- Un statut de validation s'affichera s'il [Restaurer la validation des tests](#) a été lancé lors du test (non disponible dans la console).
- Le statut de suppression indique le statut des données générées par le test de la restauration. Trois statuts de suppression sont possibles : Réussi, Suppression et Échec.

Si la suppression d'une tâche de test de la restauration a échoué, vous devrez supprimer la ressource manuellement car le flux de test de la restauration n'a pas pu la terminer automatiquement. Souvent, une suppression échouée est déclenchée si la balise `awsbackup-restore-test` est supprimée de la ressource.

AWS CLI

Affichage des tâches de test de la restauration existantes depuis la ligne de commande

- [list-restore-jobs-by-protected-resource](#)

Suppression d'un plan de test de la restauration

Console

Suppression d'un plan de test de la restauration dans la console

1. Accédez à [Affichage des plans de test de la restauration existants](#) pour voir vos plans de test de la restauration actuels.
2. Sur la page des détails du plan de test de la restauration, supprimez un plan en sélectionnant Supprimer.
3. Une fois que vous avez sélectionné Supprimer, un écran de confirmation contextuel apparaît pour confirmer que vous souhaitez supprimer votre plan. Sur cet écran, le nom de votre plan de test de la restauration spécifique sera affiché en gras. Pour continuer, saisissez le nom exact du plan de test en distinguant majuscules et minuscules, y compris les soulignements, les tirets et les points.

Si l'option Supprimer le plan de test de la restauration ne peut pas être sélectionnée, entrez à nouveau le nom jusqu'à ce qu'il corresponde au nom affiché. Une fois la correspondance exacte établie, l'option permettant de supprimer le plan de test de la restauration pourra être sélectionnée.

AWS CLI

Suppression d'un plan de test de la restauration via la ligne de commande

La commande CLI [DeleteRestoreTestingSelection](#) peut être utilisée pour supprimer une sélection de test de restauration. Incluez `RestoreTestingPlanName` et `RestoreTestingSelectionName` dans la demande.

Toutes les sélections de tests associées à un plan de test doivent être supprimées avant de supprimer le plan de test. Une fois que toutes les sélections de test ont été supprimées, vous pouvez utiliser la demande [DeleteRestoreTestingPlan](#) d'API pour supprimer un plan de test de restauration. Vous devez inclure `RestoreTestingPlanName`.

- [delete-restore-testing-selection](#)
- [delete-restore-testing-plan](#)

Tests de restauration Audit

Restaurez les intégrations de test avec AWS Backup Audit Manager pour vous aider à évaluer si une ressource restaurée a été terminée dans le délai de restauration cible.

Pour plus d'informations, consultez la contrainte [Temps de restauration des ressources pour atteindre l'objectif](#) dans [Contrôles et mesures correctives d'AWS Backup Audit Manager](#).

Restauration de quotas et de paramètres de test

- 100 plans de test de la restauration
- 50 balises peuvent être ajoutées à chaque plan de test de la restauration
- 30 sélections par plan
- 30 ressources protégées ARNs par sélection
- 30 conditions de ressources protégées par sélection (y compris celles comprises dans `StringEquals` et `StringNotEquals`)
- 30 sélecteurs de coffre-fort par sélection
- Nombre maximum de jours pour la fenêtre de sélection : 365 jours
- Heures de la fenêtre de début : min : 1 heure ; max. : 168 heures (7 jours)
- Longueur maximale du nom du plan : 50 caractères
- Longueur maximale du nom de la sélection : 50 caractères

Des informations supplémentaires concernant les limites peuvent être consultées ici : [AWS Backup quotas](#).

Résolution des problèmes liés aux tests de restauration

Si vous avez des tâches de test de restauration dont l'état de restauration est égal à `Failed`, les raisons suivantes peuvent vous aider à en déterminer la cause et à y remédier.

Les messages d'erreur [peuvent être visualisés](#) dans la AWS Backup console sur la page de détails de l'état de la tâche ou à l'aide des commandes de la CLI `list-restore-jobs-by-protected-resource` ou `list-restore-jobs`.

1. Erreur : *No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.*

Solution 1 : mettez à jour votre sélection de test de restauration et [remplacez](#) le paramètre `SubnetId`. La AWS Backup console affiche ce paramètre sous la forme « Sous-réseau ».

Solution 2 : recréer le [VPC par défaut](#).

Types de ressources concernés : Amazon EC2

2. Erreur : *No subnets found for the default VPC [vpc]. Please specify a subnet.*

Solution 1 : mettez à jour votre sélection de test de restauration et [remplacez](#) le paramètre de `SubnetId` restauration. La AWS Backup console affiche ce paramètre sous la forme « Sous-réseau ».

Solution 2 : [créer un sous-réseau par défaut](#) dans le VPC par défaut.

Types de ressources concernés : Amazon EC2

3. Erreur : *No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

Solution 1 : mettez à jour votre sélection de test de restauration et [remplacez](#) le paramètre de `DBSubnetGroupName` restauration. La AWS Backup console affiche ce paramètre en tant que groupe de sous-réseaux.

Solution 2 : [créer un sous-réseau par défaut](#) dans le VPC par défaut.

Types de ressources concernés : Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Erreur : *IAM Role cannot be assumed by AWS Backup.*

Solution : Le rôle de restauration doit être assumé par AWS Backup. Mettez à jour la politique de confiance du rôle dans IAM pour permettre à celui-ci d'être assumé par "backup.amazonaws.com" ou mettez à jour votre sélection de tests de restauration pour utiliser un rôle assumé par AWS Backup

Types de ressources concernés : tous

5. Erreur : *Access denied to KMS key. ou The specified AWS KMS key ARN does not exist, is not enabled or you do not have permissions to access it.*

Solution : Vérifiez les points suivants :

- Le rôle de restauration a accès à la AWS KMS clé utilisée pour chiffrer vos sauvegardes et, le cas échéant, à la clé KMS utilisée pour chiffrer la ressource restaurée.
- Les politiques de ressources relatives aux clés KMS ci-dessus autorisent le rôle de restauration à y accéder.

Si les conditions ci-dessus ne sont pas encore remplies, configurez le rôle de restauration et les politiques de ressources pour un accès approprié. Ensuite, exécutez à nouveau le test de restauration.

Types de ressources concernés : tous

6. Erreurs : *User **ARN** is not authorized to perform **action** on **resource** because no identity based policy allows the **action**.* ou *Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx.*

Solution : le rôle de restauration ne dispose pas des autorisations adéquates. Mettez à jour les autorisations dans IAM pour le rôle de restauration.

Types de ressources concernés : tous

7. Erreurs : *User **ARN** is not authorized to perform **action** on **resource** because no resource-based policy allows the **action**.* ou *User **ARN** is not authorized to perform **action** on **resource** with an explicit deny in a resource based policy.*

Solution : Le rôle de restauration ne dispose pas d'un accès adéquat à la ressource spécifiée dans le message. Mettez à jour la politique de ressources relative à la ressource mentionnée.

Types de ressources concernés : tous

Métadonnées déduites de tests de la restauration

La restauration d'un point de récupération nécessite de restaurer les métadonnées. Pour effectuer des tests de la restauration, AWS Backup déduit automatiquement les métadonnées susceptibles

d'aboutir à une restauration réussie. La commande `get-restore-testing-inferred-metadata` peut être utilisée pour prévisualiser ce qui AWS Backup sera déduit. La commande `get-restore-job-metadata` renvoie l'ensemble de métadonnées déduit par AWS Backup. Notez que pour certains types de ressources (Amazon FSx), AWS Backup il n'est pas possible de déduire un ensemble complet de métadonnées.

Les métadonnées de restauration déduites sont déterminées au cours du processus de test de la restauration. Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Certaines remplacements de métadonnées ne sont pas disponibles dans la AWS Backup console.

Chaque ressource prise en charge possède à la fois des clés et des valeurs de métadonnées de restauration déduites et des clés de métadonnées de restauration remplaçables. Seules les paires `RestoreMetadataOverrides` clé-valeur ou les paires clé-valeur imbriquées marquées d'un signe *required for successful restore* sont nécessaires à inclure ; les autres sont facultatives. Notez que les valeurs de clé ne sont pas sensibles à la casse.

Important

AWS Backup peut en déduire qu'une ressource doit être restaurée avec ses paramètres par défaut, comme une EC2 instance Amazon ou un cluster Amazon RDS restauré sur le VPC par défaut. Toutefois, si la valeur par défaut n'est pas présente, par exemple si le VPC ou le sous-réseau par défaut a été supprimé et qu'aucune modification des métadonnées n'a été saisie, la restauration échouera.

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
DynamoDB	<code>deletionProtection</code> , où la valeur est définie sur <code>false</code> <code>encryptionType</code> a la valeur <code>Default</code> <code>targetTableName</code> , où la valeur est définie sur une valeur aléatoire commençant	<code>encryptionType</code> <code>kmsMasterKeyArn</code>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
	par awsbackup-restore-test-	
Amazon EBS	availabilityZone , dont la valeur est définie sur une zone de disponibilité aléatoire encrypted , dont la valeur est définie sur true	availabilityZone iops kmsKeyId throughput volumesize volumetype
Amazon EC2	La valeur disableApiTermination est définie sur false La valeur instanceType est définie sur le type d'instance du point de récupération en cours de restauration La valeur requiredImdsV2 est définie sur true	iamInstanceProfileName (nul ou UseBackedUpValue) instanceType requireImdsV2 securityGroupIds subnetId

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon EFS	La valeur <code>encrypted</code> est définie sur <code>true</code> La valeur <code>file-system-id</code> est définie sur l'ID du système de fichier du point de récupération en cours de restauration <code>kmsKeyId</code> a la valeur <code>alias/aws/elasticfilesystem</code> La valeur <code>newFileSystem</code> est définie sur <code>true</code> La valeur <code>performanceMode</code> est définie sur <code>generalPurpose</code>	<code>kmsKeyId</code> <code>performanceMode</code>
Amazon FSx pour Lustre	<code>lustreConfiguration</code> possède des clés imbriquées. Une clé imbriquée est <code>automaticBackupRetentionDays</code>, dont la valeur est définie sur <code>0</code>	<code>kmsKeyId</code> <code>lustreConfiguration</code> possède une clé imbriquée <code>logConfiguration</code> <code>securityGroupIds</code> <code>subnetIds</code>, <i>required for successful restore</i>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon FSx pour NetApp ONTAP	name est défini sur une valeur aléatoire commençant par <code>awsbackup_restore_test_</code> ontapConfiguration possède des clés imbriquées, notamment : • <code>junctionPath</code> où <code>/name</code> est le nom du volume en cours de restauration • <code>sizeInMegabytes</code> , dont la valeur est définie sur la taille en mégaoctets du point de récupération en cours de restauration • <code>snapshotPolicy</code> , où la valeur est définie sur <code>none</code>	ontapConfiguration possède des clés imbriquées spécifiques remplaçables, notamment : • <code>junctionPath</code> • <code>ontapVolumeType</code> • <code>securityStyle</code> • <code>sizeInMegabytes</code> • <code>storageEfficiencyEnabled</code> • <code>storageVirtualMachineId</code> , <i>required for successful restore</i> • <code>tieringPolicy</code>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon FSx pour OpenZFS	<code>openZfsConfiguration</code> , qui possède des clés imbriquées, notamment : • <code>automaticBackupRetentionDays</code> avec une valeur définie sur 0 • <code>deploymentType</code> avec une valeur définie sur le type de déploiement du point de récupération en cours de restauration • <code>throughputCapacity</code> , dont la valeur est basée sur le <code>deploymentType</code> . Si le <code>deploymentType</code> est <code>SINGLE_AZ_1</code> , la valeur est définie sur 64 ; si le <code>deploymentType</code> est <code>SINGLE_AZ_2</code> or <code>MULTI_AZ_1</code> , la valeur est définie sur 160	<code>kmsKeyId</code> <code>openZfsConfiguration</code> possède des clés imbriquées spécifiques remplaçables, notamment : • <code>deploymentType</code> • <code>throughputCapacity</code> • <code>diskIopsConfiguration</code> <code>securityGroupIds</code> <code>subnetIds</code>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Serveur FSx de fichiers Amazon pour Windows	windowsConfiguration , qui possède des clés imbriquées, notamment : • automaticBackupRetentionDays avec une valeur définie sur 0 • deploymentType avec une valeur définie sur le type de déploiement du point de récupération en cours de restauration • throughputCapacity avec une valeur définie sur 8	kmsKeyId securityGroupIds subnetIds <i>required for successful restore</i> windowsConfiguration , avec des clés imbriquées spécifiques remplaçables • throughputCapacity • activeDirectoryId <i>required for successful restore</i> • preferredSubnetId

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon RDS, Aurora, Amazon DocumentDB, clusters Amazon Neptune	<code>availabilityZones</code> avec une valeur définie sur une liste de trois zones de disponibilité aléatoires au maximum <code>dbClusterIdentifier</code> avec une valeur aléatoire commençant par <code>awsbackup-</code> et se terminant par <code>-restore-test</code> <code>engine</code> avec une valeur définie sur le moteur du point de récupération en cours de restauration	<code>availabilityZones</code> <code>databaseName</code> <code>dbClusterParameterGroupName</code> <code>dbSubnetGroupName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>engine</code> <code>engineMode</code> <code>engineVersion</code> <code>kmskeyId</code> <code>port</code> <code>optionGroupName</code> <code>scalingConfiguration</code> <code>vpcSecurityGroupIds</code>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Instances Amazon RDS	<code>dbInstanceIdentifier</code> avec une valeur aléatoire commençant par <code>awsbackup-restore-test-</code> <code>deletionProtection</code> avec une valeur définie sur <code>false</code> <code>multiAz</code> avec une valeur définie sur <code>false</code> <code>publiclyAccessible</code> avec une valeur définie sur <code>false</code>	<code>allocatedStorage</code> <code>availabilityZones</code> <code>dbInstanceClass</code> <code>dbName</code> <code>dbParameterGroupName</code> <code>dbSubnetGroupName</code> <code>domain</code> <code>domainIamRoleName</code> <code>enableCloudwatchLogsExports</code> <code>enableIamDatabaseAuthentication</code> <code>iops</code> <code>licensemodel</code> <code>multiAz</code> <code>optionGroupName</code> <code>port</code> <code>processorFeatures</code> <code>publiclyAccessible</code> <code>storageType</code> <code>vpcSecurityGroupIds</code>

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon Simple Storage Service (Amazon S3)	<code>destinationBucketName</code> avec une valeur aléatoire commençant par <code>awsbackup-restore-test-</code> <code>encrypted</code> avec une valeur définie sur <code>true</code> <code>encryptionType</code> avec une valeur définie sur <code>SSE-S3</code> <code>newBucket</code> avec une valeur définie sur <code>true</code>	<code>encryptionType</code> <code>kmsKey</code>

Restaurer la validation des tests

Vous avez la possibilité de créer une validation pilotée par des événements qui s'exécute lorsqu'une tâche de test de restauration est terminée.

Tout d'abord, créez un flux de validation avec n'importe quelle cible prise en charge par Amazon EventBridge, telle que AWS Lambda. Ensuite, ajoutez une EventBridge règle qui attend que la tâche de restauration atteigne son statut `COMPLETED`. Troisièmement, créez un plan de test de restauration (ou laissez un plan existant s'exécuter comme prévu). Enfin, une fois le test de restauration terminé, surveillez les journaux du flux de travail de validation pour vous assurer qu'il s'est déroulé comme prévu (une fois la validation exécutée, un statut de validation s'affiche dans la [AWS Backup console](#)).

1. Configurer le flux de travail de validation

Vous pouvez configurer un flux de travail de validation à l'aide de Lambda ou de toute autre cible prise en charge par EventBridge. Par exemple, si vous validez un test de restauration contenant une EC2 instance Amazon, vous pouvez inclure du code qui envoie un ping à un point de terminaison de contrôle de santé.

Vous pouvez utiliser les détails de l'événement pour déterminer la ou les ressources à valider.

Vous pouvez utiliser des [couches Lambda](#) pour utiliser le dernier SDK (car il n'PutRestoreValidationResult pas disponible via le SDK Lambda).

Voici un exemple :

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. Ajouter une EventBridge règle

[Créez une EventBridge règle](#) qui écoute l'[COMPLETEDÉvénement](#) de la tâche de restauration.

Vous pouvez éventuellement filtrer les événements par type de ressource ou restaurer l'ARN du plan de test. Définissez la cible de cette règle pour appeler le flux de travail de validation que vous avez défini à l'étape 1. Voici un exemple :

```
{
  "source": [
    "aws.backup"
  ],
  "detail-type": [
    "Restore Job State Change"
  ],
```

```
"detail":{
  "resourceType":[
    "...",
  ],
  "restoreTestingPlanArn":[
    "...",
  ],
  "status":[
    "COMPLETED"
  ]
}
```

3. Laisser le plan de test de restauration s'exécuter et se terminer

Le plan de test de restauration s'exécutera conformément au calendrier que vous avez configuré.

Voir [Créer un plan de test de restauration](#) si vous n'en avez pas encore un ou [Mettre à jour un plan de test de restauration](#) si vous souhaitez modifier les paramètres.

4. Surveillez les résultats

Une fois qu'un plan de test de restauration a été exécuté comme prévu, vous pouvez consulter les journaux de votre flux de travail de validation pour vous assurer qu'il s'est déroulé correctement.

Vous pouvez appeler l'API `PutRestoreValidationResult` pour publier les résultats, qui seront ensuite consultables dans la [AWS Backup console](#) et via des appels d' AWS Backup API décrivant et répertoriant les tâches de restauration, telles que `DescribeRestoreJob` ou `ListRestoreJob`.

Une fois qu'un statut de validation est défini, il ne peut pas être modifié.

Arrêter une tâche de sauvegarde

Vous pouvez arrêter une tâche de sauvegarde une AWS Backup fois qu'elle a été lancée. Dans ce cas, la sauvegarde n'est pas créée et l'enregistrement de la tâche de sauvegarde est conservé avec l'état `aborted` (abandonnée).

Pour arrêter une tâche de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation de gauche, choisissez Jobs (Tâches).
3. Choisissez la tâche de sauvegarde que vous souhaitez arrêter.
4. Dans le panneau des détails de la tâche de sauvegarde, choisissez Stop (Arrêter).

Afficher les sauvegardes existantes

Vous pouvez consulter la liste de vos sauvegardes à l'aide de la [AWS Backup console](#) ou par programmation.

Rubriques

- [Liste des sauvegardes par ressource protégée dans la console](#)
- [Liste des sauvegardes par coffre-fort de sauvegarde dans la console](#)
- [Liste des sauvegardes par programmation](#)

Liste des sauvegardes par ressource protégée dans la console

Suivez les étapes ci-dessous pour afficher une liste des sauvegardes pour une ressource spécifique sur la console AWS Backup .

1. Connectez-vous au et ouvrez AWS Management Console la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Choisissez une ressource protégée dans la liste afin d'afficher la liste des sauvegardes. Seules les ressources qui ont été sauvegardées par AWS Backup sont répertoriées sous Ressources protégées.

Vous pouvez afficher les sauvegardes pour la ressource. Cette vue vous permet également de choisir une sauvegarde et de la restaurer.

Liste des sauvegardes par coffre-fort de sauvegarde dans la console

Suivez les étapes ci-dessous pour afficher une liste des sauvegardes organisées dans un coffre-fort de sauvegarde.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Dans la section Backups (Sauvegardes), affichez la liste de toutes les sauvegardes organisées dans ce coffre-fort de sauvegarde. Dans cette vue, vous pouvez trier les sauvegardes en fonction de n'importe quel en-tête de colonne (y compris le statut), ainsi que sélectionner une sauvegarde pour la restaurer, la modifier ou la supprimer.

Liste des sauvegardes par programmation

Vous pouvez répertorier les sauvegardes par programmation à l'aide des opérations d'API `ListRecoveryPoint` :

- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByResource](#)

Par exemple, la commande suivante AWS Command Line Interface (AWS CLI) répertorie toutes vos sauvegardes avec le EXPIRED statut :

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]
```

AWS Backup Audit Manager

Vous pouvez utiliser AWS Backup Audit Manager pour vérifier la conformité de vos AWS Backup politiques par rapport aux contrôles que vous définissez. Un contrôle est une procédure conçue pour réaliser un audit de la conformité d'une exigence de sauvegarde, telle que la fréquence des sauvegardes ou la période de rétention des sauvegardes.

AWS Backup Audit Manager vous aide à répondre à des questions telles que :

- « Est-ce que je sauvegarde toutes mes ressources ? »
- « Toutes mes sauvegardes sont-elles chiffrées ? »
- « Mes sauvegardes ont-elles lieu quotidiennement ? »

Vous pouvez utiliser AWS Backup Audit Manager pour rechercher les activités de sauvegarde et les ressources qui ne sont pas encore conformes aux contrôles que vous avez définis. Notez que seules les ressources actives seront incluses lorsque les contrôles évalueront la conformité des ressources. Par exemple, une EC2 instance Amazon en cours d'exécution sera évaluée. Une EC2 instance à l'état arrêté ne sera pas incluse dans l'évaluation de conformité.

Vous pouvez également l'utiliser pour générer automatiquement une piste d'audit de rapports quotidiens et à la demande à des fins de gouvernance de sauvegarde.

Les étapes suivantes fournissent une vue d'ensemble de l'utilisation d' AWS Backup Audit Manager. Pour des présentations détaillées, choisissez l'un des sujets à la fin de cette page.

1. Créez des frameworks contenant un ou plusieurs modèles de contrôle de gouvernance. Les questions précédentes sont des exemples de trois modèles de contrôle de gouvernance. Vous pouvez personnaliser les paramètres de certains modèles de contrôle de gouvernance. Par exemple, vous pouvez personnaliser le dernier contrôle pour demander : « Mes sauvegardes ont-elles lieu chaque semaine ? » plutôt que tous les jours.
2. Consultez votre framework pour voir combien de vos ressources sont conformes (ou non conformes) aux contrôles que vous avez définis dans ce framework.
3. Créez des rapports sur le statut de vos sauvegardes et de votre conformité. Conservez ces rapports comme preuve démontrable de vos pratiques de conformité ou pour identifier les activités de sauvegarde individuelles et les ressources qui ne sont pas encore conformes.

AWS Backup Audit Manager génère automatiquement un nouveau rapport toutes les 24 heures et le publie sur Amazon S3. Vous pouvez également générer des rapports à la demande.

Note

Avant de créer votre premier framework lié à la conformité, vous devez activer le suivi des ressources. Cela permet AWS Config de suivre vos AWS Backup ressources. Pour obtenir de la documentation technique sur la gestion du suivi des ressources, consultez la section [Configuration à l' AWS Config aide de la console](#) dans le guide du AWS Config développeur. Des frais s'appliquent lorsque vous activez le suivi des ressources. Pour plus d'informations sur le suivi des ressources, la tarification et la facturation pour AWS Backup Audit Manager, consultez la section [Comptage, coûts et facturation](#).

Rubriques

- [Utilisation de frameworks d'audit](#)
- [Utilisation des rapports d'audit](#)
- [Utilisation AWS Backup d'Audit Manager avec CloudFormation](#)
- [Utilisation AWS Backup d'Audit Manager avec AWS Audit Manager](#)
- [Contrôles et mesures correctives](#)

Utilisation de frameworks d'audit

Un framework est un ensemble de contrôles qui vous aide à évaluer vos pratiques de sauvegarde. Vous pouvez utiliser des contrôles personnalisables prédéfinis pour définir vos politiques et évaluer si vos pratiques de sauvegarde sont conformes à vos politiques. Vous pouvez également configurer des rapports quotidiens automatiques pour obtenir des informations sur le statut de conformité de vos frameworks.

Chaque cadre s'applique à un seul compte et Région AWS. Vous pouvez déployer un maximum de 15 frameworks par compte et par région. Vous ne pouvez pas déployer de frameworks dupliqués (cadres contenant les mêmes contrôles et paramètres).

Il existe deux types différents de frameworks :

- Le framework AWS Backup (recommandé) : utilisez le framework AWS Backup pour déployer tous les contrôles disponibles afin de surveiller votre activité de sauvegarde, votre couverture et vos ressources par rapport aux bonnes pratiques que nous recommandons.
- Un framework personnalisé que vous définissez : utilisez un framework personnalisé pour choisir un ou plusieurs contrôles spécifiques et pour personnaliser les paramètres de contrôle.

Rubriques

- [Choix de vos contrôles](#)
- [Activation du suivi des ressources](#)
- [Création de frameworks à l'aide de la console AWS Backup](#)
- [Création de frameworks à l'aide de l' AWS Backup API](#)
- [Affichage du statut de conformité du framework](#)
- [Recherche de ressources non conformes](#)
- [Mise à jour de frameworks d'audit](#)
- [Suppression de frameworks d'audit](#)

Choix de vos contrôles

Le tableau suivant répertorie les contrôles AWS Backup Audit Manager, leurs paramètres personnalisables et leurs types de ressources AWS Config d'enregistrement.

Contrôles disponibles

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Les ressources de sauvegarde sont incluses dans au moins un plan de sauvegarde	Évalue si les ressources sont incluses dans au moins un plan de sauvegarde.	Aucune	AWS Backup: backup selection
Le plan de sauvegarde a une fréquence	Évalue si la fréquence des sauvegardes est d'au moins [1 jour]	Fréquence de sauvegarde ; période de rétention	AWS Backup: backup plans

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
minimale et une rétention minimale	et si la période de rétention est d'au moins [35 jours].		
Les coffres-forts empêchent la suppression manuelle des points de récupération	Évalue si les coffres-forts de sauvegarde n'autorisent pas la suppression manuelle des points de restauration, sauf pour certains rôles Gestion des identités et des accès AWS (IAM). Par défaut, il n'existe aucune exception de rôle IAM. Il n'existe pas non plus d'exception au rôle IAM lorsque vous déployez ce contrôle avec le AWS Backup framework.	Jusqu'à 5 rôles IAM permettant la suppression manuelle des points de récupération	AWS Backup: backup vaults
Les points de récupération sont chiffrés	Évalue si les points de récupération sont chiffrés.	Aucune	AWS Backup: recovery points
Rétention minimale établie pour le point de récupération	Évalue si la période de rétention du point de récupération est d'au moins [35 jours].	Période de rétention du point de récupération	AWS Backup: recovery points

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Une copie de sauvegarde entre régions est planifiée	Évalue si une ressource est configurée pour créer des copies de ses sauvegardes vers une autre Région AWS.	Région AWS	AWS Backup: backup selection
Une copie de sauvegarde entre comptes est planifiée	Évalue si une copie de sauvegarde entre comptes est configurée pour une ressource.	AWS ID de compte	AWS Backup: backup selection
Les ressources sont incluses dans un plan de sauvegarde avec un AWS Backup Vault Lock	Évalue si une ressource dispose d'un plan de sauvegarde configuré pour stocker les sauvegardes dans un coffre de sauvegarde verrouillé.	Nombre minimum de jours de rétention ; nombre maximal de jours de rétention	AWS Backup: backup selection
Le dernier point de récupération a été créé	Évalue si un point de récupération a été créé dans le délai spécifié.	Valeur en heures [1 à 744] ou en jours [1 à 31].	AWS Backup recovery points
Temps de restauration des ressources pour atteindre l'objectif	Évalue si la tâche de tests de la restauration s'est terminée dans le délai de restauration cible	Valeur en minutes	Aucune

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Les ressources se trouvent dans un coffre hermétique logiquement	Évalue si les ressources ont au moins un point de récupération copié dans un coffre-fort logiquement isolé dans les limites de la valeur et du délai spécifiés.	Valeur en minutes, heures ou jours	AWS Backup : recovery points

Pour plus d'informations sur ces contrôles, consultez [Contrôles et mesures correctives](#).

Pour obtenir la liste des ressources AWS Backup prises en charge qui ne prennent pas en charge tous les contrôles, consultez la section AWS Backup Audit Manager du [Disponibilité des fonctionnalités par ressource](#) tableau.

Note

Si vous ne souhaitez utiliser aucune des commandes précédentes, vous pouvez toujours utiliser AWS Backup Audit Manager pour créer des rapports quotidiens sur vos tâches de sauvegarde, de copie et de restauration. Consultez [Utilisation des rapports d'audit](#).

Activation du suivi des ressources

Avant de créer votre premier framework lié à la conformité, vous devez activer le suivi des ressources. Cela permet AWS Config de suivre vos AWS Backup ressources. Pour obtenir de la documentation technique sur la gestion du suivi des ressources, consultez la section [Configuration à l' AWS Config aide de la console](#) dans le guide du AWS Config développeur.

Des frais s'appliquent lorsque vous activez le suivi des ressources. Pour plus d'informations sur le suivi des ressources, la tarification et la facturation pour AWS Backup Audit Manager, consultez la section [Comptage, coûts et facturation](#).

Rubriques

- [Activation du suivi des ressources à l'aide de la console](#)
- [Activation du suivi des ressources à l'aide de l' AWS Command Line Interface \(AWS CLI\)](#)
- [Activation du suivi des ressources avec un modèle CloudFormation](#)

Activation du suivi des ressources à l'aide de la console

Pour activer le suivi des ressources à l'aide de la console :

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, sous Audit Manager, choisissez Cadres.
3. Activez le suivi des ressources en choisissant Gérer le suivi des ressources.
4. Choisissez Accéder aux AWS Config paramètres.
5. Choisissez Activer ou désactiver l'enregistrement.
6. Choisissez Activer l'enregistrement pour tous les types de ressources suivants ou choisissez d'activer l'enregistrement pour certains types de ressources. Consultez [Contrôles et corrections d'AWS Backup Audit Manager](#) pour savoir quels types de ressources sont requis pour vos contrôles.
 - AWS Backup: backup plans
 - AWS Backup: backup vaults
 - AWS Backup: recovery points
 - AWS Backup: backup selection
7. Choisissez Fermer.
8. Attendez que la bannière bleue avec le texte Activation du suivi des ressources se transforme en bannière verte avec le texte Le suivi des ressources est activé.

Vous pouvez vérifier si vous avez activé le suivi des ressources et, dans l'affirmative, quels types de ressources vous enregistrez, à deux endroits de la AWS Backup console. Dans le volet de navigation de gauche, vous avez deux options :

- Choisissez Cadres, puis choisissez le texte sous Statut de l'enregistreur AWS Config .
- Choisissez Paramètres, puis choisissez le texte sous Statut de l'enregistreur AWS Config .

Activation du suivi des ressources à l'aide de l' AWS Command Line Interface (AWS CLI)

Si vous n'êtes pas encore inscrit à AWS Config, il peut être plus rapide de le faire en utilisant le. AWS CLI

Pour activer le suivi des ressources à l'aide de l' AWS CLI :

1. Tapez la commande suivante pour déterminer si vous avez déjà activé votre enregistreur AWS Config .

```
$ aws configservice describe-configuration-recorders
```

- a. Si votre liste ConfigurationRecorders est vide comme ceci :

```
{
  "ConfigurationRecorders": []
}
```

Votre enregistreur n'est pas activé. Passez à l'étape 2 pour créer votre enregistreur.

- b. Si vous avez déjà activé l'enregistrement pour toutes les ressources, votre sortie ConfigurationRecorders ressemblera à ceci :

```
{
  "ConfigurationRecorders": [
    {
      "recordingGroup": {
        "allSupported": true,
        "resourceTypes": [

        ],
        "includeGlobalResourceTypes": true
      },
      "roleARN": "arn:aws:iam::[account]:role/[roleName]",
      "name": "default"
    }
  ]
}
```

Comme vous avez activé toutes les ressources, vous avez déjà activé le suivi des ressources. Il n'est pas nécessaire de suivre le reste de cette procédure pour utiliser AWS Backup Audit Manager.

2. Créez un AWS Config enregistreur avec les types de ressources AWS Backup Audit Manager

```
$ aws configservice put-configuration-recorder --configuration-recorder
  name=default, \
  roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
  AWSServiceRoleForConfig \
  --recording-group
    resourceTypes=['AWS::Backup::BackupPlan', 'AWS::Backup::BackupSelection', \
  'AWS::Backup::BackupVault', 'AWS::Backup::RecoveryPoint']"
```

3. Décrivez votre AWS Config enregistreur.

```
$ aws configservice describe-configuration-recorders
```

Vérifiez qu'il possède les types de ressources AWS Backup Audit Manager en comparant votre sortie avec la sortie attendue suivante.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint"
        ]
      }
    }
  ]
}
```

4. Créez un compartiment Amazon S3 comme destination pour stocker les fichiers AWS Config de configuration.

```
$ aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

5. *policy.json* À utiliser pour accorder AWS Config l'autorisation d'accéder à votre compartiment. Consultez l'exemple suivant *policy.json*.

```
$ aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
```

```

    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  }
]
}

```

6. Configurez votre bucket comme canal AWS Config de distribution

```

$ aws configservice put-delivery-channel --delivery-channel
name=default,s3BucketName=amzn-s3-demo-bucket

```

7. Activer AWS Config l'enregistrement

```

$ aws configservice start-configuration-recorder --configuration-recorder-
name default

```

8. Vérifiez que "FrameworkStatus": "ACTIVE" se trouve dans la dernière ligne de votre sortie DescribeFramework comme suit.

```

$ aws backup describe-framework --framework-name test --region us-east-1

```

```

{
  "FrameworkName": "test",
  "FrameworkArn": "arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription": "",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters": [
        {
          "ParameterName": "requiredRetentionDays",
          "ParameterValue": "1"
        }
      ],
      "ControlScope": {
      }
    },
    {
      "ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters": [
        {

```



```

        "ParameterName": "requiredFrequencyUnit",
        "ParameterValue": "hours"
    },
    {
        "ParameterName": "requiredRetentionDays",
        "ParameterValue": "35"
    },
    {
        "ParameterName": "requiredFrequencyValue",
        "ParameterValue": "1"
    }
],
"ControlScope": {

}
},
{
    "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
    "ControlInputParameters": [

    ],
    "ControlScope": {

    }
},
{
    "ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
    "ControlInputParameters": [

    ],
    "ControlScope": {

    }
},
{
    "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
    "ControlInputParameters": [

    ],
    "ControlScope": {

    }
}
],

```

```
"CreationTime":1633463605.233,  
"DeploymentStatus":"COMPLETED",  
"FrameworkStatus":"ACTIVE"  
}
```

Activation du suivi des ressources avec un modèle CloudFormation

Pour un CloudFormation modèle qui active le suivi des ressources, consultez la section [Utilisation AWS Backup d'Audit Manager avec CloudFormation](#).

Création de frameworks à l'aide de la console AWS Backup

Après avoir activé le suivi des ressources, créez un framework en suivant les étapes ci-dessous.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Cadres.
3. Choisissez Créer un cadre.
4. Pour Nom du cadre, entrez un nom unique. Ce nom de framework doit contenir entre 1 et 256 caractères, commencer par une lettre et être composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).
5. (Facultatif) Entrez une Description du cadre.
6. Dans Contrôles, vos contrôles actifs seront affichés. Par défaut, tous les contrôles éligibles à une ressource sont répertoriés.

Pour modifier les contrôles actifs, cliquez sur Modifier les contrôles.

- a. La première case à cocher indique si le contrôle est activé. Pour désactiver un contrôle, décochez la case.
- b. Sous Choisir les ressources à évaluer, vous pouvez sélectionner le mode de sélection des ressources, soit par type, soit par balise, soit par ressource unique.

La liste des [contrôles d'AWS Backup Audit Manager](#) décrit les options de personnalisation pour chaque contrôle.

7. (Facultatif) Balisez votre framework en choisissant Ajouter une nouvelle balise. Vous pouvez utiliser des balises pour rechercher et filtrer vos frameworks ou suivre vos coûts.
8. Choisissez Créer un cadre.

AWS Backup Audit Manager peut prendre plusieurs minutes pour créer le framework.

Si l'erreur `AlreadyExists` se produit, un framework avec les mêmes contrôles et paramètres existe déjà. Pour créer correctement un nouveau framework, au moins un contrôle ou paramètre doit être différent des frameworks existants.

Création de frameworks à l'aide de l' AWS Backup API

Le tableau suivant contient des exemples de demandes d'API pour [CreateFramework](#) pour chaque contrôle, ainsi que des exemples de réponses d'API aux demandes [DescribeFramework](#) correspondantes. Pour utiliser AWS Backup Audit Manager par programmation, vous pouvez vous référer à ces extraits de code.

Contrôle	Demande d' CreateFramework	Réponse de DescribeFramework
Backup resources are included in at least one backup plan	<pre>{ "FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags":</pre>	<pre>{ "FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["RDS"] } }] }</pre>

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
	<pre>{"key1": "foo"} }</pre>	<pre> }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
Backup plan minimum frequency and minimum retention	<pre>{ "FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }, { "ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours" }, { "ParameterName": "requiredFrequencyValue", "ParameterValue": "24" }], "ControlScope": { "Tags": { "key1": "prod" } } }] }</pre>	<pre>{ "FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }, { "ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours" }, { "ParameterName": "requiredFrequencyValue", "ParameterValue": "24" }], "ControlScope": { </pre>

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
	<pre>"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>	<pre> "Tags": {"key1": "prod"} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
Vaults prevent manual deletion of recovery points	<pre>{ "FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{ "ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSEAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:role/service-role/QuickSightAction" }], "ControlScope": { "ComplianceResourceIds": ["default"] } }] }</pre>	<pre>{ "FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{ "ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSEAccess", "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer", "arn:aws:iam::123456789012:r</pre>

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
	<pre>"ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"], "ComplianceResourceTypes": ["AWS::Backup::BackupVault"] }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
Minimum retention established for recovery point	<pre>{ "FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{ "ParameterName": "requiredRetentionDays", "ParameterValue": "35" }], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags": {} }</pre>

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
		<pre>{ "key1": "foo" }</pre>

Backup recovery points are encrypted

```
{
  "FrameworkName": "Control5",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters": [],
      "ControlScope": {} // Default scope (no scope input) is all recovery points
    }
  ],
  "IdempotencyToken": "Control5",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```

```
{
  "FrameworkName": "Control5",
  "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-7e7655ae-1e31-45cb-96a0-4f43d8c19642",
  "FrameworkDescription": "This is a test framework",
  "FrameworkControls": [
    {
      "ControlName": "BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters": [],
      "ControlScope": {}
    }
  ],
  "CreationTime": 1516925490,
  "DeploymentStatus": "Active",
  "FrameworkStatus": "Completed",
  "IdempotencyToken": "Control5",
  "FrameworkTags": {
    "key1": "foo"
  }
}
```

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
Cross-Region backup copy is scheduled	<pre>{ "FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d'CreateFramework	Réponse de DescribeFramework
Cross-account backup copy is scheduled	<pre>{ "FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFrameworks
Resources are in a backup plan with an AWS Backup Vault Lock	<pre>{ "FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
Last recovery point was created	<pre>{ "FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": { "key1": "foo" } }</pre>	<pre>{ "FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
Restore time for resources meet target	<pre>{ "FrameworkName": "Control10", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters": [{ "ParameterName": "maxRestoreTime", "ParameterValue": "720" }], "ControlScope": { "ComplianceResourceIds": ["ComplianceResourceTypes": ["DynamoDB"] }], "IdempotencyToken": "Control10", "FrameworkTags": { "key1": "foo" } }] }</pre>	<pre>{ "FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control10-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d' CreateFramework	Réponse de DescribeFramework
	}	

Contrôle	Demande d>CreateFramework	Réponse de DescribeFramework
RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT	<pre>{ "FrameworkName": "Control11", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT", "ControlInputParameters": [{ "ParameterName": "recoveryPointAgeValue", "ParameterValue": "10" }, { "ParameterName": "recoveryPointAgeUnit", "ParameterValue": "days" }], "ControlScope": { "ComplianceResourceTypes": ["EC2"] } }], "IdempotencyToken": "Control11", "FrameworkTags": {</pre>	<pre>{ "FrameworkName": "Control11", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control11-ab1234cd-5e67-89fg-06a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{ "ControlName": "", "ControlInputParameters": [], "ControlScope": { "ComplianceResourceTypes": ["EC2", "EBS"] } }], "CreationTime": 1726087776.316, "DeploymentStatus": "COMPLETED", "FrameworkStatus": "ACTIVE", "IdempotencyToken": "Control11", "FrameworkTags": { "key1": "foo" } }</pre>

Contrôle	Demande d' CreateFramework	Réponse de DescribeFramework
	<pre> { "key1": "foo" } </pre>	

Affichage du statut de conformité du framework

Une fois que vous avez créé un framework d'audit, il apparaît dans votre tableau Cadres. Vous pouvez consulter ce tableau en choisissant Frameworks dans le volet de navigation de gauche de la AWS Backup console. Pour consulter les résultats de l'audit de votre framework, choisissez son Nom du cadre. Vous accédez ainsi à la page Détails du cadre, qui comporte deux sections : Résumé et Contrôles.

La section Résumé répertorie les statuts suivants de gauche à droite :

- Le Statut de conformité est le statut de conformité global de votre framework d'audit, tel que déterminé par le statut de conformité de chacun de ses contrôles. Le statut de conformité de chaque contrôle est déterminé par le statut de conformité de chaque ressource qu'il évalue.

Le statut de conformité du framework est **Compliant** si toutes les ressources concernées par vos évaluations de contrôle ont validé ces évaluations. Si une ou plusieurs ressources échouent à une évaluation de contrôle, le statut de conformité sera **Non-Compliant**. Pour en savoir plus sur comment rechercher vos ressources non conformes, consultez [Recherche de ressources non conformes](#). Pour en savoir plus sur comment rendre vos ressources conformes, consultez la section sur les corrections dans [Contrôles et corrections d'AWS Backup Audit Manager](#).

- Le Statut du cadre indique si vous avez activé le suivi des ressources pour toutes vos ressources. Les statuts possibles sont les suivants :
 - **Active** lorsque l'enregistrement est activé pour toutes les ressources que le framework évalue.
 - **Partially active** lorsque l'enregistrement est désactivé pour au moins une ressource que le framework évalue.
 - **Inactive** lorsque l'enregistrement est désactivé pour toutes les ressources que le framework évalue.
 - **Unavailable** lorsque AWS Backup Audit Manager n'est pas en mesure de valider le statut de l'enregistrement pour le moment.

Pour corriger un statut **Partially active** ou **Inactive**

1. Choisissez Cadres dans le volet de navigation de gauche.
2. Choisissez Gérer le suivi des ressources.
3. Suivez les instructions affichées dans la fenêtre contextuelle pour activer l'enregistrement qui n'était pas activé auparavant pour vos types de ressources.

Pour plus d'informations sur les types de ressources qui nécessitent un suivi des ressources en fonction des contrôles que vous avez inclus dans vos frameworks, consultez le composant de ressources [Contrôles et corrections d'AWS Backup Audit Manager](#).

- Le Statut du déploiement fait référence au statut de déploiement de votre framework. Ce statut doit le plus souvent être Completed, mais peut également être Create in progress, Update in progress, Delete in progress et Failed.
 - Un statut Failed signifie que le framework ne s'est pas déployé correctement. [Supprimer le cadre](#), puis recréez-le via la [console AWS Backup](#) ou via l'[API AWS Backup](#).
- Les Contrôles conformes indiquent le nombre de contrôles du framework, toutes les évaluations ayant réussi.
- Les Contrôles non conformes indiquent le nombre de contrôles du framework avec au moins une évaluation ayant échoué.

La section Contrôles affiche les informations suivantes :

- Le Statut du contrôle fait référence au statut de conformité de chaque contrôle. Un contrôle peut être Compliant, ce qui signifie que toutes les ressources réussissent cette évaluation, Non-compliant, ce qui signifie qu'au moins une ressource n'a pas réussi cette évaluation, ou Insufficient data, ce qui signifie que le contrôle n'a trouvé aucune ressource à évaluer dans le cadre de l'évaluation.
- La Portée de l'évaluation peut limiter chaque contrôle à un ou plusieurs Types de ressources, à un ID de ressource ou à une Clé de balise et à une Valeur de balise, en fonction de la manière dont vous avez personnalisé votre contrôle lors de la création de votre framework d'audit. Si tous les champs sont vides (comme indiqué par un tiret, « - »), le contrôle évalue toutes les ressources applicables.

Recherche de ressources non conformes

AWS Backup Audit Manager vous aide à identifier les ressources non conformes de deux manières.

- Lorsque vous [affichez le statut de conformité du cadre](#), choisissez le nom du contrôle dans la section Détails. Cela vous amène à la AWS Config console, où vous pouvez consulter la liste de vos Non-Compliant ressources.
- Après avoir [créé un plan de rapport avec le modèle de conformité des ressources](#) qui inclut votre framework, vous pouvez [afficher votre rapport](#) pour identifier toutes vos ressources Non-Compliant sur tous vos contrôles.

En outre, votre Resource compliance report indique la dernière fois qu' AWS Backup Audit Manager a évalué chacun de vos contrôles.

Mise à jour de frameworks d'audit

Vous pouvez mettre à jour la description, les contrôles et les paramètres d'un framework d'audit existant.

Pour mettre à jour un framework existant

1. Dans le volet de navigation de gauche de la AWS Backup console, choisissez Frameworks.
2. Choisissez le framework que vous souhaitez modifier par son Nom du cadre.
3. Choisissez Modifier.

Suppression de frameworks d'audit

Pour supprimer un framework existant

1. Dans le volet de navigation de gauche de la AWS Backup console, choisissez Frameworks.
2. Choisissez le framework que vous souhaitez supprimer par son Nom du cadre.
3. Sélectionnez Delete (Supprimer).
4. Tapez le nom de votre framework et choisissez Supprimer le cadre.

Utilisation des rapports d'audit

AWS Backup Les rapports d'Audit Manager sont des preuves générées automatiquement de votre AWS Backup activité, telles que :

- Quelles tâches de sauvegarde ont été terminées et à quel moment
- Quelles ressources vous avez sauvegardé

Il existe deux types de rapports. Lorsque vous créez un rapport, vous en choisissez le type.

L'un de ces types est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives avec un contexte complet sur les propriétés du coffre, les configurations du plan de sauvegarde et les paramètres du cycle de vie. Les rapports de tâches n'affichent pas un statut `completed with issues`. Pour trouver ce statut, vous pouvez filtrer les `Completed` offres d'emploi comportant un ou plusieurs messages de statut. AWS Backup n'inclura un message d'état dans le cadre du statut `Completed` d'une tâche que si le message nécessite une attention ou une action.

Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur.

AWS Backup Audit Manager fournit un rapport quotidien dans votre compartiment Amazon S3. Si le rapport concerne la région et le compte actuels, vous pouvez choisir de recevoir le rapport au format CSV ou JSON. Dans le cas contraire, le rapport est disponible au format CSV. Le calendrier de publication du rapport quotidien peut fluctuer sur plusieurs heures car AWS Backup Audit Manager effectue une randomisation pour maintenir ses performances. Vous pouvez également exécuter un rapport à la demande à tout moment.

Tous les titulaires de comptes peuvent créer des rapports entre régions ; les titulaires de comptes de gestion et d'[administrateur délégué](#) peuvent également créer des rapports entre comptes.

Tip

Pour garantir que les rapports générés par les comptes d'administrateur délégué contiennent toutes les données des comptes des membres, [créez des cadres](#) dans chacun de ces comptes membres.

Contexte de rapport de travail amélioré

AWS Backup Les rapports de travail d'Audit Manager incluent désormais un contexte étendu pour aider les clients à mieux comprendre les opérations de sauvegarde, en particulier pour la surveillance déléguée des comptes d'administrateurs au sein des organisations.

Les rapports améliorés incluent désormais :

- Informations sur le coffre-fort : type de coffre-fort, état du verrouillage et détails du chiffrement
- Contexte du plan de sauvegarde : noms des plans, noms des règles, plannings et fuseaux horaires
- Paramètres du cycle de vie : périodes de conservation et paramètres de transition vers le stockage à froid
- Détails des ressources : noms des ressources et métadonnées de travail améliorées

Ce contexte étendu élimine le besoin d'appels d'API supplémentaires pour fournir des informations complètes sur les tâches dans un seul rapport. `DescribeBackupVault` `DescribeBackupPlan` `DescribeRecoveryPoint`

Note

Le contexte étendu fournit des informations qui nécessitaient auparavant des appels d'API distincts avec des autorisations supplémentaires. Assurez-vous que les utilisateurs ayant accès à ces rapports disposent des autorisations appropriées pour les informations améliorées fournies.

Vous pouvez avoir un maximum de 20 plans de rapport par Compte AWS.

Note

Les ressources telles que RDS qui ne sont pas en mesure d'afficher des octets incrémentiels de données d'une sauvegarde spécifique afficheront 0 pour la valeur `backupSizeInBytes`.

Pour permettre à AWS Backup Audit Manager de créer des rapports quotidiens ou à la demande, vous devez d'abord créer un plan de rapport à partir d'un modèle de rapport.

Rubriques

- [Choix de votre modèle de rapport](#)
- [Création de plans de rapport à l'aide de la console AWS Backup](#)
- [Création de plans de rapports à l'aide de l' AWS Backup API](#)
- [Création de rapports à la demande](#)
- [Affichage des rapports d'audit](#)
- [Mise à jour des plans de rapport](#)
- [Suppression de plans de rapport](#)

Choix de votre modèle de rapport

Un modèle de rapport définit les informations que votre plan de rapport inclut dans votre rapport. Lorsque vous automatisez vos rapports à l'aide d'un plan de rapports, AWS Backup Audit Manager vous fournit les rapports des dernières 24 heures. AWS Backup Audit Manager crée ces rapports entre 1 h et 5 h UTC. Il propose les modèles de rapports suivants.

Modèles de rapports Backup

Modèles de rapports Backup. Ces modèles vous fournissent des mises à jour quotidiennes sur vos tâches de sauvegarde, de restauration ou de copie avec un contexte étendu, notamment les propriétés du coffre-fort, les détails du plan de sauvegarde et les paramètres du cycle de vie. Vous pouvez utiliser ces rapports pour surveiller votre posture opérationnelle, comprendre les configurations de sauvegarde et identifier les défaillances susceptibles de nécessiter des mesures supplémentaires. Le tableau suivant répertorie le nom de chaque modèle de rapport de sauvegarde et son exemple de sortie.

Modèle de rapport Backup	Exemple de rapport au format JSON
BACKUP_JOB_REPORT	<pre>{ "reportItems": [{ "reportTimePeriodStart": "2021-07-14T00:00:00Z", "reportTimePeriodEnd": "2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2",</pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
	<pre> "backupJobId": "FCCB040A -9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "MyEC2Ins tance", "backupPlanArn": "arn:aws: backup:us-west-2:1122334455 66:backup-plan:349f2247-b48 9-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8- ff4e-4f1b-92e7-e13d3e65dcfb", "initiationDate": "2021-07- 14T23:53:47.229Z", "backupPlanName": "MyBackup Plan", "backupRuleName": "DailyBac kups", "backupRuleSchedule": "cron(0 5 ? * * *)", "backupRuleTimezone": "UTC", "startWindowEnd": "2021-07- 14T23:53:47.229Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "creationDate": "2021-07- 14T23:53:47.229Z", "completionDate": "2021-07- 15T00:16:07.282Z", "recoveryPointArn": "arn:aws: ec2:us-west-2::image/ami-03 0cafb98e5a6dcdf", "jobRunTime": "00:22:20", "backupSizeInBytes": 858993459 2, "backupVaultName": "Default", </pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
	<pre data-bbox="850 212 1422 957">{ "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "UNLOCKED", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/12345678-1234-1234-1234 -123456789012", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }</pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
COPY_JOB_REPORT	<pre> { "reportItems": [{ "reportTimePeriodStart": "2021-07-14T15:48:31Z", "reportTimePeriodEnd": "2021-07-15T15:48:31Z", "accountId": "112233445566", "region": "us-west-2", "copyJobId": "E0AD48A9-0560-B66 8-3EF0-941FDC0AD6B1", "jobStatus": "RUNNING", "jobRunTime": "2021-07- 16T00:00:00.010Z", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us- west-2:112233445566:instance/ i-0bc877aee7782ba75", "resourceName": "string", "initiationDate": "2021-07- 14T15:48:31Z", "backupPlanName": "string", "backupRuleName": "string", "backupRuleSchedule": "string", "backupRuleTimezone": "string", "startWindowEnd": "2021-07- 14T15:48:31Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "creationDate": "2021-07- 15T15:42:04.771Z", "completionDate": "2021-07- 16T00:16:07.282Z", "backupSizeInBytes": 858993459 2, "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ ami-007b3819f25697299", </pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
	<pre>"sourceBackupVaultArn": "arn:aws:backup:us-west-2:1 12233445566:backup-vault:Default", "destinationRecoveryPointAr n": "arn:aws:ec2:us-east-2::image/ ami-0eba2199a0bcece3c", "destinationBackupVaultArn" : "arn:aws:backup:us-east-2:1 12233445566:backup-vault:Default", "vaultType": "BACKUP_VAULT", "vaultLockStatus": "string", "isEncrypted": true, "encryptionKeyArn": "arn:aws: kms:us-west-2:112233445566: key/...", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }] }</pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
RESTORE_JOB_REPORT	<pre>{ "reportItems": [{ "reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z", "accountId": "112233445566", "region": "us-west-2", "restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E", "jobStatus": "RUNNING", "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae", "resourceName": "string", "initiationDate": "2021-07-14T15:53:30Z", "backupPlanName": "string", "backupRuleName": "string", "backupRuleSchedule": "string", "backupRuleTimezone": "string", "startWindowEnd": "2021-07-14T15:53:30Z", "backupOptions": {}, "isParentJob": false, "parentJobId": null, "vaultType": "BACKUP_VAULT", "vaultLockStatus": "string", "isEncrypted": true, "encryptionKeyArn": "arn:aws:kms:us-west-2:112233445566:key/...", "deleteAfterDays": 30, "moveToColdAfterDays": 7, "enableArchive": false, "sourceResourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75", }] }</pre>

Modèle de rapport Backup	Exemple de rapport au format JSON
	<pre> "backupVaultArn": "arn:aws: backup:us-west-2:1122334455 66:backup-vault:Default", "creationDate": "2021-07- 15T15:52:49.797Z", "backupSizeInBytes": 858993459 }, "percentDone": "0.00%", "iamRoleArn": "arn:aws: iam::112233445566:role/service- role/AWSBackupDefaultServiceRole" }] }</pre>

Modèles de rapports de conformité

Les Modèles de rapports de conformité vous offrent des rapports quotidiens sur la conformité de votre activité de sauvegarde et de vos ressources par rapport aux contrôles que vous avez définis dans un ou plusieurs de vos frameworks. Si le statut de conformité de l'un de vos frameworks est Non-compliant, consultez un rapport de conformité pour identifier les ressources non conformes.

Types de modèles de rapports de conformité

- `Control compliance report` vous aide à suivre le statut de conformité des contrôles que vous avez définis dans vos frameworks.
- `Resource compliance report` vous aide à suivre le statut de conformité de vos ressources par rapport aux contrôles que vous avez définis dans vos frameworks. Ces rapports incluent des résultats d'évaluation détaillés, notamment des informations d'identification sur les ressources non conformes que vous pouvez utiliser pour identifier et corriger ces ressources.

Le tableau suivant montre un exemple de sortie générée à partir d'un rapport de conformité.

Modèle de rapport de conformité	Exemple de rapport au format JSON
CONTROL_COMPLIANCE_REPORT	<pre>{</pre>

Modèle de rapport de conformité	Exemple de rapport au format JSON
	<pre> "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_Hours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:19.995Z", "numResourcesCompliant": 0, "numResourcesNonCompliant": 25, "controlScope": "{ComplianceResourceTypes: [],}", "controlParameters": "{\\requiredFrequencyValue\\":\\\"1\\\",\\ </pre>

Modèle de rapport de conformité	Exemple de rapport au format JSON
	<pre>"requiredRetentionDays\" : \"35\", \"requiredFrequencyUnit\" : \"hours \"}" }] }</pre>

Modèle de rapport de conformité	Exemple de rapport au format JSON
RESOURCE_COMPLIANCE_REPORT	<pre> { "reportItems": [{ "accountId": "112233445566", "region": "us-west-2", "frameworkName": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "resourceId": "AWS::EFS ::FileSystem/fs-63c74e66", "resourceType": "AWS::EFS ::FileSystem", "resourceComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-07- 07T18:55:40.963Z" }, { "accountId": "112233445566", "region": "us-west-2", "frameworkName": "MyTestFramework", "frameworkDescription": "", "controlName": "BACKUP_L AST_RECOVERY_POINT_CREATED", "resourceId": "AWS::EFS ::FileSystem/fs-b3d7c218", "resourceType": "AWS::EFS ::FileSystem", "resourceComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-07- 07T18:55:40.961Z" }] } </pre>

Modèles de rapports de numérisation

Modèles de rapports de numérisation. Ces modèles vous fournissent des mises à jour quotidiennes sur vos tâches de numérisation avec un contexte étendu, notamment les propriétés du coffre-fort et les détails du plan de sauvegarde. Vous pouvez utiliser ces rapports pour surveiller l'état de vos tâches d'analyse, vos rapports et identifier les défaillances susceptibles de nécessiter des mesures supplémentaires. Le tableau suivant répertorie le nom d'un modèle de rapport d'analyse et son exemple de sortie.

Modèle de rapport de numérisation	Exemple de rapport au format JSON
MALWARE_JOB_REPORT	<pre>{ "reportTimePeriodStart": "2025-11-09T00:00:00Z", "reportTimePeriodEnd": "2025-11-10T00:00:00Z", "accountId": "025066259999", "region": "us-east-1", "scanJobId": "489abba3-0a57-4207-93ff-d3947d85a8d3", "scanId": "9ddd3144f68ea3ee6e388c66a0b55467", "malwareScanner": "GUARDDUTY", "jobStatus": "RUNNING", "scanResultStatus": "", "statusMessage": "", "resourceType": "EBS", "resourceArn": "arn:aws:ec2:us-east-1:025066259999:volume/vol-0f1c480a6a9b33cb7", "backupPlanArn": "arn:aws:backup:us-east-1:025066259999:backup-plan:orgs/4232272a-ed54-3a88-b1d0-ace894b6c24c", "creationDate": "2025-10-28T17:30:50.820Z", "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-03fef858bad24c7a6", "backupVaultName": "Default",</pre>

Modèle de rapport de numérisation	Exemple de rapport au format JSON
	<pre> "backupVaultArn": "arn:aws: backup:us-east-1:0250662599 99:backup-vault:Default", "iamRoleArn": "arn:aws:iam::0250 66259999:role/service-role/ AWSBackupDefaultServiceRole", "scannerRoleArn": "arn:aws: iam::025066259999:role/AWSB ackupGuardDutyRolePolicyForScans" } </pre>

Création de plans de rapport à l'aide de la console AWS Backup

Il existe deux types de rapports. L'un d'entre eux est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives. Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur. Lorsque vous créez un rapport, vous choisissez le type de rapport à créer.

En fonction de votre type de compte, l'affichage de la console peut varier. Seuls les comptes de gestion bénéficieront de la fonctionnalité multi-comptes.

À l'instar d'un plan de sauvegarde, vous créez un plan de rapport pour automatiser la création de vos rapports et définir leur compartiment Amazon S3 de destination. Un plan de rapport nécessite que vous disposiez d'un compartiment S3 pour recevoir vos rapports. Vous ne pouvez pas utiliser un bucket provenant d'un autre compte. Pour obtenir des instructions sur la configuration d'un nouveau compartiment S3, consultez [Étape 1 : Créer votre premier compartiment S3](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour créer votre plan de rapport dans la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Choisissez Créer un plan de rapport.
4. Choisissez l'un des modèles de rapport dans la liste.

5. Entrez un Nom du plan de rapport unique. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).
6. (Facultatif) Entrez une Description du plan de rapport.
7. Modèles de rapports de conformité pour un seul compte. Choisissez un ou plusieurs frameworks sur lesquels effectuer le rapport. Vous pouvez ajouter un maximum de 1 000 frameworks à un plan de rapport.
 1. Choisissez votre AWS région.
 2. Choisissez un framework dans cette région.
 3. Choisissez Ajouter un cadre.
8. (Facultatif) Pour ajouter des balises à votre plan de rapport, choisissez Ajouter des balises au plan de rapport.
9. Si vous utilisez un compte de gestion, vous pouvez spécifier les comptes que vous souhaitez inclure dans ce plan de rapport. Vous pouvez sélectionner Uniquement mon compte, qui générera des rapports uniquement sur le compte auquel vous êtes actuellement connecté. Vous pouvez également sélectionner Un ou plusieurs comptes dans mon organisation (disponibles pour les comptes de gestion et d'administrateur délégué).
10. (Si vous créez un rapport de conformité pour une seule région, ignorez cette étape.) Vous pouvez sélectionner les régions à inclure dans votre rapport. Cliquez sur le menu déroulant pour afficher les régions disponibles. Sélectionnez Toutes les régions disponibles ou les régions que vous préférez.
 - La case à cocher Inclure les nouvelles régions lorsqu'elles sont intégrées dans Backup Audit Manager déclenchera l'inclusion de nouvelles régions dans vos rapports lorsqu'elles seront disponibles.
11. Choisissez le Format de fichier de votre rapport. Tous les rapports peuvent être exportés au format CSV. En outre, les rapports d'une seule région peuvent être exportés au format JSON.
12. Pour le nom du compartiment S3, choisissez un compartiment dans votre compte.
13. (Facultatif) Entrez un préfixe de compartiment.

AWS Backup livre votre compte courant, la région actuelle rend compte à s3://*amzn-s3-demo-bucket*/prefix/Backup/*accountID*/*Region*/year/month/day/report-name.

AWS Backup fournit vos rapports multi-comptes à s3://*amzn-s3-demo-bucket*/prefix/Backup/crossaccount/*Region*/year/month/day/report-name

AWS Backup fournit vos rapports interrégionaux à `s3://amzn-s3-demo-bucket/prefix/Backup/accountID/crossregion/year/month/day/report-name`

14. Choisissez Créer un plan de rapport.

Ensuite, vous devez autoriser votre compartiment S3 à recevoir des rapports de AWS Backup. Après avoir créé un plan de rapport, AWS Backup Audit Manager génère automatiquement une politique d'accès au compartiment S3 que vous pouvez appliquer.

Si vous chiffrez votre compartiment à l'aide d'une clé KMS gérée par le client, la politique de clé KMS doit répondre aux exigences suivantes :

- L'Principalattribut doit inclure l'ARN [AWSServiceRolePolicyForBackupReports](#) du rôle lié au service Backup Audit Manager.
- L'Actionattribut doit inclure `kms:GenerateDataKey` et `kms:Decrypt` au minimum.

La politique [AWSServiceRolePolicyForBackupReports](#) dispose de ces autorisations.

Pour afficher et appliquer cette stratégie d'accès à votre compartiment S3

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Modifier.
5. Choisissez Afficher la stratégie d'accès pour le compartiment S3. Vous pouvez également utiliser la politique à la fin de cette procédure.
6. Choisissez Copier les autorisations.
7. Choisissez Modifier la politique du compartiment. Notez que tant que le rapport de sauvegarde n'est pas créé pour la première fois, le rôle lié au service mentionné dans la politique du compartiment S3 n'existera pas encore, ce qui entraîne l'erreur « Principal non valide ».
8. Copiez les autorisations dans la Politique.

Exemple de politique de compartiment

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Si vous utilisez une méthode personnalisée AWS Key Management Service pour chiffrer votre compartiment S3 cible qui stocke les rapports, incluez les actions suivantes dans votre politique :

```
"Action": [
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource": [
  "*"
],
```

Création de plans de rapports à l'aide de l' AWS Backup API

Vous pouvez également utiliser des plans de rapport par programmation.

Il existe deux types de rapports. L'un d'entre eux est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives. Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur. Lorsque vous créez un rapport, vous choisissez le type de rapport à créer.

À l'instar d'un plan de sauvegarde, vous créez un plan de rapport pour automatiser la création de vos rapports et définir leur compartiment Amazon S3 de destination. Un plan de rapport nécessite que vous disposiez d'un compartiment S3 pour recevoir vos rapports. Pour obtenir des instructions sur la configuration d'un nouveau compartiment S3, consultez [Étape 1 : Créer votre premier compartiment S3](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous chiffrez votre compartiment à l'aide d'une clé KMS personnalisée, la politique de clé KMS doit répondre aux exigences suivantes :

- L'Principalattribut doit inclure l'ARN [AWSServiceRolePolicyForBackupReports](#) du rôle lié au service Backup Audit Manager.
- L'Actionattribut doit inclure kms:GenerateDataKey et kms:Decrypt au minimum.

La politique [AWSServiceRolePolicyForBackupReports](#) dispose de ces autorisations.

Pour les rapports à compte unique ou à région unique, utilisez la syntaxe suivante pour appeler [CreateReportPlan](#).

```
{
  "ReportPlanName": "string",
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
    "ReportDeliveryChannel": {
      "S3BucketName": "string",
      "S3KeyPrefix": "string",
      "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
CSV if left blank.
    },
    "ReportPlanTags": {
      "string" : "string" // Optional.
    }
  }
}
```

```

},
"IdempotencyToken": "string"
}

```

Lorsque vous appelez [DescribeReportPlan](#) avec le nom unique d'un plan de rapport, l'API AWS Backup répond avec les informations suivantes.

```

{
  "ReportPlanArn": "string",
  "ReportPlanName": "string",
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "ReportTemplate": enum,
  },
  "ReportDeliveryChannel": {
    "S3BucketName": "string",
    "S3KeyPrefix": "string",
    "Formats": [ enum ]
  },
  "DeploymentStatus": enum
  "CreationTime": timestamp,
  "LastAttemptExecutionTime": timestamp,
  "LastSuccessfulExecutionTime": timestamp
}

```

Pour les rapports à comptes multiples et régions multiples, utilisez la syntaxe suivante pour appeler [CreateReportPlan](#).

```

{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ], *//Organization report only support CSV file*
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportPlanTags": {
    "string" : "string"
  },
  "ReportSetting": {
    "Accounts": [ "string" ], // Use string value of "R00T" to include all
    organizational units
  }
}

```

```

    "OrganizationUnits": [ "string" ],
    "Regions": ["string"], // Use wildcard value in string to include all Regions
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "ReportTemplate": "string"
  }
}

```

Lorsque vous appelez [DescribeReportPlan](#) avec le nom unique d'un plan de rapport, l'API AWS Backup répond avec les informations suivantes pour les plans à comptes multiples et régions multiples :

```

{
  "ReportPlan": {
    "CreationTime": number,
    "DeploymentStatus": "string",
    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
    },
    "ReportPlanArn": "string",
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportSetting": {
      "Accounts": [ "string" ],
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
    }
  }
}

```

Création de rapports à la demande

Vous pouvez générer de nouveaux rapports à votre convenance en créant un rapport à la demande en suivant les étapes suivantes. AWS Backup Audit Manager fournit votre rapport à la demande au compartiment Amazon S3 que vous avez spécifié dans votre plan de rapport.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Créer un rapport à la demande.

Vous pouvez générer un rapport à la demande pour un plan de rapport existant.

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Rapports sur les plans, sélectionnez un plan de rapport en cliquant sur la case d'option à côté du nom du plan de rapport.
4. Cliquez sur Actions, puis sur Créer un rapport à la demande.

Vous pouvez le faire pour plusieurs rapports, même s'ils sont en cours de génération.

Affichage des rapports d'audit

Vous pouvez ouvrir, consulter et analyser les rapports AWS Backup Audit Manager à l'aide des programmes que vous utilisez habituellement pour travailler avec des fichiers CSV ou JSON. Notez que les rapports pour plusieurs régions ou plusieurs comptes ne sont disponibles qu'au format CSV.

Les fichiers volumineux sont divisés en plusieurs rapports si la taille totale du fichier dépasse 50 Mo. Si les fichiers obtenus dépassent 50 Mo, AWS Backup Audit Manager créera des fichiers CSV supplémentaires avec le reste du rapport.

Pour afficher un rapport

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Sous Tâches du rapport, cliquez sur le lien du rapport pour afficher le rapport.
5. Si Statut du rapport est souligné en pointillé, choisissez-le pour obtenir des informations sur votre rapport.
6. Choisissez le rapport à afficher en fonction de son Heure d'achèvement.
7. Cliquez sur le lien S3. Cela ouvre votre compartiment S3 de destination.

8. Sous Nom, choisissez le nom d'un rapport que vous voulez afficher.
9. Pour enregistrer le rapport sur votre ordinateur, choisissez Télécharger.

Mise à jour des plans de rapport

Vous pouvez mettre à jour la description d'un plan de rapport existant, sa destination de livraison et son format. Le cas échéant, vous pouvez également ajouter ou supprimer des frameworks dans le plan de rapport.

Pour mettre à jour un plan de rapport existant

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Modifier.
5. Vous pouvez modifier les détails du plan de rapport, y compris le nom et la description du rapport, ainsi que les comptes et les régions inclus dans le rapport.

Suppression de plans de rapport

Vous pouvez supprimer un plan de rapport existant. Lorsque vous supprimez un plan de rapport, tous les rapports déjà créés par ce plan de rapport restent dans leur compartiment Amazon S3 de destination.

Pour supprimer un plan de rapport existant

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Sélectionnez Delete (Supprimer).
5. Entrez le nom de votre plan de rapport, puis choisissez Supprimer le plan de rapport.

Utilisation AWS Backup d'Audit Manager avec CloudFormation

Nous fournissons les exemples de CloudFormation modèles suivants à titre de référence :

Rubriques

- [Activation du suivi des ressources](#)
- [Déploiement des contrôles par défaut](#)
- [Exonération des rôles IAM de l'évaluation des contrôles](#)
- [Création d'un plan de rapport](#)

Activation du suivi des ressources

Le modèle suivant active le suivi des ressources, comme décrit dans [Activation du suivi des ressources](#).

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
```

```
    default: Configuration delivery channel name
Frequency:
    default: Snapshot delivery frequency
TopicArn:
    default: SNS topic name
NotificationEmail:
    default: Notification Email (optional)
```

Parameters:

AllSupported:

Type: String

Default: True

Description: Indicates whether to record all supported resource types.

AllowedValues:

- True
- False

IncludeGlobalResourceTypes:

Type: String

Default: True

Description: Indicates whether AWS Config records all supported global resource types.

AllowedValues:

- True
- False

ResourceTypes:

Type: List<String>

Description: A list of valid AWS resource types to include in this recording group, such as AWS::EC2::Instance or AWS::CloudTrail::Trail.

Default: <All>

DeliveryChannelName:

Type: String

Default: <Generated>

Description: The name of the delivery channel.

Frequency:

Type: String

Default: 24hours

Description: The frequency with which AWS Config delivers configuration snapshots.

AllowedValues:

- 1hour
- 3hours

- 6hours
- 12hours
- 24hours

TopicArn:

Type: String

Default: <New Topic>

Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification Service (Amazon SNS) topic that AWS Config delivers notifications to.

NotificationEmail:

Type: String

Default: <None>

Description: Email address for AWS Config notifications (for new topics).

Conditions:

IsAllSupported: !Equals

- !Ref AllSupported
- True

IsGeneratedDeliveryChannelName: !Equals

- !Ref DeliveryChannelName
- <Generated>

CreateTopic: !Equals

- !Ref TopicArn
- <New Topic>

CreateSubscription: !And

- !Condition CreateTopic
- !Not
 - !Equals
 - !Ref NotificationEmail
 - <None>

Mappings:**Settings:****FrequencyMap:**

1hour : One_Hour
3hours : Three_Hours
6hours : Six_Hours
12hours : Twelve_Hours
24hours : TwentyFour_Hours

Resources:**ConfigBucket:**

DeletionPolicy: Retain

Type: AWS::S3::Bucket

Properties:

BucketEncryption:

ServerSideEncryptionConfiguration:

- ServerSideEncryptionByDefault:

SSEAlgorithm: AES256

ConfigBucketPolicy:

Type: AWS::S3::BucketPolicy

Properties:

Bucket: !Ref ConfigBucket

PolicyDocument:

Version: 2012-10-17

Statement:

- Sid: AWSConfigBucketPermissionsCheck

Effect: Allow

Principal:

Service:

- config.amazonaws.com

Action: s3:GetBucketAcl

Resource:

- !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}"

- Sid: AWSConfigBucketDelivery

Effect: Allow

Principal:

Service:

- config.amazonaws.com

Action: s3:PutObject

Resource:

- !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}/AWSLogs/

\${AWS::AccountId}/*"

- Sid: AWSConfigBucketSecureTransport

Action:

- s3:*

Effect: Deny

Resource:

- !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}"

- !Sub "arn:\${AWS::Partition}:s3:::\${ConfigBucket}/*"

Principal: "*"

Condition:

Bool:

aws:SecureTransport:

false

```
ConfigTopic:
  Condition: CreateTopic
  Type: AWS::SNS::Topic
  Properties:
    TopicName: !Sub "config-topic-${AWS::AccountId}"
    DisplayName: AWS Config Notification Topic
    KmsMasterKeyId: "alias/aws/sns"
```

```
ConfigTopicPolicy:
  Condition: CreateTopic
  Type: AWS::SNS::TopicPolicy
  Properties:
    Topics:
      - !Ref ConfigTopic
    PolicyDocument:
      Statement:
        - Sid: AWSConfigSNSPolicy
          Action:
            - sns:Publish
          Effect: Allow
          Resource: !Ref ConfigTopic
          Principal:
            Service:
              - config.amazonaws.com
```

```
EmailNotification:
  Condition: CreateSubscription
  Type: AWS::SNS::Subscription
  Properties:
    Endpoint: !Ref NotificationEmail
    Protocol: email
    TopicArn: !Ref ConfigTopic
```

```
ConfigRecorderServiceRole:
  Type: AWS::IAM::ServiceLinkedRole
  Properties:
    AWSServiceName: config.amazonaws.com
    Description: Service Role for AWS Config
```

```
ConfigRecorder:
  Type: AWS::Config::ConfigurationRecorder
  DependsOn:
    - ConfigBucketPolicy
```

```

    - ConfigRecorderServiceRole
  Properties:
    RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
    RecordingGroup:
      AllSupported: !Ref AllSupported
      IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
      ResourceTypes: !If
        - IsAllSupported
        - !Ref AWS::NoValue
        - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
    ConfigSnapshotDeliveryProperties:
      DeliveryFrequency: !FindInMap
        - Settings
        - FrequencyMap
        - !Ref Frequency
    S3BucketName: !Ref ConfigBucket
    SnsTopicARN: !If
      - CreateTopic
      - !Ref ConfigTopic
      - !Ref TopicArn

```

Déploiement des contrôles par défaut

Le modèle suivant crée un framework avec les contrôles par défaut décrits dans [Contrôles et corrections d'AWS Backup Audit Manager](#).

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:

```



```

- ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
  ControlInputParameters:
    - ParameterName: requiredRetentionDays
      ParameterValue: '35'
- ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
  ControlInputParameters:
    - ParameterName: requiredRetentionDays
      ParameterValue: '35'
    - ParameterName: requiredFrequencyUnit
      ParameterValue: 'hours'
    - ParameterName: requiredFrequencyValue
      ParameterValue: '24'
  ControlScope:
    Tags:
      - Key: customizedKey
        Value: customizedValue
- ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
  ControlInputParameters:
    - ParameterName: crossRegionList
      ParameterValue: 'eu-west-2'
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
  ControlInputParameters:
    - ParameterName: crossAccountList
      ParameterValue: '111122223333'
- ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
- ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
- ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
  ControlInputParameters:
    - ParameterName: maxRestoreTime
      ParameterValue: '720'

```

Outputs:

FrameworkArn:

Value: !GetAtt TestFramework.FrameworkArn

Exonération des rôles IAM de l'évaluation des contrôles

Le contrôle `BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED` vous permet d'exempter jusqu'à cinq rôles IAM qui peuvent toujours supprimer manuellement des points de récupération. Le modèle suivant déploie ce contrôle et exempté également deux rôles IAM.

```

AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
      ControlInputParameters:
        - ParameterName: "principalArnList"
          ParameterValue: !Sub
            "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
            ConfigRole"

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn

```

Création d'un plan de rapport

Le modèle suivant crée un plan de rapport.

```

Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:

```

```
Formats:
  - "CSV"
S3BucketName: !Ref S3BucketName
S3KeyPrefix: !Ref S3KeyPrefix
ReportSetting:
  ReportTemplate: !Ref ReportTemplate
  Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
  Accounts: ['123456789098']
  OrganizationUnits: ['ou-abcd-1234wxyz']
ReportPlanTags:
  - Key: "a"
    Value: "1"
  - Key: "b"
    Value: "2"

Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

Utilisation AWS Backup d'Audit Manager avec AWS Audit Manager

AWS Backup Les contrôles d'Audit Manager sont mappés aux contrôles standard prédéfinis AWS Audit Manager, ce qui vous permet d'importer les résultats de conformité de votre AWS Backup Audit Manager dans vos AWS Audit Manager rapports. Vous souhaitez peut-être le faire pour aider un agent de la conformité, un responsable de l'audit ou un autre collègue qui rend compte des activités de sauvegarde dans le cadre de la posture de conformité globale de votre organisation.

Vous pouvez importer les résultats de conformité de vos contrôles AWS Backup Audit Manager dans vos AWS Audit Manager frameworks. AWS Audit Manager Pour permettre de collecter automatiquement des données à partir de vos contrôles AWS Backup Audit Manager, créez un contrôle personnalisé en AWS Audit Manager suivant les instructions de [personnalisation d'un contrôle existant](#) dans le Guide de l'AWS Audit Manager utilisateur. En suivant ces instructions, notez que la source de données des AWS Backup contrôles est AWS Config.

Pour obtenir la liste des AWS Backup commandes, consultez la section [Choix de vos commandes](#).

Contrôles et mesures correctives

Cette page répertorie les contrôles disponibles pour AWS Backup Audit Manager. Vous pouvez choisir le volet d'informations approprié pour afficher la liste des contrôles et accéder à un contrôle

spécifique. Pour comparer rapidement les contrôles, consultez le tableau dans [Choix de vos contrôles](#). Pour définir des contrôles par programmation, consultez les extraits de code dans [Création de cadres à l'aide de l'API AWS Backup](#).

Vous pouvez utiliser jusqu'à 50 contrôles par compte et par région. L'utilisation du même contrôle dans deux frameworks différents compte comme l'utilisation de deux contrôles de la limite de 50.

Cette page répertorie chaque contrôle avec les informations suivantes :

- Description. Les valeurs entre crochets (« [] ») sont les valeurs des paramètres par défaut.
- La ou les ressources évaluées par le contrôle.
- Les paramètres de la commande.
- Occasion où il y a perte de contrôle.
- L'étendue du contrôle, comme suit :
 - Vous pouvez spécifier Ressources par type en choisissant un ou plusieurs services pris en charge par AWS Backup.
 - Vous spécifiez une étendue des Ressources balisées avec une seule clé de balise et une valeur facultative.
 - Vous pouvez spécifier une ressource unique à l'aide de la liste déroulante Ressource unique.
- Étapes de correction pour rendre les ressources applicables conformes.

Notez que seules les ressources actives seront incluses lorsque les contrôles évalueront la conformité des ressources. Par exemple, une EC2 instance Amazon en cours d'exécution sera évaluée par le contrôle [Last recovery point was created](#). Une EC2 instance à l'état arrêté ne sera pas incluse dans l'évaluation de conformité.

Les ressources de sauvegarde sont incluses dans au moins un plan de sauvegarde

Description : Évalue si les ressources sont incluses dans au moins un plan de sauvegarde.

Ressource : AWS Backup: backup selection

Paramètres : Aucun

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type (par défaut)
- Ressource unique

Correction : attribuez les ressources à un plan de sauvegarde. AWS Backup protège automatiquement vos ressources une fois que vous les avez attribuées à un plan de sauvegarde. Pour plus d'informations, consultez [Affectation de ressources à un plan de sauvegarde](#).

Fréquence minimale du plan de sauvegarde et conservation minimale

Description : évalue si les plans de sauvegarde contiennent au moins une règle de sauvegarde dont la fréquence de sauvegarde est d'au moins [1 jour] et la période de rétention est d'au moins [35 jours].

Ressource : AWS Backup: backup plans

Paramètres :

- Fréquence de sauvegarde requise en nombre d'heures ou de jours.
- Période de rétention requise en jours, semaines, mois ou années. Nous recommandons une période de conservation à chaud d'au moins une semaine afin de permettre AWS Backup d'effectuer des sauvegardes incrémentielles lorsque cela est possible, en évitant des frais supplémentaires.

Se produit : modifications de configuration

Portée:

- Ressources balisées
- Ressource unique

Correction : [mettez à jour un plan de sauvegarde](#) pour modifier sa fréquence de sauvegarde, sa période de rétention ou les deux. La mise à jour de votre plan de sauvegarde modifie la période de rétention des points de récupération créés par le plan après votre mise à jour.

Les coffres-forts empêchent la suppression manuelle des points de récupération

Description : évalue si les coffres-forts de sauvegarde n'autorisent pas la suppression manuelle des points de récupération, sauf pour certains rôles IAM.

Ressource : AWS Backup: `backup vaults`

Paramètres : Les Amazon Resource Names (ARNs) d'un maximum de cinq rôles IAM permettaient de supprimer manuellement des points de récupération.

Se produit : modifications de configuration

Portée:

- Ressources balisées
- Ressource unique

Correction : créez ou modifiez une stratégie d'accès basée sur les ressources pour un coffre-fort de sauvegarde. Pour obtenir un exemple de politique et des instructions sur la façon de définir une politique d'accès au coffre de sauvegarde, consultez [Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde](#).

Les points de récupération sont chiffrés

Description : évalue si les points de récupération sont chiffrés.

Ressource : AWS Backup: `recovery points`

Paramètres : Aucun

Se produit : modifications de configuration

Portée:

- Ressources balisées

Correction : configurez le chiffrement pour les points de récupération. La façon dont vous configurez le chiffrement pour les points de AWS Backup récupération varie en fonction du type de ressource.

Vous pouvez configurer le chiffrement pour les types de ressources qui prennent en charge AWS Backup la gestion complète lors de l'utilisation AWS Backup. Si le type de ressource ne prend pas en charge AWS Backup la gestion complète, vous devez configurer son chiffrement de sauvegarde en suivant les instructions de ce service, telles que le [chiffrement Amazon EBS](#) dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud. Pour consulter la liste des types de ressources qui prennent en charge la AWS Backup gestion complète, consultez la section « AWS Backup Gestion complète » du [Disponibilité des fonctionnalités par ressource](#) tableau.

Rétention minimale établie pour le point de récupération

Description : évalue si la période de rétention du point de récupération est d'au moins [35 jours].

Ressource : AWS Backup: recovery points

Paramètres : période de rétention du point de récupération requise en jours, semaines, mois ou années. Nous recommandons une période de conservation à chaud d'au moins une semaine afin de permettre AWS Backup d'effectuer des sauvegardes incrémentielles lorsque cela est possible, en évitant des frais supplémentaires.

Se produit : modifications de configuration

Portée:

- Ressources balisées

Correction : modifiez les périodes de rétention de vos points de récupération. Pour plus d'informations, consultez [Modification d'une sauvegarde](#).

Une copie de sauvegarde entre régions est planifiée

Description : Évalue si une ressource est configurée pour créer des copies de ses sauvegardes AWS dans une autre région.

Ressource : AWS Backup: backup selection

Paramètres :

- Sélectionnez le Région AWS ou les endroits où la copie de sauvegarde doit se trouver (facultatif)
- Région

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction : mettez [à jour un plan de sauvegarde](#) pour modifier l' Région AWS endroit où la copie de sauvegarde doit se trouver.

Une copie de sauvegarde entre comptes est planifiée

Description : évalue si une ressource est configurée pour créer des copies de ses sauvegardes vers un autre compte. Vous pouvez ajouter jusqu'à 5 comptes pour que le contrôle soit évalué. Le compte de destination doit se trouver dans la même organisation que le compte source dans AWS Organizations.

Ressource : AWS Backup: backup selection

Paramètres :

- Sélectionnez le ou les ID de AWS compte sur lesquels la copie de sauvegarde doit exister (facultatif)
- ID de compte

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction : [mettez à jour un plan de sauvegarde](#) pour modifier ou ajouter le ou les identifiants de AWS compte sur lesquels la copie doit se trouver.

Les ressources sont incluses dans un plan de sauvegarde avec un AWS Backup Vault Lock

Description : évalue si une ressource possède des sauvegardes immuables stockées dans un coffre-fort de sauvegarde verrouillé.

Ressource : `AWS Backup: backup selection`

Paramètres :

- Entrez les jours de rétention minimum et maximum pour AWS Backup Vault Lock (facultatif)
- Nombre minimum de jours de rétention
- Nombre maximum de jours de rétention

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction : [verrouillez un coffre-fort de sauvegarde](#) pour définir son nom, modifiez ses jours de rétention minimum ou maximum, ou les deux. Peut également inclure `ChangeableForDays` pour un verrouillage de coffre-fort en mode conformité.

Le dernier point de récupération a été créé

Description : ce contrôle évalue si un point de récupération a été créé dans le délai spécifié (en jours ou en heures).

Le contrôle est conforme si un point de récupération de la ressource a été créé dans le délai spécifié. Le contrôle n'est pas conforme si aucun point de récupération n'a été créé dans le nombre de jours ou d'heures spécifié.

Ressource : `AWS Backup: recovery points`

Paramètres :

- Entrez le délai spécifié en nombres entiers, en heures ou en jours.
- Les valeurs hours peuvent être comprises entre 1 et 744.
- Les valeurs days peuvent être comprises entre 1 et 31.

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction:

- [Mettez à jour un plan de sauvegarde](#) pour modifier le délai spécifié pour la création du point de récupération.
- En outre, vous pouvez créer une sauvegarde à la demande.

Temps de restauration des ressources pour atteindre l'objectif

Description : évalue si la restauration des ressources protégées est terminée dans le délai de restauration cible.

Ce contrôle vérifie si le temps de restauration d'une ressource donnée correspond à la durée cible. La règle est NON_COMPLIANT si la LatestRestoreExecutionTimeMinutes du type de ressource est supérieure à maxRestoreTime exprimée en minutes.

Paramètres :

- maxRestoreTime (en minutes)

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées

- Ressources par type
- Ressource unique

 Note

AWS Backup ne fournit aucun accord de niveau de service (SLAs) pour une durée de restauration. Les temps de restauration peuvent varier en fonction de la charge et de la capacité du système, même pour les restaurations contenant les mêmes ressources.

Des ressources dans un coffre hermétique

Description : Ce contrôle évalue si les ressources ont au moins un point de récupération copié dans un coffre-fort logiquement espacé dans les limites de la valeur et du délai spécifiés. Ce contrôle est `NON_COMPLIED` si aucun point de récupération n'a été copié dans un coffre-fort logiquement espacé dans le délai configuré pour le contrôle.

Ressource : `AWS Backup: recovery points`

Paramètres :

- `recoveryPointAgeValue`
- `recoveryPointAgeUnit`

Entrez la période. Spécifiez l'unité dans `days` ou `hours`. Spécifiez une valeur pour cette unité. Les valeurs des heures peuvent être comprises entre 24 et 2184 inclusivement. Les valeurs des jours peuvent être comprises entre 1 et 91 inclusivement.

Une valeur minimale de 7 jours ou 168 d'heures est recommandée. La valeur de contrôle ne doit pas être plus fréquente que la fréquence de création de copies de votre plan de sauvegarde ; dans le cas contraire, vous risquez de voir un `NON_COMPLIANT` état inattendu jusqu'à ce que votre prochaine sauvegarde soit copiée dans un coffre-fort séparé de manière logique et que ce contrôle soit exécuté.

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources par type

- Ressource unique

Gestion AWS Backup des ressources entre plusieurs Comptes AWS

Note

Avant de gérer les ressources sur plusieurs Comptes AWS AWS Backup entrées, vos comptes doivent appartenir à la même organisation dans le AWS Organizations service.

Vue d'ensemble de la gestion entre comptes

Vous pouvez utiliser la fonctionnalité de gestion entre comptes AWS Backup pour gérer et surveiller vos tâches de sauvegarde, de restauration et de copie avec Comptes AWS AWS Organizations lesquelles vous les configurez. [AWS Organizations](#) est un service qui propose une gestion basée sur des règles pour plusieurs personnes Comptes AWS à partir d'un seul compte de gestion. Elle vous permet de standardiser la façon dont vous mettez en œuvre les stratégies de sauvegarde, en réduisant simultanément les erreurs et les efforts liés aux procédures manuelles. À partir d'une vue centralisée, vous pouvez facilement identifier les ressources dans tous les comptes qui répondent aux critères qui vous intéressent.

Si vous le configurez AWS Organizations, vous pouvez le configurer AWS Backup pour surveiller les activités de tous vos comptes en un seul endroit. Vous pouvez également créer une politique de sauvegarde et l'appliquer à certains comptes faisant partie de votre organisation et consulter les activités agrégées des tâches de sauvegarde directement depuis la AWS Backup console. Cette fonctionnalité permet aux administrateurs de sauvegarde de surveiller efficacement le statut des tâches de sauvegarde pour des centaines de comptes dans l'ensemble de leur entreprise à partir d'un seul compte principal. Les [Quotas AWS Organizations](#) s'appliquent.

Par exemple, vous définissez une stratégie de sauvegarde A qui prend les sauvegardes quotidiennes de ressources spécifiques et les conserve pendant 7 jours. Vous choisissez d'appliquer la stratégie de sauvegarde A à l'ensemble de l'organisation. (Ceci signifie que chaque compte de l'organisation bénéficie de cette politique de sauvegarde, ce qui crée un plan de sauvegarde correspondant visible dans ce compte.) Ensuite, vous créez une unité d'organisation nommée Finance et vous décidez de conserver ses sauvegardes pendant seulement 30 jours. Dans ce cas, vous définissez une stratégie de sauvegarde B, qui remplace la valeur du cycle de vie, et l'attachez à cette unité d'organisation Finance. Ceci signifie que tous les comptes de l'unité d'organisation Finance bénéficient d'un

nouveau plan de sauvegarde efficace qui prend les sauvegardes quotidiennes de toutes les ressources spécifiées et les conserve pendant 30 jours.

Dans cet exemple, la politique de sauvegarde A et la politique de sauvegarde B ont été fusionnées en une seule politique de sauvegarde, qui définit la politique de protection pour tous les comptes sous l'unité d'organisation nommée Finance. Tous les autres comptes de l'organisation restent protégés par la politique de sauvegarde A. La fusion est effectuée uniquement pour les politiques de sauvegarde qui partagent le même nom de plan de sauvegarde. Vous pouvez également faire coexister les stratégies A et B dans ce compte sans les fusionner. Vous pouvez utiliser des opérateurs de fusion avancés dans la vue JSON de la console uniquement. Pour plus d'informations sur la fusion des politiques, consultez [Définition des politiques, syntaxe des politiques et héritage de politique](#) dans le Guide de l'utilisateur AWS Organizations . Pour des références et des cas d'utilisation supplémentaires, consultez le blog [Gérer les sauvegardes à grande échelle dans le cadre de votre AWS Organizations utilisation AWS Backup](#) et le didacticiel vidéo [Gérer les sauvegardes à grande échelle dans le cadre de votre AWS Organizations utilisation AWS Backup](#).

La gestion entre comptes comprend la surveillance entre comptes, les sauvegardes entre comptes, les politiques de sauvegarde et les comptes administrateurs délégués. Tous ces éléments ne sont pas disponibles dans toutes les régions. Pour plus d'informations sur les domaines dans lesquels la gestion entre comptes est disponible, voir [Disponibilité des fonctionnalités par AWS région](#).

Pour utiliser la gestion entre comptes

1. Créez un compte de gestion AWS Organizations et ajoutez-y des comptes.
2. Activez la fonctionnalité de gestion entre comptes dans AWS Backup
3. Créez une politique de sauvegarde à appliquer à tous les utilisateurs Comptes AWS de votre compte de gestion.

 Note

Pour les plans de sauvegarde gérés par Organizations, les paramètres d'activation des ressources dans le compte de gestion remplacent les paramètres d'un compte membre, même si un ou plusieurs comptes d'administrateur délégué sont configurés. Les comptes d'administrateur délégué sont des comptes membres dotés de fonctionnalités améliorées et ne peuvent pas remplacer les paramètres comme le fait un compte de gestion.

4. Gérez les tâches de sauvegarde, de restauration et de copie dans tous vos Comptes AWS.

Création d'un compte de gestion dans Organizations

Tout d'abord, vous devez [créer votre organisation](#) et la configurer avec AWS les comptes des membres AWS Organizations. Pour obtenir des instructions, veuillez consulter [Didacticiel : Création et configuration d'une organisation](#) dans le Guide de l'utilisateur AWS Organizations .

Lorsque vous ajoutez des comptes membres à votre organisation, assurez-vous que chaque compte possède :

- Au moins un coffre-fort de sauvegarde and/or logiquement isolé
- Un rôle IAM

Les politiques de sauvegarde que vous créez comporteront un plan de sauvegarde, mais elles identifieront également le ou les coffres utilisés dans le plan de sauvegarde, les ressources qui seront sauvegardées et le rôle IAM qui sera utilisé pour créer la sauvegarde. Régions AWS Les politiques de sauvegarde qui font référence à des comptes ne disposant pas des informations requises ne fonctionneront pas comme prévu.

Pour plus d'informations, consultez [la section Syntaxe des politiques de sauvegarde](#) dans le Guide de AWS Organizations l'utilisateur.

Activation de la gestion entre comptes

Avant de pouvoir utiliser la gestion entre comptes dans AWS Backup, le compte de gestion doit activer cette fonctionnalité (c'est-à-dire l'activer). Une fois que le compte de gestion a activé la gestion entre comptes, vous pouvez créer des politiques de sauvegarde qui gèrent les ressources de plusieurs comptes.

Pour activer la gestion inter-comptes

1. Ouvrez le Console AWS Backup chat <https://console.aws.amazon.com/backup/>. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page de gestion inter-comptes.
3. Dans la section Stratégies de sauvegarde choisissez Activer.

Ceci vous donne accès à tous les comptes et vous permet de créer des stratégies qui automatisent la gestion de plusieurs comptes dans votre organisation simultanément.

4. Dans la section Surveillance inter-comptes choisissez Activer.

Ceci vous permet de surveiller les activités de sauvegarde, de copie et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.

Politiques de sauvegarde

Vous pouvez associer des plans de sauvegarde à l'évolutivité des [politiques AWS Organizations pour créer des politiques de sauvegarde](#) afin de simplifier la gestion au sein de votre organisation.

Consultez le guide de AWS Organizations l'utilisateur pour savoir comment activer les politiques de sauvegarde pour votre entreprise afin de pouvoir :

- [Création d'une politique de sauvegarde](#)
- [Mettre à jour une politique de sauvegarde](#) ; ou
- [Supprimer une politique de sauvegarde](#)
- [Syntaxe et exemples de politique de sauvegarde](#)

Voir [AWS Backup quotas](#) pour les quotas AWS Backup spécifiques sur les éléments contenus dans une politique.

Administrateur délégué

L'administration déléguée permet aux utilisateurs assignés à un compte membre enregistré d'effectuer la plupart des tâches AWS Backup administratives de manière pratique. Vous pouvez choisir de déléguer l'administration AWS Backup à un compte membre AWS Organizations, étendant ainsi la capacité de gestion AWS Backup depuis l'extérieur du compte de gestion et à l'ensemble de l'organisation.

Par défaut, un compte de gestion est le compte utilisé pour modifier et gérer les politiques. À l'aide de la fonctionnalité d'administrateur délégué, vous pouvez déléguer ces fonctions de gestion aux comptes membres que vous désignez. À leur tour, ces comptes peuvent gérer les politiques, en plus du compte de gestion.

Une fois qu'un compte membre a été enregistré pour l'administration déléguée, il devient un compte administrateur délégué. Notez que les comptes, et non les utilisateurs, sont désignés comme administrateurs délégués.

L'activation des comptes d'administrateur délégué permet de gérer les politiques de sauvegarde, de minimiser le nombre d'utilisateurs ayant accès au compte de gestion et de permettre le suivi des tâches entre comptes.

Le tableau ci-dessous présente les fonctions du compte de gestion, les comptes délégués en tant qu'administrateurs de Backup et les comptes membres de l' AWS organisation.

 Note

Les comptes d'administrateur délégué sont des comptes membres dotés de fonctionnalités améliorées, mais ne peuvent pas remplacer les paramètres d'activation du service d'autres comptes membres comme le fait un compte de gestion.

PRIVILÈGES	COMPTE DE GESTION	ADMINISTRATEUR DÉLÉGUÉ	COMPTE MEMBRE
Enregistrer/annuler l'enregistrement des comptes d'administrateurs délégués	Oui	Non	Non
Activez la gestion entre comptes	Oui	Non	Non
Gérez les politiques de sauvegarde entre les comptes dans AWS Organizations	Oui	Oui	Non
Surveiller les tâches entre comptes	Oui	Oui	Non

Conditions préalables

Avant de pouvoir déléguer l'administration des sauvegardes, vous devez d'abord enregistrer au moins un compte membre dans votre AWS organisation en tant qu'administrateur délégué. Avant de

pouvoir enregistrer un compte en tant qu'administrateur délégué, vous devez d'abord configurer les éléments suivants :

- [AWS Organizations doit être activé et configuré](#) avec au moins un compte membre en plus de votre compte de gestion par défaut.
- Il est recommandé que le rôle lié au service de AWS Backup sauvegarde (AWS Backup ServiceRoleForBackup) soit présent sur le compte de gestion de l'organisation afin de synchroniser automatiquement les autorisations d'administrateur déléguées avec les organisations. Cela garantit aux administrateurs délégués un accès approprié lorsque vous activez les régions optionnelles ou que vous modifiez l'affectation des administrateurs. Si le rôle lié au service de sauvegarde n'est pas présent ou a été supprimé, les clients ont plusieurs options pour le créer :
 - Enabling the Delegated Administrator feature.
 - Access the Backup Vaults Console page.
 - Manually create it following the documentation in [Création du rôle de service par défaut](#).
- Dans la AWS Backup console, assurez-vous que les politiques de sauvegarde, la surveillance entre comptes, la sauvegarde entre comptes et les fonctionnalités d'administration déléguée sont activées. Ils se trouvent sous le volet Administrateurs délégués de la AWS Backup console.
 - [La surveillance entre comptes](#) vous permet de surveiller les activités de sauvegarde sur tous les comptes de votre organisation à partir du compte de gestion, ainsi que des comptes d'administrateur délégué.
 - Facultatif : sauvegarde entre comptes, qui permet aux comptes de votre organisation de copier des sauvegardes vers d'autres comptes (pour les ressources multicomptes prises en charge par Backup).
 - Facultatif : administrateur délégué, qui permet à AWS Backup Backup de créer automatiquement le rôle lié au service de sauvegarde afin de synchroniser les autorisations d'administrateur déléguées avec les Organizations.
 - Activez [l'accès au service](#) avec AWS Backup.

Deux étapes sont impliquées dans la configuration de l'administration déléguée. La première étape consiste à déléguer le suivi des tâches entre comptes. La deuxième étape consiste à déléguer la gestion des politiques de sauvegarde.

Enregistrement d'un compte membre en tant que compte administrateur délégué

Voici la première section : Utilisation de la AWS Backup console pour enregistrer un compte d'administrateur délégué afin de surveiller les tâches entre comptes. Pour déléguer AWS Backup des politiques, vous allez utiliser la console Organizations dans la section suivante.

Pour enregistrer un compte membre à l'aide de la AWS Backup console :

1. Ouvrez le Console AWS Backup chat <https://console.aws.amazon.com/backup/>. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Sous Mon compte, dans le menu de navigation de gauche de la console, choisissez Paramètres.
3. Dans le volet Administrateur délégué, cliquez sur Enregistrer l'administrateur délégué ou Ajouter un administrateur délégué.
4. Sur la page Enregistrer l'administrateur délégué, sélectionnez le compte que vous souhaitez enregistrer, puis choisissez Enregistrer un compte.

Ce compte désigné sera désormais enregistré en tant qu'administrateur délégué, doté de privilèges administratifs lui permettant de surveiller les tâches entre les comptes de l'organisation et de consulter et de modifier les politiques (délégation de politiques). Ce compte membre ne peut pas enregistrer ou annuler l'enregistrement d'autres comptes administrateur délégué. Vous pouvez utiliser la console pour enregistrer jusqu'à 5 comptes en tant qu'administrateurs délégués.

Assurez-vous que l'administrateur délégué dispose des autorisations accordées par [the section called "AWSBackupOrganizationAdminAccess"](#).

Pour enregistrer un compte membre par programmation :

Utilisez la commande `register-delegated-administrator` de l'interface de ligne de commande. Vous pouvez spécifier les paramètres suivants dans votre demande d'interface de ligne de commande :

- `service-principal`
- `account-id`

Vous trouverez ci-dessous un exemple de demande d'interface de ligne de commande pour enregistrer un compte membre par programmation :

```
aws organizations register-delegated-administrator \  
--account-id 012345678912 \  
--service-principal "backup.amazonaws.com"
```

Annuler l'enregistrement d'un compte membre

Utilisez la procédure suivante pour supprimer l'accès administratif AWS Backup en annulant l'enregistrement d'un compte membre de votre AWS organisation qui avait été précédemment désigné comme administrateur délégué.

Pour annuler l'enregistrement d'un compte membre à l'aide de la console

1. Ouvrez le Console AWS Backup chat <https://console.aws.amazon.com/backup/>. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Sous Mon compte, dans le menu de navigation de gauche de la console, choisissez Paramètres.
3. Dans la section Administrateur délégué, cliquez sur Annuler l'enregistrement du compte.
4. Sélectionnez le compte ou les comptes dont vous voulez annuler l'enregistrement.
5. Dans la boîte de dialogue Annuler l'enregistrement du compte, examinez les implications en matière de sécurité, puis tapez `confirm` pour terminer l'annulation.
6. Sélectionnez `Deregister account`.

Pour annuler l'enregistrement d'un compte membre par programmation :

Utilisez la commande d'interface de ligne de commande `deregister-delegated-administrator` pour annuler l'inscription d'un compte administrateur délégué. Vous pouvez spécifier les paramètres suivants dans votre demande d'API :

- `service-principal`
- `account-id`

Vous trouverez ci-dessous un exemple de demande d'interface de ligne de commande pour annuler l'enregistrement d'un compte membre par programmation :

```
aws organizations deregister-delegated-administrator \  
--account-id 012345678912 \  
--service-principal "backup.amazonaws.com"
```

Déléguez AWS Backup les politiques via AWS Organizations

Dans la AWS Organizations console, vous pouvez déléguer l'administration de plusieurs politiques, y compris les politiques de Backup.

À partir du compte de gestion connecté à la [console AWS Organizations](#), vous pouvez créer, afficher ou supprimer une politique de délégation basée sur les ressources pour votre organisation. Pour connaître les étapes de délégation des politiques, consultez [Création d'une politique de délégation basée sur les ressources](#) dans le Guide de l'utilisateur AWS Organizations .

Surveillance des activités dans plusieurs Comptes AWS

Pour surveiller les tâches de sauvegarde, de copie et de restauration entre les comptes, vous devez activer la surveillance inter-comptes. Ceci vous permet de surveiller les activités de sauvegarde dans tous les comptes à partir du compte de gestion de votre organisation. Après votre inscription, toutes les tâches de votre organisation qui ont été créées après l'inscription sont visibles. Lorsque vous vous désinscrivez, AWS Backup conserve les tâches dans la vue agrégée pendant 30 jours (à partir de l'état Terminus). Les tâches créées après la désinscription ne sont pas visibles et n'affichent pas les tâches de sauvegarde nouvellement créées. Pour obtenir des instructions sur l'inscription, veuillez consulter [Activation de la gestion entre comptes](#).

Pour surveiller plusieurs comptes

1. Ouvrez le Console AWS Backup chat <https://console.aws.amazon.com/backup/>. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page de gestion inter-comptes.
3. Dans la section Surveillance inter-comptes choisissez Activer.

Ceci vous permet de surveiller les activités de sauvegarde et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.

4. Dans le volet de navigation de gauche, choisissez Surveillance inter-comptes.
5. Sur la page Surveillance inter-comptes, cliquez sur l'onglet Tâches de sauvegarde, Tâches de restauration ou Tâches de copie pour afficher toutes les tâches créées dans l'ensemble de vos comptes. Vous pouvez voir chacune de ces tâches par Compte AWS identifiant, et vous pouvez voir toutes les tâches d'un compte donné.

6. Dans la zone de recherche, vous pouvez filtrer les tâches par ID de compte, Statut ou ID de tâche.

Par exemple, vous pouvez cliquer sur l'onglet Tâches de sauvegarde et afficher toutes les tâches de sauvegarde créées dans l'ensemble de vos comptes. Vous pouvez filtrer la liste par ID de compte et afficher toutes les tâches de sauvegarde créées dans ce compte.

Règles d'activation des ressources

Si le plan de sauvegarde d'un compte membre a été créé par une politique de sauvegarde au niveau des organisations, les paramètres d' AWS Backup opt-in du compte de gestion des organisations remplaceront les paramètres d'opt-in de ce compte membre, mais uniquement pour ce plan de sauvegarde.

Si le compte membre dispose également de plans de sauvegarde locaux créés par les utilisateurs, ces plans de sauvegarde suivront les paramètres d'acceptation du compte membre, sans référence aux paramètres d'activation du compte de gestion Organizations.

Définition des politiques, syntaxe des politiques et héritage de politique

Les sujets suivants sont documentés dans le guide de AWS Organizations l'utilisateur.

- Stratégies de sauvegarde : consultez [Stratégies de sauvegarde](#).
- Syntaxe d'une politique : consultez [Syntaxe et exemples d'une stratégie de balise](#).
- Héritage pour les types de politique de gestion : consultez [Héritage pour les types de politique de gestion](#).

AWS Backup et CloudFormation

En général

Vous pouvez ainsi approvisionner et gérer vos AWS ressources de manière sûre et reproductible à l'aide de modèles que vous créez. CloudFormation Vous pouvez utiliser des CloudFormation modèles et StackSets gérer vos plans de sauvegarde, vos sélections de ressources de sauvegarde et vos coffres-forts de sauvegarde. Pour plus d'informations sur CloudFormation, consultez [Fonctionnement d' CloudFormation](#) dans Guide de l'utilisateur AWS CloudFormation .

Avant de créer votre CloudFormation modèle StackSet, tenez compte des points suivants :

- Créez des modèles distincts pour vos plans de sauvegarde et vos coffres-forts de sauvegarde. Vous ne pouvez supprimer que des coffres-forts de sauvegarde vides. Vous ne pouvez pas supprimer une pile qui inclut des coffres-forts de sauvegarde s'ils contiennent des points de récupération.
- Vérifiez que vous disposez d'une fonction du service disponible avant de créer votre pile. Le rôle de service AWS Backup par défaut est créé pour vous la première fois que vous affectez des ressources à un plan de sauvegarde. Si vous n'avez pas attribué de ressources à votre plan de sauvegarde, faites-le avant de créer votre pile. Vous pouvez également spécifier un rôle personnalisé que vous créez. Pour plus d'informations sur les rôles , consultez [Fonctions du service IAM](#).

Déploiement d'un coffre de sauvegarde, d'un plan de sauvegarde et d'attribution de ressources à l'aide de CloudFormation

Pour un exemple de CloudFormation modèle qui déploie un coffre de sauvegarde, des plans de sauvegarde et une attribution de ressources, consultez [Attribuez AWS Backup des ressources via CloudFormation](#).

Déploiement de plans de sauvegarde en utilisant CloudFormation

Pour des exemples CloudFormation de modèles qui déploient des plans de sauvegarde, consultez [the section called “CloudFormation modèles de plans de sauvegarde”](#).

Déploiement AWS Backup des frameworks Audit Manager et des plans de rapports à l'aide de CloudFormation

Pour des exemples CloudFormation de modèles qui déploient les frameworks AWS Backup Audit Manager et les plans de rapports, consultez [the section called “Utilisation CloudFormation pour déployer les ressources AWS Backup d'Audit Manager”](#).

Déploiement de plans de sauvegarde entre comptes à l'aide de CloudFormation

Vous pouvez [l'utiliser AWS CloudFormation StackSets sur plusieurs comptes au sein d'une AWS organisation](#). Des exemples de modèles sont disponibles dans le [Guide de l'utilisateur CloudFormation](#).

La publication [Automatiser la sauvegarde centralisée à grande échelle pour tous les AWS services utilisateurs constitue un excellent point de départ et une excellente](#) référence AWS Backup. Avec Ibukun Oyewumi et Sabith Venkitachalapathy (juillet 2021).

En savoir plus sur CloudFormation

Pour plus d'informations sur l'utilisation CloudFormation avec AWS Backup, reportez-vous à la section [Référence AWS Backup des types de ressources](#) dans le guide de AWS CloudFormation l'utilisateur.

Pour plus d'informations sur le contrôle de l'accès aux ressources du AWS service lors de l'utilisation CloudFormation, consultez la section [Contrôler l'accès avec Gestion des identités et des accès AWS](#) dans le guide de AWS CloudFormation l'utilisateur.

AWS Backup réseau

AWS Backup points de terminaison

AWS Backup propose des points de terminaison publics et privés pour répondre à vos besoins de connectivité. Pour ces points de terminaison, AWS Backup prend en charge les protocoles Internet version 4 (IPv4) et version 6 (IPv6) pour les types de ressources compatibles IPv6.

Le nouveau point de terminaison public backup . *[Region]* . api . aws possède des fonctionnalités de double pile et peut résoudre l'un ou les deux IPv4 points de terminaison. IPv6 Lorsque vous envoyez une demande à un point de terminaison d' AWS Backup API à double pile, le point de terminaison est résolu à l'adresse déterminée par la configuration du protocole utilisé par votre réseau et votre client.

L'ancien point de terminaison ne backup . *[Region]* . amazonaws . com peut être utilisé que pour les appels faisant référence IPv4.

Vous pouvez consulter les [points de terminaison du service public AWS Backup](#) dans le Référence générale d'Amazon Web Services. Vous pouvez consulter les étapes de configuration de points de terminaison privés [AWS Backup via VPC](#).

AWS Backup via des points de terminaison VPC

Vous pouvez établir une connexion privée entre votre cloud privé virtuel (VPC) et en AWS Backup créant un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par [AWS PrivateLink](#) une technologie qui vous permet d'accéder à l' AWS Backup API sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de Direct Connect connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les points de terminaison de AWS Backup l'API. Vos instances n'ont pas non plus besoin d'adresses IP publiques pour utiliser les opérations d' AWS Backup API et d'API Backup Gateway disponibles.

Pour plus d'informations, consultez la section [Accès aux AWS services AWS PrivateLink](#) dans le AWS PrivateLink Guide.

Considérations relatives aux points de terminaison d'un VPC Amazon

Toutes les AWS Backup opérations relatives à la gestion de vos ressources sont disponibles depuis votre VPC à l'aide de. AWS PrivateLink

Les politiques de point de terminaison d'un VPC sont prises en charge pour les points de terminaison de Backup. Par défaut, l'accès complet aux opérations de Backup est autorisé via le point de terminaison. Vous pouvez également associer un groupe de sécurité aux interfaces réseau du point de terminaison pour contrôler le trafic AWS Backup passant par le point de terminaison de l'interface.

Vous pouvez sélectionner IPv4 ou effectuer une double pile lors de la création d'un point de terminaison. IPv6 Vous recevrez les mêmes noms DNS (qui comporteront à la fois des IPv6 adresses IPv4 et des adresses si vous sélectionnez Dual Stack).

AWS Backup pour SAP HANA n'est pas pris en charge AWS PrivateLink. Les sauvegardes SAP HANA sont activées par le Agent AWS Backint, qui ne prend pas en charge les points de terminaison VPC ; il envoie des données de sauvegarde au point de terminaison de stockage pour. AWS Backup

Création d'un point de AWS Backup terminaison VPC

Vous pouvez créer un point de terminaison VPC à AWS Backup l'aide de la console Amazon VPC ou de la (AWS Command Line Interface CLI).AWS Pour plus d'informations, consultez [Création d'un point de terminaison d'interface](#) dans le Guide AWS PrivateLink .

PrivateLink les points de terminaison utilisent la même structure de noms IPv4, bien que chaque point de terminaison puisse être configuré pour IPv4 IPv6, ou pour une double pile.

Créez un point de terminaison VPC pour AWS Backup utiliser le nom du service.
`com.amazonaws.region.backup`

Dans les régions Chine (Beijing) et Chine (Ningxia), le nom du service doit être
`cn.com.amazonaws.region.backup`.

Pour les points de terminaison Backup gateway, utilisez `com.amazonaws.region.backup-gateway`.

Les ports TCP suivants doivent être autorisés dans le groupe de sécurité lors de la création d'un point de terminaison d'un VPC pour Backup gateway :

- TCP 443
- TCP 1026

- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protocole	Port	Direction	Source	Destination	Usage
TCP	443 (HTTPS)	Sortant	Backup Gateway	AWS	Pour les communications entre Backup Gateway et le point de terminaison du AWS service

Utiliser un point de terminaison VPC

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API AWS Backup au point de terminaison VPC en utilisant son nom DNS par défaut pour la AWS région, par exemple. `backup.us-east-1.api.aws`

Toutefois, pour les régions de Chine (Pékin) et de Chine (Ningxia) Régions AWS, les demandes d'API doivent être effectuées avec le point de terminaison VPC à l'`backup.cn-north-1.amazonaws.com.cn` et `backup.cn-northwest-1.amazonaws.com.cn` et, respectivement.

Création d'une stratégie de point de terminaison de VPC

Vous pouvez attacher une politique de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à l'API Amazon Backup. La politique spécifie :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

⚠ Important

Lorsqu'une politique autre que celle par défaut est appliquée à un point de terminaison VPC d'interface AWS Backup pour, certaines demandes d'API ayant échoué, telles que celles `RequestLimitExceeded` émanant de, peuvent ne pas être enregistrées sur Amazon AWS CloudTrail ou sur Amazon. CloudWatch

Pour plus d'informations, consultez [Contrôle de l'accès aux services à l'aide de politiques de point de terminaison](#) dans le Guide AWS PrivateLink .

Exemple : politique de point de terminaison VPC pour les actions AWS Backup

Voici un exemple de politique de point de terminaison pour AWS Backup. Lorsqu'elle est attachée à un point de terminaison, cette politique donne accès aux AWS Backup actions répertoriées pour tous les principes sur toutes les ressources.

```
{
  "Statement": [
    {
      "Action": "backup:*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Exemple : politique de point de terminaison d'un VPC qui refuse tout accès à partir d'un compte AWS spécifié

La politique de point de terminaison VPC suivante refuse au AWS compte 123456789012 tout accès aux ressources utilisant le point de terminaison. La politique autorise toutes les actions provenant d'autres comptes.

JSON

```
{
  "Id": "Policy1645236617225",
  "Version": "2012-10-17",
```

```
"Statement":[
  {
    "Sid":"Stmt1645236612384",
    "Action":"backup:*",
    "Effect":"Deny",
    "Resource":"*",
    "Principal":{"
      "AWS":[
        "123456789012"
      ]
    }
  }
]
```

Pour plus d'informations sur les réponses d'API disponibles, consultez le [guide des API](#).

Sécurité dans AWS Backup

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des [programmes de conformité AWS](#). Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Backup, consultez la section [AWS Services concernés par programme de conformité](#).
- Sécurité dans le cloud : votre responsabilité pour AWS Backup inclut, sans toutefois s'y limiter, les éléments suivants. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.
 - Répondre aux communications que vous recevez de AWS.
 - Gestion des informations d'identification que vous et votre équipe utilisez. Pour plus d'informations, consultez la section [Gestion des identités et des accès dans AWS Backup](#).
 - Configuration de vos plans de sauvegarde et attributions de ressources pour refléter les politiques de protection des données de votre organisation. Pour plus d'informations, consultez [Gestion des plans de sauvegarde](#).
 - Tester régulièrement votre capacité à trouver certains points de récupération et à les restaurer. Pour plus d'informations, consultez la page [Utilisation des sauvegardes](#).
 - Intégrer AWS Backup des procédures dans les procédures écrites de reprise après sinistre et de continuité des activités de votre organisation. Pour un point de départ, consultez [Mise en route avec AWS Backup](#).
 - Assurez-vous que vos employés connaissent et se sont entraînés à utiliser AWS Backup les procédures de votre organisation en cas d'urgence. Pour plus d'informations, consultez le [Cadre AWS Well-Architected](#).

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Backup. Les rubriques suivantes expliquent comment procéder

à la configuration AWS Backup pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Backup ressources.

Rubriques

- [Validation de conformité pour AWS Backup](#)
- [Protection des données dans AWS Backup](#)
- [Gestion des identités et des accès dans AWS Backup](#)
- [Sécurité de l'infrastructure dans AWS Backup](#)
- [Intégrité des données dans AWS Backup](#)
- [Retenues légales et AWS Backup](#)
- [Protection contre les logiciels malveillants dans AWS Backup](#)
- [Résilience dans AWS Backup](#)

Validation de conformité pour AWS Backup

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez [AWS la documentation de sécurité](#).

Protection des données dans AWS Backup

AWS Backup est conforme au [modèle de responsabilité AWS partagée](#), qui inclut des réglementations et des directives pour la protection des données. AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS services. AWS conserve le contrôle des données hébergées sur cette infrastructure, y compris les contrôles de configuration de sécurité pour le

traitement du contenu client et des données personnelles. AWS les clients et les AWS partenaires du réseau de partenaires (APN), agissant en tant que responsables du traitement des données ou en tant que sous-traitants, sont responsables de toutes les données personnelles qu'ils saisissent dans le AWS Cloud.

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes utilisateur individuels avec Gestion des identités et des accès AWS (IAM). Cela permet de garantir que chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour les besoins de ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) pour communiquer avec les ressources AWS .
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.

Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Nom. Cela inclut lorsque vous travaillez avec AWS Backup ou avec d'autres AWS services à l'aide de la console AWS CLI, de l'API ou AWS SDKs. Toutes les données que vous entrez dans AWS Backup ou d'autres services peuvent être récupérées pour être insérées dans des journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Pour en savoir plus sur la protection des données, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD](#) sur le Blog sur la sécurité d'AWS .

Chiffrement pour les sauvegardes dans AWS Backup

Chiffrement indépendant

AWS Backup propose un chiffrement indépendant pour les [types de ressources qui prennent en charge AWS Backup la gestion complète](#). Le chiffrement indépendant signifie que les points de restauration (sauvegardes) que vous créez AWS Backup peuvent avoir une méthode de chiffrement autre que celle déterminée par le chiffrement de la ressource source. Par exemple, votre sauvegarde d'un compartiment Amazon S3 peut utiliser une méthode de chiffrement différente de celle du

compartiment source que vous avez chiffré avec le chiffrement Amazon S3. Ce chiffrement est contrôlé par le biais de la configuration des AWS KMS clés dans le coffre de sauvegarde dans lequel votre sauvegarde est stockée.

Les sauvegardes de types de ressources qui ne sont pas entièrement gérés par héritent AWS Backup généralement des paramètres de chiffrement de leur ressource source. Vous pouvez configurer ces paramètres de chiffrement conformément aux instructions de ce service, telles que le [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Votre rôle IAM doit avoir accès à la clé KMS utilisée pour sauvegarder et restaurer l'objet. Dans le cas contraire, la tâche est réussie mais les objets ne sont ni sauvegardés ni restaurés. Les autorisations de la politique IAM et de la politique des clés KMS doivent être cohérentes. Pour plus d'informations, consultez la section [Spécification des clés KMS dans les déclarations de politique IAM](#) du Guide du AWS Key Management Service développeur.

Le tableau suivant répertorie chaque type de ressource pris en charge. Il indique également la façon dont le chiffrement est configuré pour les sauvegardes et si un chiffrement indépendant est pris en charge pour les sauvegardes. Lorsqu' AWS Backup chiffre une sauvegarde de manière indépendante, il utilise l'algorithme de chiffrement AES-256 standard. Pour plus d'informations sur le chiffrement dans AWS Backup, consultez [la section Sauvegarde entre régions](#) et [entre comptes](#).

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Simple Storage Service (Amazon S3)	Les sauvegardes Amazon S3 sont chiffrées à l'aide d'une clé AWS KMS (AWS Key Management Service) associée au coffre de sauvegarde. La clé AWS KMS peut être une clé gérée par le client ou une clé AWS gérée associée au service. AWS Backup chiffre toutes les sauvegardes même si les compartiments Amazon S3 source ne sont pas chiffrés.	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
VMware machines virtuelles	Les sauvegardes de machines virtuelles sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes de machines virtuelles est configurée dans le AWS Backup coffre dans lequel les sauvegardes de machines virtuelles sont stockées.	Pris en charge
Amazon DynamoDB après avoir activé Sauvegarde DynamoDB avancée	Les sauvegardes DynamoDB sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes DynamoDB est configurée dans AWS Backup le coffre dans lequel les sauvegardes DynamoDB sont stockées.	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon DynamoDB sans avoir activé Sauvegarde DynamoDB avancée	Les sauvegardes DynamoDB sont automatiquement chiffrées avec la même clé de chiffrement que celle utilisée pour chiffrer la table DynamoDB source. Les instantanés de tables DynamoDB non chiffrés ne sont pas chiffrés non plus. AWS Backup Pour créer une sauvegarde d'une table DynamoDB chiffrée, vous devez ajouter les <code>kms:Decrypt</code> autorisations <code>kms:GenerateDataKey</code> et le rôle IAM utilisé pour la sauvegarde. Vous pouvez également utiliser le rôle de service AWS Backup par défaut.	Non pris en charge
Amazon Elastic File System (Amazon EFS)	Les sauvegardes Amazon EFS sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes Amazon EFS est configurée dans le AWS Backup coffre dans lequel les sauvegardes Amazon EFS sont stockées.	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Elastic Block Store (Amazon EBS)	Par défaut, les sauvegardes Amazon EBS sont soit chiffrées à l'aide de la clé utilisée pour chiffrer le volume source, soit elles ne sont pas chiffrées. Pendant la restauration, vous pouvez choisir de remplacer la méthode de chiffrement par défaut en spécifiant une clé KMS.	Non pris en charge
Amazon Elastic Compute Cloud (Amazon EC2) AMIs	AMIs ne sont pas chiffrés. Les instantanés EBS sont chiffrés selon les règles de chiffrement par défaut pour les sauvegardes EBS (voir l'entrée relative à EBS). Les instantanés EBS des données et des volumes racines peuvent être chiffrés et attachés à une AMI.	Non pris en charge
Amazon Relational Database Service (Amazon RDS)	Les instantanés Amazon RDS sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer la base de données Amazon RDS source. Les instantanés de bases de données Amazon RDS non chiffrés ne sont pas chiffrés non plus.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Aurora	Les instantanés de cluster Aurora sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Amazon Aurora source. Les instantanés de clusters Aurora non chiffrés ne sont pas chiffrés.	Non pris en charge
AWS Storage Gateway	Les instantanés Storage Gateway sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le volume Storage Gateway source. Les instantanés de volumes Storage Gateway non chiffrés ne sont pas chiffrés non plus. Vous n'avez pas besoin d'utiliser une clé gérée par le client pour tous les services pour activer Storage Gateway. Il vous suffit de copier la sauvegarde Storage Gateway dans un coffre-fort qui a configuré une clé KMS. Cela est dû au fait que Storage Gateway ne possède pas de clé AWS KMS gérée spécifique au service.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon FSx	Les fonctionnalités de chiffrement des systèmes de FSx fichiers Amazon varient en fonction du système de fichiers sous-jacent. Pour en savoir plus sur votre système de FSx fichiers Amazon en particulier, consultez le guide de FSx l'utilisateur approprié.	Non pris en charge
Amazon DocumentDB	Les instantanés de cluster Amazon DocumentDB sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Amazon DocumentDB source. Les instantanés de clusters Amazon DocumentDB non chiffrés ne sont pas chiffrés.	Non pris en charge
Amazon Neptune	Les instantanés de cluster Neptune sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Neptune source. Les instantanés de clusters Neptune non chiffrés ne sont pas chiffrés.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Timestream	Les sauvegardes d'instantanés de la table Timestream sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes Timestream est configurée dans le coffre de sauvegarde dans lequel les sauvegardes Timestream sont stockées.	Pris en charge
Amazon Redshift	Les clusters Amazon Redshift sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Amazon Redshift source. Les instantanés de clusters Amazon Redshift non chiffrés ne sont pas chiffrés.	Non pris en charge
Amazon Redshift sans serveur	Les instantanés Redshift Serverless sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer la source.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
CloudFormation	CloudFormation les sauvegardes sont toujours cryptées. La clé de CloudFormation chiffrement pour les CloudFormation sauvegardes est configurée dans le CloudFormation coffre dans lequel les CloudFormation sauvegardes sont stockées.	Pris en charge
Bases de données SAP HANA sur les instances Amazon EC2	Les sauvegardes de base de données SAP HANA sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes de base de données SAP HANA est configurée dans le AWS Backup coffre dans lequel les sauvegardes de base de données sont stockées.	Pris en charge

 Tip

[AWS Backup Audit Manager](#) vous aide à détecter automatiquement les sauvegardes non chiffrées.

Chiffrement des copies d'une sauvegarde sur un autre compte ou Région AWS

Lorsque vous copiez vos sauvegardes entre comptes ou régions, les copies sont AWS Backup automatiquement chiffrées pour la plupart des types de ressources, même si la sauvegarde d'origine n'est pas chiffrée. AWS Backup chiffre la copie à l'aide de la clé KMS du coffre cible.

Avant de copier une sauvegarde d'un compte vers un autre (tâche de copie entre comptes) ou de copier une sauvegarde d'une région à une autre (tâche de copie interrégionale), tenez compte des conditions suivantes, dont la plupart dépendent du fait que le type de ressource de la sauvegarde (point de restauration) est [entièrement géré par AWS Backup ou non entièrement géré](#).

- Une copie d'une sauvegarde vers une autre Région AWS est chiffrée à l'aide de la clé du coffre de destination.
- Pour obtenir une copie d'un point de restauration (sauvegarde) d'une ressource entièrement gérée par AWS Backup, vous pouvez choisir de la chiffrer à l'aide d'une [clé gérée par le client \(CMK\)](#) ou d'une clé AWS Backup gérée (aws/backup).

Pour une copie d'un point de restauration d'une ressource qui n'est pas entièrement gérée par AWS Backup, la clé associée au coffre de destination doit être une clé CMK ou la clé gérée du service propriétaire de la ressource sous-jacente. Par exemple, si vous copiez une EC2 instance, une clé gérée Backup ne peut pas être utilisée. Au lieu de cela, une clé CMK ou Amazon EBS KMS (aws/ebs) doit être utilisée pour éviter l'échec de la tâche de copie.

- La copie entre comptes avec clés AWS gérées n'est pas prise en charge pour les ressources qui ne sont pas entièrement gérées par AWS Backup. La [politique clé](#) d'une clé AWS gérée est immuable, ce qui empêche de copier la clé d'un compte à un autre. Si vos ressources sont chiffrées à l'aide de clés AWS gérées et que vous souhaitez effectuer une copie entre comptes, vous pouvez [remplacer les clés de chiffrement](#) par une clé gérée par le client, qui peut être utilisée pour la copie entre comptes. Vous pouvez également suivre les instructions de la [section Protection des instances Amazon RDS chiffrées avec des sauvegardes entre comptes et entre régions](#) pour continuer à utiliser AWS des clés gérées.
- Les copies des clusters Amazon Aurora, Amazon DocumentDB et Amazon Neptune non chiffrés sont également déchiffrées.

AWS Backup autorisations, autorisations et déclarations de refus

Pour éviter l'échec des tâches, vous pouvez examiner la politique AWS KMS clé pour vous assurer qu'elle dispose des autorisations requises et qu'elle ne contient aucune déclaration de refus empêchant le succès des opérations.

Les tâches échouées peuvent se produire en raison d'une ou de plusieurs instructions Deny appliquées à la clé KMS ou en raison d'une [autorisation](#) révoquée pour la clé.

Dans une politique d'accès AWS gérée telle que [AWSBackupFullAccess](#), certaines actions Autoriser permettent de créer une interface AWS Backup AWS KMS pour créer une autorisation sur une clé KMS au nom d'un client dans le cadre des opérations de sauvegarde, de copie et de stockage.

La politique clé nécessite au minimum les autorisations suivantes :

- kms:createGrant
- kms:generateDataKey
- kms:decrypt

Si des politiques de refus sont nécessaires, vous devrez autoriser la liste des rôles requis pour les opérations de sauvegarde et de restauration.

Ces éléments peuvent ressembler à :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "KmsPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
      },
      "Action": [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Sid": "KmsCreateGrantPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/root"
      },
      "Action": [
```

```

        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "kms:EncryptionContextKeys": "aws:backup:backup-vault"
        },
        "Bool": {
            "kms:GrantIsForAWSResource": true
        },
        "StringLike": {
            "kms:ViaService": "backup.*.amazonaws.com"
        }
    }
}
]
}

```

Ces autorisations doivent faire partie de la clé, qu'elles soient AWS gérées ou gérées par le client.

1. Assurez-vous que les autorisations requises font partie de la politique clé de KMS
 - a. Exécutez KMS CLI `get-key-policy` ([kms:GetKeyPolicy](#)) pour afficher la politique de clé attachée à la clé KMS spécifiée.
 - b. Vérifiez les autorisations renvoyées.
2. Assurez-vous qu'aucune instruction Deny n'affecte les opérations
 - a. Exécutez (ou réexécutez) CLI `get-key-policy` ([kms:GetKeyPolicy](#)) pour afficher la politique de clé attachée à la clé KMS spécifiée.
 - b. Passez en revue la politique.
 - c. Supprimez les instructions Deny pertinentes de la politique de clé KMS.
3. Si nécessaire, exécutez [kms:put-key-policy](#) pour remplacer ou mettre à jour la politique clé avec des autorisations révisées et des instructions Deny supprimées.

En outre, la clé associée au rôle à l'origine d'une tâche de copie interrégionale doit figurer `"kms:ResourcesAliases": "alias/aws/backup"` dans l'`DescribeKey` autorisation.

Chiffrement des informations d'identification de l'hyperviseur de machine virtuelle

Les machines virtuelles [gérées par un hyperviseur](#) utilisent [AWS Backup Gateway](#) pour connecter les systèmes sur site à AWS Backup. Il est important que les hyperviseurs disposent de la même sécurité robuste et fiable. Cette sécurité peut être atteinte en chiffrant l'hyperviseur, soit à l'aide de clés AWS détenues, soit à l'aide de clés gérées par le client.

AWS clés détenues et gérées par le client

AWS Backup fournit le chiffrement des informations d'identification de l'hyperviseur afin de protéger les informations de connexion sensibles des clients à l'aide de clés de chiffrement AWS détenues. Vous avez la possibilité d'utiliser des clés gérées par le client à la place.

Par défaut, les clés utilisées pour chiffrer les informations d'identification dans votre hyperviseur sont des clés AWS détenues. AWS Backup utilise ces clés pour chiffrer automatiquement les informations d'identification de l'hyperviseur. Vous ne pouvez ni consulter, ni gérer, ni utiliser AWS les clés que vous possédez, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section sur les clés AWS détenues dans le [Guide du AWS KMS développeur](#).

Les informations d'identification peuvent également être chiffrées à l'aide de clés gérées par le client. AWS Backup prend en charge l'utilisation de clés symétriques gérées par le client que vous créez, possédez et gérez pour effectuer votre chiffrement. Étant donné que vous avez le contrôle total de ce chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établissement et gestion des politiques IAM et des octrois
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Lorsque vous utilisez une clé gérée par le client, AWS Backup vérifie si votre rôle est autorisé à déchiffrer à l'aide de cette clé (avant l'exécution d'une tâche de sauvegarde ou de restauration). Vous

devez ajouter l'action kms : Decrypt au rôle utilisé pour démarrer une tâche de sauvegarde ou de restauration.

Comme l'action kms : Decrypt ne peut pas être ajoutée au rôle de sauvegarde par défaut, vous devez utiliser un rôle autre que le rôle de sauvegarde par défaut pour utiliser les clés gérées par le client.

Pour plus d'informations, consultez [Clés gérées par le client](#) dans le Manuel du développeur AWS Key Management Service .

Octroi requis lors de l'utilisation des clés gérées par le client

AWS KMS nécessite une [autorisation](#) pour utiliser votre clé gérée par le client. Lorsque vous importez une [configuration d'hyperviseur](#) chiffrée à l'aide d'une clé gérée par le client, AWS Backup vous créez une autorisation en votre nom en envoyant une [CreateGrant](#) demande à AWS KMS. AWS Backup utilise des autorisations pour accéder à une clé KMS dans un compte client.

Vous pouvez révoquer l'accès à l'autorisation ou supprimer AWS Backup l'accès à la clé gérée par le client à tout moment. Dans ce cas, toutes les passerelles associées à votre hyperviseur ne pourront plus accéder au nom d'utilisateur et au mot de passe de l'hyperviseur chiffrés par la clé gérée par le client, ce qui affectera vos tâches de sauvegarde et de restauration. Plus précisément, les tâches de sauvegarde et de restauration que vous effectuez sur les machines virtuelles de cet hyperviseur échoueront.

Backup gateway utilise cette opération `RetireGrant` pour supprimer un octroi lorsque vous supprimez un hyperviseur.

Surveillance des clés de chiffrement

Lorsque vous utilisez une clé gérée par le AWS KMS client avec vos AWS Backup ressources, vous pouvez utiliser [AWS CloudTrailAmazon CloudWatch Logs](#) pour suivre les demandes AWS Backup envoyées à AWS KMS.

Recherchez les AWS CloudTrail événements contenant les "eventName" champs suivants pour surveiller les AWS KMS opérations appelées pour accéder AWS Backup aux données chiffrées par votre clé gérée par le client :

- "eventName": "CreateGrant"
- "eventName": "Decrypt"

- "eventName": "Encrypt"
- "eventName": "DescribeKey"

Gestion des identités et des accès dans AWS Backup

L'accès à AWS Backup nécessite des informations d'identification. Ces informations d'identification doivent être autorisées à accéder aux ressources AWS , par exemple une base de données Amazon DynamoDB ou un système de fichiers Amazon EFS. De plus, les points de récupération créés par AWS Backup certains services AWS Backup pris en charge ne peuvent pas être supprimés à l'aide du service source (tel qu'Amazon EFS). Vous pouvez supprimer ces points de récupération à l'aide de AWS Backup.

Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser [Gestion des identités et des accès AWS \(IAM\)](#) et AWS Backup pour sécuriser l'accès à vos ressources.

Warning

AWS Backup utilise le même rôle IAM que celui que vous avez choisi lors de l'attribution des ressources pour gérer le cycle de vie de votre point de restauration. Si vous supprimez ou modifiez ce rôle, vous AWS Backup ne pouvez pas gérer le cycle de vie de votre point de restauration. Dans ce cas, il tentera d'utiliser un rôle lié à un service pour gérer votre cycle de vie. Dans un faible pourcentage de cas, cela peut également ne pas fonctionner, laissant des points de récupération EXPIRED sur votre stockage, ce qui peut entraîner des coûts indésirables. Pour supprimer des points de récupération EXPIRED, supprimez-les manuellement à l'aide de la procédure décrite dans [Suppression des sauvegardes](#).

Rubriques

- [Authentification](#)
- [Contrôle d'accès](#)
- [Fonctions du service IAM](#)
- [Politiques gérées pour AWS Backup](#)
- [Utilisation des rôles liés à un service pour AWS Backup](#)
- [Prévention du cas de figure de l'adjoint désorienté entre services](#)

Authentification

L'accès aux services que vous sauvegardez AWS Backup ou AWS aux services que vous sauvegardez nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Vous pouvez y accéder AWS sous l'un des types d'identités suivants :

- **Compte AWS utilisateur root** — Lorsque vous vous inscrivez AWS, vous fournissez une adresse e-mail et un mot de passe associés à votre AWS compte. Il s'agit de votre utilisateur root du Compte AWS . Ses informations d'identification fournissent un accès complet à toutes vos AWS ressources.

Important

Pour des raisons de sécurité, nous vous conseillons d'utiliser les informations d'utilisateur racine uniquement pour créer un administrateur. L'administrateur est un utilisateur IAM disposant des autorisations complètes sur votre Compte AWS. Vous pouvez ensuite utiliser cet utilisateur administrateur pour créer d'autres rôles et utilisateurs IAM dotés d'autorisations limitées. Pour plus d'informations, consultez [Bonnes pratiques IAM](#) et [Création de votre premier utilisateur administrateur et groupe IAM](#) dans le Guide de l'utilisateur IAM.

- **Utilisateur IAM** : un [utilisateur IAM](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations personnalisées spécifiques (par exemple, des autorisations pour créer un coffre-fort de sauvegarde dans lequel stocker vos sauvegardes). [Vous pouvez utiliser un nom d'utilisateur et un mot de passe IAM pour vous connecter à des AWS pages Web sécurisées telles que AWS Management Console les forums de AWS discussion ou le AWS Support centre.](#)

En plus de générer un nom utilisateur et un mot de passe, vous pouvez générer des [clés d'accès](#) pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux AWS services par programmation, soit par le biais [de l'une des nombreuses SDKs clés, soit à l'aide de la AWS Command Line Interface \(AWS CLI\)](#). Les outils AWS CLI et les SDK utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas les outils AWS , vous devez signer la demande vous-même. Pour plus d'informations sur l'authentification des demandes, consultez [Processus de signature Signature Version 4](#) dans le document Références générales AWS.

- **Rôle IAM** : un [rôle IAM](#) est une autre identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'un utilisateur IAM, mais ce rôle n'est pas associé à une personne en particulier. Un rôle IAM vous permet d'obtenir des clés

d'accès temporaires qui peuvent être utilisées pour accéder aux AWS services et aux ressources. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités utilisateur préexistantes provenant de Directory Service l'annuaire des utilisateurs de votre entreprise ou d'un fournisseur d'identité Web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un [fournisseur d'identité](#). Pour plus d'informations sur les utilisateurs fédérés, consultez [Utilisateurs fédérés et rôles](#) dans le Guide de l'utilisateur IAM.
- Administration entre comptes : vous pouvez utiliser un rôle IAM dans votre compte pour accorder d'autres Compte AWS autorisations afin d'administrer les ressources de votre compte. À titre d'exemple, voir [Tutoriel : accès délégué à Comptes AWS l'aide de rôles IAM](#) dans le guide de l'utilisateur IAM.
- AWS accès au service : vous pouvez utiliser un rôle IAM dans votre compte pour accorder à un AWS service l'autorisation d'accéder aux ressources de votre compte. Pour plus d'informations, consultez la section [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le guide de l'utilisateur IAM.
- Applications exécutées sur Amazon Elastic Compute Cloud (Amazon EC2) : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires des applications exécutées sur une EC2 instance Amazon et effectuant des demandes d' AWS API. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le guide de l'utilisateur IAM.

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais si vous ne disposez pas des autorisations appropriées, vous ne pouvez pas accéder aux AWS Backup ressources telles que les coffres-forts de sauvegarde. Vous ne pouvez pas non plus sauvegarder AWS des ressources telles que les volumes Amazon Elastic Block Store (Amazon EBS).

Chaque AWS ressource appartient à un Compte AWS, et les autorisations de création ou d'accès à une ressource sont régies par des politiques d'autorisation. Un administrateur de compte peut

associer des politiques d'autorisation aux identités Gestion des identités et des accès AWS (IAM) (c'est-à-dire aux utilisateurs, aux groupes et aux rôles). Certains services prennent également en charge l'attachement de stratégies d'autorisation aux ressources.

Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté d'autorisations d'administrateur. Pour plus d'informations, consultez [Bonnes pratiques IAM](#) dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Les sections suivantes expliquent le fonctionnement des stratégies d'accès et leur utilisation pour protéger vos sauvegardes.

Rubriques

- [Ressources et opérations](#)
- [Propriété des ressources](#)
- [Spécification des éléments d'une politique : actions, effets et principaux](#)
- [Spécification de conditions dans une politique](#)
- [Autorisations d'API : référence des actions, ressources et conditions](#)
- [Autorisations de copie de balises](#)
- [politiques d'accès](#)

Ressources et opérations

Une ressource est un objet qui existe au sein d'un service. AWS Backup les ressources incluent les plans de sauvegarde, les coffres-forts de sauvegarde et les sauvegardes. Backup est un terme général qui fait référence aux différents types de ressources de sauvegarde qui existent dans AWS. Par exemple, les instantanés Amazon EBS, les instantanés Amazon Relational Database Service (Amazon RDS) et les sauvegardes Amazon DynamoDB sont tous des types de ressources de sauvegarde.

Dans AWS Backup, les sauvegardes sont également appelées points de restauration. Lors de l'utilisation AWS Backup, vous travaillez également avec les ressources d'autres AWS services que vous essayez de protéger, tels que les volumes Amazon EBS ou les tables DynamoDB. Ces ressources sont associées à des noms de ressources Amazon (ARNs) uniques. ARNs identifier les

AWS ressources de manière unique. Vous devez disposer d'un ARN pour spécifier une ressource sans aucune ambiguïté au sein d' AWS, par exemple dans les politiques IAM ou les appels d'API.

Le tableau suivant répertorie les ressources, les sous-ressources, le format ARN et un exemple d'ID unique.

AWS Backup ressource ARNs

Type de ressource	Format ARN	Exemple d'ID unique
Plan de sauvegarde	arn:aws:backup: <i>region</i> : <i>account-id</i> :backup-plan:*	
Coffre-fort de sauvegarde	arn:aws:backup: <i>region</i> : <i>account-id</i> :backup-vault:*	
Point de récupération pour Amazon EBS	arn:aws:ec2: <i>region</i> :::snapshot/*	snapshot/snap-05f426fd8kdjb4224
Point de récupération pour les EC2 images Amazon	arn:aws:ec2: <i>region</i> :::image/ami-*	image/ami-1a2b3e4f5e6f7g890
Point de récupération pour Amazon RDS	arn:aws:rds: <i>region</i> : <i>account-id</i> :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Point de récupération pour Aurora	arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Point de restauration pour Aurora DSQL	arn:aws:backup: <i>region</i> : <i>account-id</i> :recovery-	arn:aws:backup:us-east-1:012345678901:recovery-point:8

Type de ressource	Format ARN	Exemple d'ID unique
	point: <i>recovery-point-id</i>	a92c3f1-b475-4d9e-95e6-7c138f2d4b0a
Point de récupération pour Storage Gateway	arn:aws:e c2: <i>region</i> ::snapshot/ *	snapshot/snap-0d40e49137e31d9e0
Point de récupération pour DynamoDB sans Sauvegarde DynamoDB avancée	arn:aws:d ynamodb: <i>region:account-id</i> :table/*/backup/*	table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3
Point de récupération pour DynamoDB avec Sauvegarde DynamoDB avancée activé	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Point de récupération pour Amazon EFS	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e
Point de récupération pour Amazon FSx	arn:aws:f sx: <i>region:account-id</i> :backup/backup-*	backup/backup-1a20e49137e31d9e0
Point de récupération pour une machine virtuelle	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	1801234a-5b6b-7dc8-8032-836f7ffc623b
Point de récupération pour la sauvegarde continue Amazon S3	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucket</i> -5ec207d0
Point de récupération pour la sauvegarde périodique S3	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	<i>amzn-s3-demo-bucket</i> -20211231900000-5ec207d0

Type de ressource	Format ARN	Exemple d'ID unique
Point de récupération pour Amazon DocumentDB	arn:aws:rs: ds: <i>region:account-id</i> :cluster-snapshot: awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Point de reprise pour Neptune	arn:aws:rs: ds: <i>region:account-id</i> :cluster-snapshot: awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Point de reprise pour Amazon Redshift	arn:aws:rs: edshift: <i>region:account-id</i> :snapshot : <i>resource</i> /awsbacku p:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Point de reprise pour Amazon Redshift Serverless	arn:aws:redshift- serverless : <i>region:account-id</i> :snapshot: <i>resource</i> / awsbackup:*	awsbackup:job-ab12 cd3e-4567-8901-fg1 h-234567i89012
Point de récupération pour Amazon Timestream	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012_be ta
Point de récupération pour le AWS CloudFormation modèle	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012
Point de récupération pour la base de données SAP HANA sur une instance Amazon EC2	arn:aws:b ackup: <i>region:account-id</i> :recovery-point:*	recovery-point:1a2 b3cde-f405-6789-01 2g-3456hi789012

Les ressources qui prennent en charge AWS Backup la gestion complète comportent toutes des points de récupération au format `arn:aws:backup:region:account-id::recovery-point:*`, ce qui vous permet d'appliquer plus facilement des politiques d'autorisation pour protéger ces points de récupération. Pour savoir quelles ressources prennent en charge AWS Backup la gestion complète, consultez cette section du [Disponibilité des fonctionnalités par ressource](#) tableau.

AWS Backup fournit un ensemble d'opérations permettant de travailler avec AWS Backup les ressources. Pour obtenir la liste des opérations disponibles, consultez AWS Backup [Actions](#).

Propriété des ressources

Il Compte AWS est propriétaire des ressources créées dans le compte, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire Compte AWS de la ressource est l'[entité principale](#) (c'est-à-dire l'utilisateur Compte AWS root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création de ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification de l'utilisateur Compte AWS root Compte AWS pour créer un coffre-fort de sauvegarde, vous Compte AWS en êtes le propriétaire.
- Si vous créez un utilisateur IAM dans votre coffre Compte AWS et que vous accordez à cet utilisateur l'autorisation de créer un coffre de sauvegarde, celui-ci peut créer un coffre de sauvegarde. Toutefois, votre compte AWS, auquel l'utilisateur appartient, est propriétaire de la ressource que constitue le coffre-fort de sauvegarde.
- Si vous créez un rôle IAM Compte AWS avec les autorisations nécessaires pour créer un coffre-fort de sauvegarde, toute personne susceptible d'assumer ce rôle peut créer un coffre-fort. Vous Compte AWS, à qui appartient le rôle, êtes propriétaire de la ressource du coffre de sauvegarde.

Spécification des éléments d'une politique : actions, effets et principaux

Pour chaque AWS Backup ressource (voir [Ressources et opérations](#)), le service définit un ensemble d'opérations d'API (voir [Actions](#)). Pour accorder des autorisations pour ces opérations d'API AWS Backup, définissez un ensemble d'actions que vous pouvez spécifier dans une politique. Une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments les plus élémentaires d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour de plus amples informations, veuillez consulter [Ressources et opérations](#).

- **Action** : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser.
- **Effet** – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- **Principal** – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource).

Pour plus d'informations sur la syntaxe des politiques IAM et pour obtenir des descriptions, consultez [Référence de politique JSON IAM](#) dans le manuel Guide de l'utilisateur IAM.

Pour un tableau présentant toutes les actions de l' AWS Backup API, consultez [Autorisations d'API : référence des actions, ressources et conditions](#).

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage des politiques IAM afin de spécifier les conditions définissant à quel moment une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez [Condition](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

AWS Backup définit son propre ensemble de clés de condition. Pour consulter la liste des clés de AWS Backup condition, reportez-vous à la section [Clés de condition pour AWS Backup](#) la référence d'autorisation de service.

Autorisations d'API : référence des actions, ressources et conditions

Lorsque vous configurez [Contrôle d'accès](#) et que vous créez une stratégie d'autorisation que vous pouvez attacher à une identité IAM (stratégies basées sur une identité), vous pouvez utiliser la

de tableaux ci-dessous comme référence. Le chaque opération d' AWS Backup API, les actions correspondantes pour lesquelles vous pouvez accorder des autorisations pour effectuer l'action et la AWS ressource pour laquelle vous pouvez accorder les autorisations. Vous spécifiez les actions dans le champ `Action` de la politique ainsi que la valeur des ressources dans le champ `Resource` de la politique. Si le champ `Resource` est vide, vous pouvez utiliser le caractère générique (*) pour inclure toutes les ressources.

Vous pouvez utiliser des AWS clés de condition larges dans vos AWS Backup polices pour exprimer des conditions. Pour obtenir la liste complète des touches AWS-wide, consultez la section [Clés disponibles](#) dans le guide de l'utilisateur IAM.

¹ Utilisez la politique d'accès au coffre existante.

² Voir [AWS Backup ressource ARNs](#) pour le point de récupération spécifique à la ressource. ARNs

³ `StartRestoreJob` doit contenir la paire clé-valeur dans les métadonnées de la ressource. Pour obtenir les métadonnées de la ressource, appelez l'API `GetRecoveryPointRestoreMetadata`.

Pour plus d'informations, consultez la rubrique [Actions, ressources et clés de condition pour AWS Backup](#) dans la section Référence de l'autorisation de service.

Autorisations de copie de balises

Lorsqu'il AWS Backup exécute une tâche de sauvegarde ou de copie, il tente de copier les balises de votre ressource source (ou point de récupération dans le cas d'une copie) vers votre point de restauration.

Note

AWS Backup ne copie pas les balises de manière native pendant les tâches de restauration. Pour une architecture axée sur les événements qui copiera les balises pendant les tâches de restauration, voir [Comment conserver les balises de ressources dans les tâches de AWS Backup restauration](#).

Au cours d'une tâche de sauvegarde ou de copie, AWS Backup agrège les balises que vous spécifiez dans votre plan de sauvegarde (ou plan de copie, ou sauvegarde à la demande) avec les balises de votre ressource source. Cependant, AWS impose une limite de 50 balises par ressource, qui AWS Backup ne peut pas être dépassée. Lorsqu'une tâche de sauvegarde ou de copie regroupe

les balises du plan et de la ressource source, elle peut découvrir plus de 50 balises au total ; elle ne pourra pas terminer la tâche et échouera. Cela est conforme aux meilleures pratiques en matière de balisage à grande AWS échelle.

- Votre ressource possède plus de 50 balises après avoir agrégé vos balises de tâche de sauvegarde avec vos balises de ressource source. AWS prend en charge jusqu'à 50 balises par ressource.
- Le rôle IAM que vous attribuez n'est AWS Backup pas autorisé à lire les balises source ou à définir les balises de destination. Pour plus d'informations et des exemples de politiques de rôle IAM, consultez [Politiques gérées](#).

Vous pouvez utiliser votre plan de sauvegarde (balises ajoutées aux points de récupération) pour créer des balises qui contredisent les balises de vos ressources sources. Lorsque les deux sont en conflit, les balises de votre plan de sauvegarde ont priorité. Utilisez cette technique si vous préférez ne pas copier la valeur d'une balise depuis votre ressource source. Spécifiez la même clé de balise, mais une valeur différente ou vide, à l'aide de votre plan de sauvegarde.

Autorisations requises pour attribuer des balises aux sauvegardes

Type de ressource	Autorisation obligatoire
Système de fichiers Amazon EFS	<code>elasticfilesystem:DescribeTags</code>
Système de FSx fichiers Amazon	<code>fsx:ListTagsForResource</code>
Base de données Amazon RDS et cluster Amazon Aurora	<code>rds:AddTagsToResource</code> <code>rds:ListTagsForResource</code>
Volume Storage Gateway	<code>storagegateway:ListTagsForResource</code>
EC2 Instance Amazon et volume Amazon EBS	<code>EC2:CreateTags</code> <code>EC2:DescribeTags</code>

DynamoDB ne prend pas en charge l'attribution de balises aux sauvegardes, sauf si vous activez d'abord [Sauvegarde DynamoDB avancée](#).

Lorsqu'une EC2 sauvegarde Amazon crée un point de restauration d'image et un ensemble de snapshots, elle AWS Backup copie les balises dans l'AMI qui en résulte. AWS Backup copie également les balises des volumes associés à l'EC2 instance Amazon vers les instantanés qui en résultent.

politiques d'accès

Une permissions policy (politique d'autorisation) décrit qui a accès à quoi. Les politiques attachées à une identité IAM sont appelées des politiques basées sur l'identité (politiques IAM). Les politiques associées à une ressource sont appelées politiques basées sur les ressources. AWS Backup prend en charge à la fois les politiques basées sur l'identité et les politiques basées sur les ressources.

Note

Cette section décrit l'utilisation d'IAM dans le contexte de AWS Backup. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, veuillez consulter [Qu'est-ce qu'IAM ?](#) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, veuillez consulter [Référence de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Politiques basées sur une identité (politiques IAM)

Les politiques basées sur une identité sont des politiques que vous pouvez attacher à une identité IAM, par exemple à des utilisateurs ou des rôles. Par exemple, vous pouvez définir une politique qui permet à un utilisateur de visualiser et de sauvegarder AWS des ressources, mais l'empêche de restaurer des sauvegardes.

Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez [Identités \(utilisateurs, groupes et rôles\)](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur l'utilisation de politiques IAM pour contrôler l'accès aux sauvegardes, consultez [Politiques gérées pour AWS Backup](#).

Politiques basées sur les ressources

AWS Backup prend en charge les politiques d'accès basées sur les ressources pour les coffres-forts de sauvegarde. Vous pouvez ainsi définir une stratégie d'accès qui peut contrôler quels utilisateurs disposent d'un type d'accès particulier aux sauvegardes organisées dans un coffre-fort de

sauvegarde. Les stratégies d'accès basées sur une ressource pour les coffres-forts de sauvegarde permettent de contrôler de manière simple l'accès à vos sauvegardes.

Les politiques d'accès au coffre de sauvegarde contrôlent l'accès des utilisateurs lorsque vous les utilisez AWS Backup APIs. Certains types de sauvegarde, tels que les instantanés Amazon Elastic Block Store (Amazon EBS) et Amazon Relational Database Service (Amazon RDS), sont également accessibles à l'aide de ces services ». APIs Vous pouvez créer des politiques d'accès distinctes dans IAM qui contrôlent l'accès à celles-ci APIs afin de contrôler totalement l'accès aux sauvegardes.

Pour savoir comment créer une stratégie d'accès pour les coffres-forts de sauvegarde, consultez [Stratégies d'accès aux coffres](#).

Fonctions du service IAM

Un rôle Gestion des identités et des accès AWS (IAM) est similaire à un utilisateur, dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. Un rôle de service est un rôle qu'un AWS service assume pour effectuer des actions en votre nom. AWS Backup étant le service qui effectue des opérations de sauvegarde en votre nom, vous devez lui transmettre un rôle à assumer lors des opérations de sauvegarde en votre nom. Pour plus d'informations sur les rôles IAM, consultez [Rôles IAM](#) dans le Guide de l'utilisateur IAM.

Le rôle auquel vous passez AWS Backup doit disposer d'une politique IAM avec les autorisations permettant d'effectuer des actions associées AWS Backup aux opérations de sauvegarde, telles que la création, la restauration ou l'expiration de sauvegardes. Des autorisations différentes sont requises pour chacun des AWS services pris en AWS Backup charge. Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS Backup permet d'assumer le rôle.

Lorsque vous attribuez des ressources à un plan de sauvegarde ou que vous effectuez une sauvegarde, une copie ou une restauration à la demande, vous devez transmettre un rôle de service autorisé à effectuer les opérations sous-jacentes sur les ressources spécifiées. AWS Backup utilise ce rôle pour créer, étiqueter et supprimer des ressources dans votre compte.

Utilisation de AWS rôles pour contrôler l'accès aux sauvegardes

Vous pouvez utiliser des rôles pour contrôler l'accès à vos sauvegardes en définissant des rôles étroitement limités et en spécifiant quelles personnes peuvent transmettre ce rôle à AWS Backup.

Par exemple, vous pouvez créer un rôle qui accorde uniquement des autorisations pour sauvegarder des bases de données Amazon Relational Database Service (Amazon RDS) et uniquement autoriser les propriétaires de bases de données Amazon RDS à transmettre ce rôle. AWS Backup AWS Backup fournit plusieurs politiques gérées prédéfinies pour chacun des services pris en charge. Vous pouvez attacher ces politiques gérées aux rôles que vous créez. Cela facilite la création de rôles spécifiques au service dotés des autorisations requises. AWS Backup

Pour plus d'informations sur les politiques AWS gérées pour AWS Backup, consultez [Politiques gérées pour AWS Backup](#).

Rôle de service par défaut pour AWS Backup

Lorsque vous utilisez la AWS Backup console pour la première fois, vous pouvez choisir de AWS Backup créer un rôle de service par défaut pour vous. Ce rôle dispose des autorisations AWS Backup nécessaires pour créer et restaurer des sauvegardes en votre nom.

Note

Le rôle par défaut est automatiquement créé lorsque vous utilisez la AWS Management Console. Vous pouvez créer le rôle par défaut à l'aide du AWS Command Line Interface (AWS CLI), mais cela doit être fait manuellement.

Si vous préférez utiliser des rôles personnalisés, tels que des rôles distincts pour différents types de ressources, vous pouvez également le faire et transmettre vos rôles personnalisés à AWS Backup. Pour voir des exemples de rôles qui permettent la sauvegarde et la restauration pour des types de ressources individuels, consultez la table [Politiques gérées par le client](#).

Le rôle de service par défaut est nommé `AWSBackupDefaultServiceRole`. Ce rôle de service contient deux politiques gérées, [AWSBackupServiceRolePolicyForBackup](#) et [AWSBackupServiceRolePolicyForRestores](#).

`AWSBackupServiceRolePolicyForBackup` inclut une politique IAM qui accorde des AWS Backup autorisations pour décrire la ressource sauvegardée, ainsi que la possibilité de créer, de supprimer, de décrire ou d'ajouter des balises à une sauvegarde, quelle que soit la AWS KMS clé avec laquelle elle est chiffrée.

`AWSBackupServiceRolePolicyForRestores` inclut une politique IAM qui accorde des AWS Backup autorisations pour créer, supprimer ou décrire la nouvelle ressource créée à partir d'une

sauvegarde, quelle que soit la AWS KMS clé avec laquelle elle est chiffrée. Il inclut également des autorisations pour baliser les ressources nouvellement créés.

Pour restaurer une EC2 instance Amazon, vous devez lancer une nouvelle instance.

Création d'une fonction du service par défaut dans la console

Les actions spécifiques que vous effectuez dans la AWS Backup console créent le rôle de service AWS Backup par défaut.

Pour créer le rôle de service AWS Backup par défaut dans votre AWS compte

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Pour créer le rôle pour votre compte, attribuez des ressources à un plan de sauvegarde ou créez une sauvegarde à la demande.
 - a. Créez un plan de sauvegarde et attribuez des ressources à la sauvegarde. Voir [Création d'un plan de sauvegarde](#).
 - b. Vous pouvez également créer une sauvegarde à la demande. Consultez [Création d'une sauvegarde à la demande](#).
3. Vérifiez que vous avez créé le `AWSBackupDefaultServiceRole` dans votre compte en suivant ces étapes :
 - a. Patientez quelques minutes. Pour plus d'informations, consultez [Les modifications que j'apporte ne sont pas toujours visibles immédiatement](#) dans le Guide de l'utilisateur AWS Identity and Access Management.
 - b. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
 - c. Dans le menu de navigation de gauche, choisissez Rôles.
 - d. Dans la barre de recherche, saisissez `AWSBackupDefaultServiceRole`. Si cette sélection existe, vous avez créé le rôle AWS Backup par défaut et terminé cette procédure.
 - e. Si `AWSBackupDefaultServiceRole` n'apparaît toujours pas, ajoutez les autorisations suivantes à l'utilisateur IAM ou au rôle IAM que vous utilisez pour accéder à la console.

JSON

```
{  
  "Version": "2012-10-17",
```

```

"Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "iam:CreateRole",
      "iam:AttachRolePolicy",
      "iam:PassRole"
    ],
    "Resource":"arn:aws:iam::*:role/service-role/
AWSBackupDefaultServiceRole"
  },
  {
    "Effect":"Allow",
    "Action":[
      "iam:ListRoles"
    ],
    "Resource":""
  }
]
}

```

Pour les régions de Chine, remplacez **aws** par **aws-cn**. Pour AWS GovCloud (US) les régions, remplacez **aws** par **aws-us-gov**.

- f. Si vous ne pouvez pas ajouter d'autorisations à votre utilisateur IAM ou à votre rôle IAM, demandez à votre administrateur de créer manuellement un rôle sous un nom autre que `AWSBackupDefaultServiceRole` et de l'associer à ces politiques gérées :
 - `AWSBackupServiceRolePolicyForBackup`
 - `AWSBackupServiceRolePolicyForRestores`

Politiques gérées pour AWS Backup

Les politiques gérées sont des politiques autonomes basées sur l'identité que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre compte AWS. Lorsque vous attachez une politique à une entité principale, vous accordez à cette dernière les autorisations définies dans la politique.

AWS les politiques gérées sont créées et administrées par AWS. Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique

AWS gère les AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée.

Les politiques gérées par le client vous fournissent des contrôles précis pour définir l'accès aux sauvegardes. AWS Backup Par exemple, vous pouvez les utiliser pour donner à votre administrateur de sauvegarde de base de données l'accès aux sauvegardes Amazon RDS, mais pas à celles d'Amazon EFS.

Pour plus d'informations, consultez la section [Politiques gérées](#) dans le guide de l'utilisateur IAM.

AWS politiques gérées

AWS Backup fournit les politiques AWS gérées suivantes pour les cas d'utilisation courants. Ces stratégies facilitent la définition des autorisations appropriées et le contrôle de l'accès à vos sauvegardes. Il existe deux types de stratégies gérées. L'un des types est conçu pour être affecté aux utilisateurs afin de contrôler leur accès à AWS Backup. L'autre type de stratégie gérée est conçu pour être attaché à des rôles que vous transmettez à AWS Backup. Le tableau suivant répertorie toutes les stratégies gérées fournies par AWS Backup et explique comment elles sont définies. Vous pouvez trouver ces politiques gérées dans la section Politiques de la console IAM.

Stratégies

- [AWSBackupAuditAccess](#)
- [AWSBackupDataTransferAccess](#)
- [AWSBackupFullAccess](#)
- [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#)
- [AWSBackupGuardDutyRolePolicyForScans](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupSearchOperatorAccess](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForItemRestores](#)

- [AWSBackupServiceRolePolicyForIndexing](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForSauvegarde S3](#)
- [AWSBackupServiceRolePolicyForRestauration S3](#)
- [AWSBackupServiceRolePolicyForScans](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)

AWSBackupAuditAccess

Cette politique autorise les utilisateurs à créer des contrôles et des cadres qui définissent leurs attentes en matière de AWS Backup ressources et d'activités, et à auditer les AWS Backup ressources et les activités par rapport à leurs contrôles et cadres définis. Cette politique accorde des autorisations AWS Config et des services similaires pour décrire les attentes des utilisateurs lors des audits.

Cette politique accorde également des autorisations pour fournir des rapports d'audit à Amazon S3 et à des services similaires, et permet aux utilisateurs de rechercher et d'ouvrir leurs rapports d'audit.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupAuditAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupDataTransferAccess

Cette politique fournit des autorisations pour le transfert des données du plan de AWS Backup stockage APIs, permettant à l'agent AWS Backint d'effectuer le transfert des données de sauvegarde avec le plan AWS Backup de stockage. Vous pouvez associer cette politique aux rôles assumés par les EC2 instances Amazon exécutant SAP HANA avec l'agent Backint.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupDataTransferAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupFullAccess

L'administrateur de sauvegarde dispose d'un accès complet aux AWS Backup opérations, notamment à la création ou à la modification de plans de sauvegarde, à l'affectation de AWS ressources aux plans de sauvegarde et à la restauration des sauvegardes. Les administrateurs

de sauvegarde sont chargés de déterminer et d'appliquer la conformité des sauvegardes en définissant des plans de sauvegarde conformes aux exigences professionnelles et réglementaires de l'entreprise. Les administrateurs de sauvegarde s'assurent également que les AWS ressources de leur organisation sont affectées au plan approprié.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupFullAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Cette politique autorise la passerelle de sauvegarde à synchroniser les métadonnées des machines virtuelles en votre nom.

Pour voir les autorisations de cette stratégie, consultez

[AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupGuardDutyRolePolicyForScans

Cette politique doit être ajoutée à un nouveau rôle d'analyse qui GuardDuty autorise Amazon à lire et à analyser vos sauvegardes. Vous devez associer ce rôle d'analyse à votre plan de sauvegarde dans les paramètres de protection contre les logiciels malveillants ou de scan. Lorsque AWS Backup lance une analyse, elle transmet ce rôle d'analyse à Amazon GuardDuty.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupGuardDutyRolePolicyForScans](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupOperatorAccess

Les opérateurs de sauvegarde sont des utilisateurs chargés de veiller à ce que les ressources dont ils sont responsables sont correctement sauvegardées. Les opérateurs de sauvegarde sont autorisés à affecter AWS des ressources aux plans de sauvegarde créés par l'administrateur de sauvegarde. Ils sont également autorisés à créer des sauvegardes à la demande de leurs AWS ressources et à configurer la période de conservation des sauvegardes à la demande. Les opérateurs de sauvegarde ne sont pas autorisés à créer ni modifier les plans de sauvegarde, ni supprimer les sauvegardes planifiées après leur création. Les opérateurs de sauvegarde peuvent restaurer les sauvegardes. Vous pouvez limiter les types de ressources qu'un opérateur de sauvegarde peut affecter à un plan de sauvegarde ou restaurer à partir d'une sauvegarde. Pour ce faire, vous n'autorisez le transfert AWS Backup que de certains rôles de service dotés d'autorisations pour un certain type de ressource.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupOperatorAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupOrganizationAdminAccess

L'administrateur de l'organisation dispose d'un accès complet aux AWS Organizations opérations, notamment à la création, à la modification ou à la suppression de politiques de sauvegarde, à l'attribution de politiques de sauvegarde aux comptes et aux unités organisationnelles et à la surveillance des activités de sauvegarde au sein de l'organisation. Les administrateurs de l'organisation sont responsables de la protection des comptes de leur organisation avec la définition et l'affectation de stratégies de sauvegarde qui répondent aux exigences commerciales et réglementaires de leur organisation.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupOrganizationAdminAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupRestoreAccessForSAPHANA

Cette politique AWS Backup autorise la restauration d'une sauvegarde de SAP HANA sur Amazon EC2.

Pour consulter les autorisations associées à cette politique, consultez [AWSBackupRestoreAccessForSAPHANA](#) dans le manuel AWS Managed Policy Reference.

AWSBackupSearchOperatorAccess

Le rôle d'opérateur de recherche permet de créer des index de sauvegarde et de créer des recherches dans les métadonnées de sauvegarde indexées.

Cette politique contient les autorisations nécessaires pour ces fonctions.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupSearchOperatorAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupServiceLinkedRolePolicyForBackup

Cette politique est attachée au rôle lié au service nommé AWSServiceRoleforBackup pour permettre d' AWS Backup appeler les AWS services en votre nom pour gérer vos sauvegardes. Pour de plus amples informations, veuillez consulter [the section called "Sauvegarde et copie"](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSBackupServiceLinkedRolePolicyforBackup](#) à la référence des politiques AWS gérées.

AWSBackupServiceLinkedRolePolicyForBackupTest

Pour voir les autorisations de cette stratégie, consultez

[AWSBackupServiceLinkedRolePolicyForBackupTest](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupServiceRolePolicyForBackup

Permet de AWS Backup créer des sauvegardes de tous les types de ressources pris en charge en votre nom.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupServiceRolePolicyForBackup](#) dans le AWS Guide de référence des stratégies gérées par.

AWSBackupServiceRolePolicyForItemRestores

Description

Cette politique accorde aux utilisateurs l'autorisation de restaurer des fichiers et des éléments individuels dans un instantané (point de restauration périodique des sauvegardes) sur un compartiment Amazon S3 nouveau ou existant ou sur un nouveau volume Amazon EBS. Ces autorisations incluent : les autorisations de lecture accordées à Amazon EBS pour les instantanés gérés par des autorisations de AWS Backup lecture/écriture pour les compartiments Amazon S3, et la génération et la description des autorisations pour les clés. AWS KMS

Utilisation de cette politique

Vous pouvez associer `AWSBackupServiceRolePolicyForItemRestores` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure de création : 21 novembre 2024, 22:45 UTC
- Heure d'édition : Première instance
- ARN : `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Version de la politique : v1 (par défaut)

La version de cette politique définit les autorisations associées à la politique. Lorsque l'utilisateur ou le rôle doté de la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser ou non la demande.

Document de politique JSON :

AWSBackupServiceRolePolicyForItemRestores JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "EBSDirectReadAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "S3ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
    },
  ]
}
```

```

        "Resource": "arn:aws:s3:::*"
    },
    {
        "Sid": "S3PermissionsForFileLevelRestore",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:AbortMultipartUpload",
            "s3:ListMultipartUploadParts"
        ],
        "Resource": "arn:aws:s3:::*/*"
    },
    {
        "Sid": "KMSDataKeyForS3AndEC2Permissions",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": [
                    "ec2.*.amazonaws.com",
                    "s3.*.amazonaws.com"
                ]
            }
        }
    }
]
}

```

AWSBackupServiceRolePolicyForIndexing

Description

Cette politique accorde aux utilisateurs l'autorisation d'indexer les instantanés, également appelés points de restauration périodiques. Ces autorisations incluent : les autorisations de lecture accordées à Amazon EBS pour les instantanés gérés par des autorisations de AWS Backup lecture/écriture pour les compartiments Amazon S3, et la génération et la description des autorisations pour les clés. AWS KMS

Utilisation de cette politique

Vous pouvez associer `AWSBackupServiceRolePolicyForIndexing` à vos utilisateurs, groupes et rôles.

Détails de la politique

- Type : politique AWS gérée
- Heure d'édition : Première instance
- ARN : `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Version de la politique : v1 (par défaut)

La version de cette politique définit les autorisations associées à la politique. Lorsque l'utilisateur ou le rôle associé à la politique fait une demande d'accès à une AWS ressource, AWS vérifie la version par défaut de la politique pour déterminer s'il convient d'autoriser ou non la demande.

Document de politique JSON :

`AWSBackupServiceRolePolicyForIndexing` JSON

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EBSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSReadOnlyPermissions",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "*"
    }
  ],
}
```

```

    {
      "Sid": "EBSDirectReadAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid": "KMSDataKeyForEC2Permissions",
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:*::key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

AWSBackupServiceRolePolicyForRestores

Permet de AWS Backup restaurer les sauvegardes de tous les types de ressources pris en charge en votre nom.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupServiceRolePolicyForRestores](#) dans le AWS Guide de référence des stratégies gérées par.

Pour les restaurations d' EC2 instance, vous devez également inclure les autorisations suivantes pour lancer l' EC2 instance :

AWSBackupServiceRolePolicyForSauvegarde S3

Cette politique contient les autorisations nécessaires AWS Backup pour sauvegarder n'importe quel compartiment S3. Cela inclut l'accès à tous les objets d'un compartiment et à toute AWS KMS clé associée.

Pour consulter les autorisations associées à cette politique, consultez [AWSBackupServiceRolePolicyForS3Backup](#) dans le manuel AWS Managed Policy Reference.

AWSBackupServiceRolePolicyForRestauration S3

Cette politique contient les autorisations nécessaires AWS Backup pour restaurer une sauvegarde S3 dans un compartiment. Cela inclut les autorisations de lecture et d'écriture sur les buckets et l'utilisation de n'importe quelle AWS KMS clé en ce qui concerne les opérations S3.

Pour consulter les autorisations associées à cette politique, consultez [AWSBackupServiceRolePolicyForS3Restore](#) dans le manuel AWS Managed Policy Reference.

AWSBackupServiceRolePolicyForScans

La politique doit être attachée au rôle IAM que vous utilisez dans la sélection des ressources de votre plan de sauvegarde. Ce rôle accorde à AWS Backup l'autorisation de lancer des scans sur Amazon GuardDuty.

Pour voir les autorisations de cette stratégie, consultez [AWSBackupServiceRolePolicyForScans](#) dans le AWS Guide de référence des stratégies gérées par.

AWSServiceRolePolicyForBackupReports

AWS Backup utilise cette politique pour le rôle [AWSServiceRoleForBackupReports](#) lié au service. Ce rôle lié à un service donne AWS Backup les autorisations nécessaires pour surveiller et établir des rapports sur la conformité de vos paramètres de sauvegarde, de vos tâches et de vos ressources avec vos frameworks.

Pour voir les autorisations de cette stratégie, consultez [AWSServiceRolePolicyForBackupReports](#) dans le AWS Guide de référence des stratégies gérées par.

AWSServiceRolePolicyForBackupRestoreTesting

Pour voir les autorisations de cette stratégie, consultez [AWSServiceRolePolicyForBackupRestoreTesting](#) dans le AWS Guide de référence des stratégies gérées par.

Politiques gérées par le client

Les sections suivantes décrivent les autorisations de sauvegarde et de restauration recommandées pour les AWS services et les applications tierces pris en charge par AWS Backup. Vous pouvez

utiliser les politiques AWS gérées existantes comme modèle lorsque vous créez vos propres documents de politique, puis les personnaliser pour restreindre davantage l'accès à vos AWS ressources.

Important

Lorsque vous utilisez des rôles IAM personnalisés pour AWS Backup, vous devez inclure des autorisations spécifiques aux ressources en plus des autorisations. AWS Backup Par exemple, lorsque vous faites appel `backup:ListTags` à une ressource Amazon RDS, votre rôle IAM personnalisé doit également inclure `rds:ListTagsForResource` une autorisation. Bien que ces autorisations soient incluses dans le rôle de AWS Backup service par défaut, elles doivent être explicitement ajoutées aux politiques gérées par le client. Les autorisations de ressources sous-jacentes requises dépendent du AWS service et de l'opération spécifiques exécutés.

Amazon Aurora

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `RDSPermissions` déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Amazon Aurora DSQL

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- `DSQLBackupPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `DSQLRestorePermissions` déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Amazon DynamoDB

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Restaurer

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForRestores](#):

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- EBSResourcePermissions
- EBSTagAndDeletePermissions
- EBSCopyPermissions
- EBSSnapshotTierPermissions
- GetResourcesPermissions
- BackupVaultPermissions

Restaurer

Commencez par la EBSPermissions déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Ajoutez la déclaration suivante.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
    ],
    "Resource": "*"
},
```

Amazon EC2

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions

- BackupVaultPermissions

Restaurer

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForRestores](#):

- EBSPermissions
- EC2DescribePermissions
- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

Ajoutez la déclaration suivante.

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Remplacez *role-name* par le nom du rôle de profil d' EC2 instance qui sera attaché à l' EC2 instance restaurée. Il ne s'agit pas du rôle de AWS Backup service, mais du rôle IAM qui fournit des autorisations aux applications exécutées sur l' EC2 instance.

Amazon EFS

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- EFSPermissions
- GetResourcesPermissions
- BackupVaultPermissions

Restaurer

Commencez par la EFSPermissions déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Amazon FSx

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- FsxBackupPermissions
- FsxCreateBackupPermissions
- FsxPermissions
- FsxVolumePermissions
- FsxListTagsPermissions
- FsxDeletePermissions
- FsxResourcePermissions
- KMSPermissions

Restaurer

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForRestores](#):

- FsxPermissions
- FsxTagPermissions
- FsxBackupPermissions
- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon Neptune

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `RDSPermissions` déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Amazon RDS

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `RDSPermissions` déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Amazon S3

Sauvegarde

Commencez par [AWSBackupServiceRolePolicyForS3Backup](#).

Ajoutez les `BackupVaultCopyPermissions` instructions `BackupVaultPermissions` et si vous devez copier des sauvegardes sur un autre compte.

Restaurer

Commencez par [AWSBackupServiceRolePolicyForS3Restore](#).

AWS Storage Gateway

Sauvegarde

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForBackup](#):

- StorageGatewayPermissions
- EBSTagAndDeletePermissions
- GetResourcesPermissions
- BackupVaultPermissions

Ajoutez la déclaration suivante.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSnapshots"
  ],
  "Resource": "*"
},
```

Restaurer

Commencez par les affirmations suivantes provenant de [AWSBackupServiceRolePolicyForRestores](#):

- StorageGatewayVolumePermissions
- StorageGatewayGatewayPermissions
- StorageGatewayListPermissions

Machine virtuelle

Sauvegarde

Commencez par la BackupGatewayBackupPermissions déclaration de [AWSBackupServiceRolePolicyForBackup](#).

Restaurer

Commencez par la `GatewayRestorePermissions` déclaration de [AWSBackupServiceRolePolicyForRestores](#).

Sauvegarde cryptée

Pour restaurer une sauvegarde chiffrée, effectuez l'une des actions suivantes :

- Ajoutez votre rôle à la liste d'autorisation pour la politique AWS KMS clé
- Ajoutez les instructions suivantes [AWSBackupServiceRolePolicyForRestores](#) à partir de votre rôle IAM pour les restaurations :
 - `KMSDescribePermissions`
 - `KMSPermissions`
 - `KMSCreateGrantPermissions`

Mises à jour des politiques pour AWS Backup

Consultez les détails des mises à jour des politiques AWS gérées AWS Backup depuis que ce service a commencé à suivre ces modifications.

Modifier	Description	Date
AWSBackupGuardDutyRolePolicyForScans : nouvelle politique	AWS Backup a ajouté une nouvelle politique AWS gérée qui GuardDuty autorise Amazon à lire et à scanner les sauvegardes des clients. AWS Backup transmet un rôle associé à cette politique GuardDuty lors du lancement des opérations <code>StartMalwareScan</code> . Cela est nécessaire pour fournir toutes les autorisations nécessaires aux analyses de programmes malveillants sur les points de récupération	19 novembre 2025

Modifier	Description	Date
	des ressources Amazon EC2, Amazon EBS et Amazon S3. Pour plus d'informations, consultez la politique gérée AWSBackupGuardDutyRolePolicyForScans.	
AWSBackupServiceRolePolicyForScans : nouvelle politique	AWS Backup a ajouté une nouvelle politique AWS gérée qui AWS Backup autorise le lancement d'analyses de programmes malveillants sur vos points de récupération. Cela est nécessaire pour fournir toutes les autorisations nécessaires aux analyses de programmes malveillants sur les points de récupération des ressources Amazon EC2, Amazon EBS et Amazon S3. Pour plus d'informations, consultez la politique gérée AWSBackupServiceRolePolicyForScans.	19 novembre 2025
AWSBackupFullAccess : mise à jour d'une politique existante	Ajouté malware-protection.guardduty.amazonaws.com à IAMPassRolePermissions, ce qui est nécessaire pour lancer des tâches d'analyse des logiciels malveillants.	19 novembre 2025

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : - malware-protection.guardduty.amazonaws.com sur IamPassRolePermissions - backup:StartScanJob Ces autorisations sont nécessaires pour lancer des tâches d'analyse des programmes malveillants.	19 novembre 2025
AWSBackupFullAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : - eks:ListClusters - eks:ListTagsForResource - eks:DescribeCluster Ces autorisations permettent de AWS Backup sauvegarder et de restaurer les clusters Amazon EKS.	10 novembre 2025

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> Ces autorisations permettent de AWS Backup sauvegarder et de restaurer les clusters Amazon EKS.	10 novembre 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10 novembre 2025

Modifier	Description	Date
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Ces autorisations permettent à AWS Backup de créer des sauvegardes des clusters Amazon EKS et de leurs ressources associées pour le compte des clients.	

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>eks:ListClusters</code> • <code>eks:ListTagsForResource</code> • <code>eks:DescribeCluster</code> • <code>eks:ListAddons</code> • <code>eks:DescribeAddon</code> • <code>eks:ListNodegroups</code> • <code>eks:DescribeNodegroup</code> • <code>eks:ListPodIdentityAssociations</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:ListAccessEntries</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:ListFargateProfiles</code> • <code>eks:DescribeFargateProfile</code> • <code>ec2:DescribeLaunchTemplateVersions</code> • <code>eks:CreateAccessEntry</code>	10 novembre 2025

Modifier	Description	Date
	• <code>eks:AssociateAccessPolicy</code> • <code>eks:DisassociateAccessPolicy</code> Ces autorisations permettent à AWS Backup de créer des sauvegardes des clusters Amazon EKS et de leurs ressources associées pour le compte des clients.	

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>eks:CreateCluster</code> • <code>eks:DescribeCluster</code> • <code>eks:CreateAccessEntry</code> • <code>eks:DescribeAccessEntry</code> • <code>eks:AssociateAccessPolicy</code> • <code>eks:ListAssociatedAccessPolicies</code> • <code>eks:CreateAddon</code> • <code>eks:DescribeAddon</code> • <code>eks:CreateNodegroup</code> • <code>eks:DescribeNodegroup</code> • <code>eks:CreateFargateProfile</code> • <code>eks:DescribeFargateProfile</code> • <code>eks:CreatePodIdentityAssociation</code> • <code>eks:DescribePodIdentityAssociation</code> • <code>eks:TagResource</code> • <code>eks:DisassociateAccessPolicy</code> • <code>iam:PassRole</code>	10 novembre 2025

Modifier	Description	Date
	• <code>ec2:DescribeLaunchTemplateVersions</code> • <code>ec2:DescribeSubnets</code> • <code>ec2:RunInstances</code> • <code>ec2:CreateTags</code> • <code>iam:GetRole</code> • <code>iam:ListAttachedRolePolicies</code> • <code>backup:StartRestoreJob</code> • <code>backup:ListRestoreJobs</code> • <code>backup:ListRecoveryPointsByBackupVault</code> • <code>backup:DescribeRestoreJob</code> Ces autorisations permettent AWS Backup d'effectuer des opérations de restauration pour les clusters Amazon EKS et leurs ressources associées pour le compte des clients.	

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté l'autorisation suivante à cette politique : • <code>organizations:ListDelegatedAdministrators</code> Cette autorisation permet de AWS Backup synchroniser les informations de l'administrateur délégué avec les Organizations pour les fonctionnalités de gestion entre comptes.	9 septembre 2025

Modifier	Description	Date
AWSBackupGuardDutyRolePolicyForScans : nouvelle politique	AWS Backup a ajouté une nouvelle politique AWS gérée qui GuardDuty autorise Amazon à lire et à scanner les sauvegardes des clients. AWS Backup transmet un rôle associé à cette politique GuardDuty lors du lancement des opérations <code>StartMalwareScan</code> . Cela est nécessaire pour fournir toutes les autorisations nécessaires aux analyses de programmes malveillants sur les points de récupération des ressources Amazon EC2, Amazon EBS et Amazon S3. Pour plus d'informations, consultez la politique gérée AWSBackupGuardDutyRolePolicyForScans.	24 novembre 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForScans : nouvelle politique	AWS Backup a ajouté une nouvelle politique AWS gérée qui AWS Backup autorise le lancement d'analyses de programmes malveillants sur vos points de récupération. Cela est nécessaire pour fournir toutes les autorisations nécessaires aux analyses de programmes malveillants sur les points de récupération des ressources Amazon EC2, Amazon EBS et Amazon S3. Pour plus d'informations, consultez la politique gérée AWSBackupServiceRolePolicyForScans.	24 novembre 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>dsql:UpdateCluster</code> • <code>dsql:AddPeerCluster</code> • <code>dsql:RemovePeerCluster</code> • <code>dsql:GetCluster</code> Ces autorisations sont nécessaires pour AWS Backup effectuer des opérations de restauration multirégionales orchestrées pour les ressources DSQL pour le compte des clients.	17 juillet 2025

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>mpa:GetApprovalTeam</code> • <code>mpa:ListApprovalTeams</code> • <code>mpa:StartSession</code> • <code>mpa:CancelSession</code> • <code>mpa:GetSession</code> • <code>mpa:ListSessions</code> Ces autorisations sont nécessaires pour AWS Backup l'intégration. Les clients ont AWS Organizations donc la possibilité d'obtenir une approbation multipartite (MPA) dans le cadre de leurs coffres-forts logiquement espacés. Gestion de compte AWS	17 juin 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores — Mise à jour d'une politique existante :	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> Ces autorisations sont nécessaires pour permettre aux clients de restaurer des instantanés de zones de disponibilité multiples (multi-AZ) d'Amazon FSx pour OpenZFS via. AWS Backup	27 mai 2025
AWSBackupFullAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Ces autorisations permettent AWS Backup de sauvegarder et de restaurer les ressources SQL Amazon Aurora.	21 mai 2025

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>dsql:GetCluster</code> • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Ces autorisations permettent AWS Backup de sauvegarder et de restaurer les ressources SQL Amazon Aurora.	21 mai 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • kms:Decrypt • kms:ReEncryptTo • kms:ReEncryptFrom • dsql:StartBackupJob • dsql:GetBackupJob • dsql:StopBackupJob • dsql:GetCluster • dsql:ListClusters • dsql:ListTagsForResource Ces autorisations permettent AWS Backup de créer, de supprimer, de récupérer et de gérer des instantanés SQL Amazon Aurora pour le compte des clients.	21 mai 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>ec2:DescribeRouteTables</code> • <code>ec2:CreateTags</code> • <code>dsql:StartRestoreJob</code> • <code>dsql:GetRestoreJob</code> • <code>dsql:StopRestoreJob</code> • <code>dsql:TagResource</code> • <code>dsql>CreateCluster</code> • <code>dsql:PutMultiRegionProperties</code> • <code>dsql:PutWitnessRegion</code> • <code>kms:DescribeKey</code> Ces autorisations permettent AWS Backup de créer, de supprimer, de récupérer, de chiffrer, de déchiffrer et de gérer des instantanés Amazon Aurora DSQL pour le compte des clients.	21 mai 2025

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>dsql:ListClusters</code> • <code>dsql:ListTagsForResource</code> Ces autorisations permettent de AWS Backup gérer les sauvegardes Aurora DSQL à des intervalles spécifiés par le client.	21 mai 2025

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>aws:CalledVia</code> • <code>redshift-serverless>DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Ces autorisations sont nécessaires pour que les clients désignés aient un accès complet aux sauvegardes Amazon Redshift Serverless, y compris les autorisations de lecture requises ainsi que la possibilité de supprimer les points de restauration Amazon Redshift Serverless (sauvegardes instantanées).	31 mars 2025

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListWorkgroups</code> Ces autorisations sont nécessaires pour que les clients désignés disposent de toutes les autorisations de sauvegarde nécessaires pour Amazon Redshift Serverless, y compris les autorisations de lecture requises.	31 mars 2025

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>redshift-serverless:DeleteSnapshot</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:GetWorkgroup</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:ListWorkgroups</code> Ces autorisations sont nécessaires AWS Backup pour gérer les instantanés Amazon Redshift Serverless aux intervalles spécifiés par le client.	31 mars 2025

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>redshift-serverless:CreateSnapshot</code> • <code>redshift-serverless>DeleteSnapshot</code> avec une condition pour autoriser uniquement la suppression des instantanés avec le tag <code>"aws:backup:source-resource"</code> • <code>redshift-serverless:GetNamespace</code> • <code>redshift-serverless:GetSnapshot</code> • <code>redshift-serverless:ListNamespaces</code> • <code>redshift-serverless:ListSnapshots</code> • <code>redshift-serverless:ListTagsForResource</code> • <code>redshift-serverless:TagResource</code> Ces autorisations sont nécessaires pour créer, supprimer, récupérer et gérer les instantanés Amazon Redshift Serverless pour le	31 mars 2025

Modifier	Description	Date
	compte des clients. AWS Backup	
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations suivantes à cette politique : • <code>redshift-serverless:GetNamespaces</code> • <code>redshift-serverless:GetTableRestoreStatus</code> • <code>redshift-serverless:RestoreTableFromSnapshot</code> Ces autorisations sont nécessaires pour AWS Backup restaurer les instantanés Amazon Redshift et Amazon Redshift Serverless pour le compte du client.	31 mars 2025
AWSBackupSearchOperatorAccess — Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique <code>AWSBackupSearchOperatorAccess</code> AWS gérée.	27 février 2025

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup a ajouté l'autorisation <code>rds:AddTagsToResource</code> de prendre en charge la copie instantanée multi-tenant de plusieurs comptes Amazon RDS des sauvegardes. Cette autorisation est nécessaire pour terminer les opérations lorsqu'un client choisit de créer une copie multicompte d'un instantané RDS partagé.	8 janvier 2025
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	AWS Backup a ajouté les autorisations <code>rds:CreateTenantDatabase</code> et <code>rds>DeleteTenantDatabase</code> à cette politique pour soutenir le processus de restauration des ressources Amazon RDS. Ces autorisations sont nécessaires pour terminer les opérations client relatives à la restauration des instantanés multi-locataires.	8 janvier 2025
AWSBackupServiceRolePolicyForItemRestores — Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique <code>AWSBackupServiceRolePolicyForItemRestores</code> AWS gérée.	26 novembre 2024

Modifier	Description	Date
AWSBackupServiceRolePolicyForIndexing — Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique AWSBackupServiceRolePolicyForIndexing AWS gérée.	26 novembre 2024
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup autorisation ajoutée backup : TagResource à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024
AWSBackupServiceRolePolicyForS3Backup — Mise à jour d'une politique existante	AWS Backup autorisation ajoutée backup : TagResource à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	AWS Backup autorisation ajoutée backup : TagResource à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	L'autorisation a été ajoutée <code>ds:DeleteDBInstanceAutomatedBackups</code> . Cette autorisation est nécessaire pour AWS Backup prendre en charge la sauvegarde continue et point-in-time-restore les instances Amazon RDS.	1 mai 2024
AWSBackupFullAccess : mise à jour d'une politique existante	AWS Backup a mis à jour l'Amazon Resource Name (ARN) dans l'autorisation <code>storagegateway:ListVolumes</code> de <code>arn:aws:storagegateway:*:*:gateway/*</code> à <code>*</code> afin de tenir compte d'une modification du modèle d'API Storage Gateway.	1 mai 2024
AWSBackupOperatorAccess : mise à jour d'une politique existante	AWS Backup a mis à jour l'Amazon Resource Name (ARN) dans l'autorisation <code>storagegateway:ListVolumes</code> de <code>arn:aws:storagegateway:*:*:gateway/*</code> à <code>*</code> afin de tenir compte d'une modification du modèle d'API Storage Gateway.	1 mai 2024

Modifier	Description	Date
AWSServiceRolePolicyForBackupRestoreTesting : mise à jour d'une politique existante	Ajout des autorisations suivantes pour décrire et répertorier les points de récupération et les ressources protégées afin de réaliser des plans de test de restauration : <code>backup:DescribeRecoveryPoint</code> <code>backup:DescribeProtectedResource</code> ,<code>backup:ListProtectedResources</code> , et <code>backup:ListRecoveryPointsByResource</code> . Ajout de l'autorisation <code>ec2:DescribeSnapshotTierStatus</code> de prendre en charge le stockage au niveau des archives Amazon EBS. Ajout de l'autorisation <code>rds:DescribeDBClusterAutomatedBackups</code> de prendre en charge les sauvegardes continues d'Amazon Aurora. Les autorisations suivantes ont été ajoutées pour prendre en charge les tests de restauration des sauvegardes Amazon Redshift : <code>redshift:DescribeC</code>	14 février 2024

Modifier	Description	Date
	clusters et. redshift: DeleteCluster Ajout de l'autorisation timestream:DeleteTable de prendre en charge les tests de restauration des sauvegardes Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout des autorisations ec2:DescribeSnapshotTierStatus ec2:RestoreSnapshotTier . Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de restaurer les ressources Amazon EBS stockées à AWS Backup partir du stockage d'archives. Pour les restaurations d'EC2 instance, vous devez également inclure les autorisations, comme indiqué dans la déclaration de politique suivante pour lancer l' EC2 instance :	27 novembre 2023

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Ajout des autorisations <code>ec2:DescribeSnapshotTierStatus</code> et <code>ec2:ModifySnapshotTier</code> de la prise en charge d'une option de stockage supplémentaire pour les ressources Amazon EBS sauvegardées à transférer vers le niveau de stockage des archives. Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives.	27 novembre 2023

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout des autorisations <code>ec2:DescribeSnapshotTierStatus</code> et <code>ec2:ModifySnapshotTier</code> de la prise en charge d'une option de stockage supplémentaire pour les ressources Amazon EBS sauvegardées à transférer vers le niveau de stockage des archives. Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives. Ajout des autorisations <code>rds:DescribeDBClusterSnapshots</code> et <code>rds:RestoreDBClusterToPointInTime</code> des autorisations nécessaires pour les PITR (point-in-time restaurations) des clusters Aurora.	

Modifier	Description	Date
AWSServiceRolePolicyForBackupRestoreTesting : nouvelle politique	Fournit les autorisations nécessaires pour effectuer des tests de restauration. Les autorisations incluent les actions <code>list</code> , <code>read</code> , and <code>write</code> relatives aux services suivants à inclure dans les tests de restauration : Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon, EC2 Amazon EFS, pour Lustre, pour Windows File Server FSx , pour ONTAP FSx , pour OpenZFS FSx , Amazon Neptune, FSx Amazon RDS et Amazon S3.	27 novembre 2023
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout de <code>restore-testing.backup.amazonaws.com</code> à <code>IamPassRolePermissions</code> et <code>IamCreateServiceLinkedRolePermissions</code> . Cet ajout est nécessaire pour AWS Backup effectuer des tests de restauration pour le compte des clients.	27 novembre 2023

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout des autorisations <code>rds:DescribeDBClusterSnapshots</code> et <code>rds:RestoreDBClusterToPointInTime</code> des autorisations nécessaires pour les PITR (point-in-time restaurations) des clusters Aurora.	6 septembre 2023
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout de l'autorisation <code>rds:DescribeDBClusterAutomatedBackups</code> , qui est nécessaire pour la sauvegarde et la point-in-time restauration continues des clusters Aurora.	6 septembre 2023
AWSBackupOperatorAccess : mise à jour d'une politique existante	Ajout de l'autorisation <code>rds:DescribeDBClusterAutomatedBackups</code> , qui est nécessaire pour la sauvegarde et la point-in-time restauration continues des clusters Aurora.	6 septembre 2023

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	L'autorisation a été ajoutée <code>rds:DescribeDBClusterAutomatedBackups</code>. Cette autorisation est nécessaire pour AWS Backup prendre en charge la sauvegarde et la point-in-time restauration continues des clusters Aurora. Ajout de l'autorisation permettant <code>rds:DeleteDBClusterAutomatedBackups</code> au AWS Backup cycle de vie de supprimer et de dissocier les points de restauration continue Amazon Aurora à la fin d'une période de rétention. Cette autorisation est nécessaire pour que le point de récupération Aurora évite une transition vers un état EXPIRED. Ajout de l'autorisation <code>rds:ModifyDBCluster</code> qui permet AWS Backup d'interagir avec les clusters Aurora. Cet ajout permet aux utilisateurs d'activer ou de désactiver les sauvegardes continues en fonction des configurations souhaitées.	6 septembre 2023

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout de l'action permettant d'accorder <code>ram:GetResourceShareAssociations</code> à l'utilisateur l'autorisation d'obtenir des associations de partage de ressources pour le nouveau type de coffre-fort.	08 août 2023
AWSBackupOperatorAccess : mise à jour d'une politique existante	Ajout de l'action permettant d'accorder <code>ram:GetResourceShareAssociations</code> à l'utilisateur l'autorisation d'obtenir des associations de partage de ressources pour le nouveau type de coffre-fort.	08 août 2023
AWSBackupServiceRolePolicyForS3Backup — Mise à jour d'une politique existante	Ajout de l'autorisation <code>s3:PutInventoryConfiguration</code> d'améliorer les performances de sauvegarde en utilisant un inventaire des compartiments.	1er août 2023

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour autoriser l'utilisateur à ajouter des balises afin de restaurer les ressources : <code>storagegateway:AddTagsToResource</code> , <code>elasticfilesystem:TagResource</code> , uniquement <code>ec2:CreateTags</code> pour <code>ec2:CreateAction</code> cela inclut l'un <code>RunInstances</code> ou l'autre <code>CreateVolume</code> , <code>fsx:TagResource</code> , et <code>cloudformation:TagResource</code> .	22 mai 2023
AWSBackupAuditAccess : mise à jour d'une politique existante	La sélection des ressources dans l'API <code>config:DescribeComplianceByConfigRule</code> a été remplacée par une ressource générique afin de faciliter la sélection des ressources par un utilisateur.	11 avril 2023
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout de l'autorisation suivante pour restaurer Amazon EFS à l'aide d'une clé gérée par le client : <code>kms:GenerateDataKeyWithoutPlaintext</code> . Cela permet de garantir que les utilisateurs disposent des autorisations requises pour restaurer les ressources Amazon EFS.	27 mars 2023

Modifier	Description	Date
AWSServiceRolePolicyForBackupReports : mise à jour d'une politique existante	Mise à jour des config:DescribeConfigRuleEvaluationStatus actions config:DescribeConfigRules et pour permettre à AWS Backup Audit Manager d'accéder aux règles gérées par AWS Backup Audit Manager AWS Config .	9 mars 2023
AWSBackupServiceRolePolicyForS3Restore — Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées : kms:Decrypt s3:PutBucketOwnershipControls , et s3:GetBucketOwnershipControls à la politique AWSBackupServiceRolePolicyForS3Restore . Ces autorisations sont nécessaires pour prendre en charge les restaurations d'objets lorsque le chiffrement KMS est utilisé dans la sauvegarde d'origine et pour restaurer des objets lorsque la propriété des objets est configurée sur le compartiment d'origine au lieu de la liste ACL.	13 février 2023

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout des autorisations suivantes pour planifier les sauvegardes à l'aide de VMware balises de machines virtuelles et pour prendre en charge la limitation de bande passante basée sur la planification : <code>backup-gateway:GetHypervisorPropertyMappings</code> , <code>backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings</code> , <code>backup-gateway:GetHypervisor</code> et <code>backup-gateway:StartVirtualMachinesMetadataSync</code> <code>backup-gateway:GetBandwidthRateLimitSchedule</code> <code>backup-gateway:PutBandwidthRateLimitSchedule</code>	15 décembre 2022

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	Ajout des autorisations suivantes pour planifier les sauvegardes à l'aide de VMware balises de machines virtuelles et pour prendre en charge la limitation de bande passante basée sur la planification : <code>backup-gateway:GetHypervisorPropertyMappings</code> ,, et. <code>backup-gateway:GetVirtualMachine</code> <code>backup-gateway:GetHypervisor</code> <code>backup-gateway:GetBandwidthRateLimitSchedule</code>	15 décembre 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync : nouvelle politique	Permet à AWS Backup Gateway de synchroniser les métadonnées des machines virtuelles sur les réseaux locaux avec Backup Gateway.	15 décembre 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde Timestream : timestream:StartAwsBackupJob timestream:GetAwsBackupStatus ,timestream:ListTables ,timestream:ListDatabases ,timestream:ListTagsForResource , timestream:DescribeTable timestream:DescribeDatabase , et timestream:DescribeEndpoints	13 décembre 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de restauration Timestream : timestream:StartAwsRestoreJob timestream:GetAwsRestoreStatus timestream:ListTables timestream:ListTagsForResource timestream:ListDatabases timestream:DescribeTable timestream:DescribeDatabase s3:GetBucketAcl , et timestream:DescribeEndpoints	13 décembre 2022
AWSBackupFullAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream : timestream:ListTables timestream:ListDatabases , s3:ListAllMyBuckets et timestream:DescribeEndpoints	13 décembre 2022

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream : <code>timestream:ListDatabases</code> , <code>timestream:ListTables</code> <code>s3:ListAllMyBuckets</code> , et. <code>timestream:DescribeEndpoints</code>	13 décembre 2022
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream : <code>timestream:ListDatabases</code> <code>timestream:ListTables</code> , <code>timestream:ListTagsForResource</code> , <code>timestream:DescribeDatabase</code> , <code>timestream:DescribeTable</code> , <code>timestream:GetAwsBackupStatus</code> <code>timestream:GetAwsRestoreStatus</code> , et. <code>timestream:DescribeEndpoints</code>	13 décembre 2022

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Amazon Redshift : redshift:DescribeClusters redshift:DescribeClusterSubnetGroups ,redshift:DescribeNodeConfigurationOptions ,redshift:DescribeOrderableClusterOptions ,redshift:DescribeClusterParameterGroups , redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules , et. ec2:DescribeAddresses	27 novembre 2022

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Amazon Redshift : <code>redshift:DescribeClusters</code> <code>redshift:DescribeClusterSubnetGroups</code> <code>redshift:DescribeNodeConfigurationOptions</code> <code>redshift:DescribeOrderableClusterOptions</code> <code>redshift:DescribeClusterParameterGroups</code> <code>redshift:DescribeClusterTracks</code> <code>redshift:DescribeSnapshotSchedules</code> <code>elastic2:DescribeAddresses</code>	27 novembre 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de restauration Amazon Redshift : <code>redshift:RestoreFromClusterSnapshot</code> , <code>redshift:RestoreTableFromClusterSnapshot</code> <code>redshift:DescribeClusters</code> , et <code>redshift:DescribeTableRestoreStatus</code>	27 novembre 2022
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde Amazon Redshift : <code>redshift:CreateClusterSnapshot</code> , <code>redshift:DescribeClusterSnapshots</code> , <code>redshift:DescribeTags</code> , <code>redshift>DeleteClusterSnapshot</code> <code>redshift:DescribeClusters</code> , et <code>redshift:CreateTags</code>	27 novembre 2022
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout de l'autorisation suivante pour les CloudFormation ressources de support : <code>cloudformation:ListStacks</code> .	27 novembre 2022

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	Ajout de l'autorisation suivante pour les CloudFormation ressources de support : <code>cloudformation:ListStacks</code> .	27 novembre 2022
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour CloudFormation les ressources de support : <code>redshift:DescribeClusterSnapshots</code> <code>redshift:DescribeTags</code> , <code>redshift>DeleteClusterSnapshot</code> , et <code>redshift:DescribeClusters</code> .	27 novembre 2022
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde de la pile d'CloudFormation applications : <code>cloudformation:GetTemplate</code> <code>cloudformation:DescribeStacks</code> , et <code>cloudformation:ListStackResources</code> .	16 novembre 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout des autorisations suivantes pour prendre en charge les tâches de sauvegarde de la pile d'CloudFormation applications : <code>cloudformation:CreateChangeSet</code> et <code>cloudformation:DescribeChangeSet</code>	16 novembre 2022
AWSBackupOrganizationAdminAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées à cette politique pour permettre aux administrateurs de l'organisation d'utiliser la fonctionnalité d'administration déléguée : <code>organizations:ListDelegatedAdministrators</code> , <code>organizations:RegisterDelegatedAdministrator</code> , et <code>organizations:DeregisterDelegatedAdministrator</code>	27 novembre 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur EC2 les instances Amazon : ssm-sap:GetOperation ssm-sap:ListDatabases ,ssm-sap:BackupDatabase ,ssm-sap:UpdateHanaBackupSettings ,ssm-sap:GetDatabase , etssm-sap:ListTagsForResource .	20 novembre 2022
AWSBackupFullAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur EC2 les instances Amazon : ssm-sap:GetOperation ssm-sap:ListDatabases ,ssm-sap:GetDatabase , etssm-sap:ListTagsForResource .	20 novembre 2022
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur EC2 les instances Amazon : ssm-sap:GetOperation ssm-sap:ListDatabases ,ssm-sap:GetDatabase , etssm-sap:ListTagsForResource .	20 novembre 2022

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout de l'autorisation suivante pour prendre en charge les EC2 instances SAP HANA sur Amazon : <code>ssm-sap:GetOperation</code> .	20 novembre 2022
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	L'autorisation suivante a été ajoutée pour prendre en charge les tâches de restauration de la passerelle Backup sur une EC2 instance : <code>ec2:CreateTags</code> .	20 novembre 2022
AWSBackupDataTransferAccess : mise à jour d'une politique existante	Ajout des autorisations suivantes pour prendre en charge le transfert sécurisé des données de stockage pour les EC2 ressources SAP HANA On Amazon : <code>backup-storage:StartObject backup-storage:PutChunk ,backup-storage:GetChunk ,backup-storage:ListChunks ,backup-storage:ListObjects ,backup-storage:GetObjectMetadata ,etbackup-storage:NotifyObjectComplete</code> .	20 novembre 2022

Modifier	Description	Date
AWSBackupRestoreAccessForSAPHANA — Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour permettre aux propriétaires de ressources d'effectuer la restauration EC2 des ressources SAP HANA On Amazon : <code>backup:Get*</code> <code>backup:List*</code> <code>backup:Describe*</code> <code>backup:StartBackupJob</code> <code>backup:StartRestoreJob</code> <code>ssm-sap:GetOperation</code> <code>ssm-sap:ListDatabases</code> <code>ssm-sap:BackupDatabase</code> <code>ssm-sap:RestoreDatabase</code> <code>ssm-sap:UpdateHanaBackupSettings</code> <code>ssm-sap:GetDatabase</code> <code>ssm-sap:ListTagsForResource</code> .	20 novembre 2022
AWSBackupServiceRolePolicyForS3Backup — Mise à jour d'une politique existante	Ajout de l'autorisation <code>s3:GetBucketAcl</code> de prendre en charge les opérations de sauvegarde AWS Backup pour Amazon S3.	24 août 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout des actions suivantes pour autoriser l'accès à la création d'une instance de base de données prenant en charge la fonctionnalité de zone de disponibilité multiple (Multi-AZ) : <code>rds:CreateDBInstance</code>	20 juillet 2022
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout de <code>s3:GetBucketTagging</code> autorisation d'accorder à l'utilisateur l'autorisation de sélectionner des buckets à sauvegarder avec un caractère générique de ressource. Sans cette autorisation, les utilisateurs qui sélectionnent les compartiments à sauvegarder avec un caractère générique de ressource échouent.	6 mai 2022
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Ajout de ressources de volume dans le cadre des <code>fsx:ListTagsForResource</code> actions existantes <code>fsx:CreateBackup</code> et ajout d'une nouvelle action FSx pour <code>fsx:DescribeVolumes</code> prendre en charge les sauvegardes ONTAP au niveau du volume.	27 avril 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour accorder aux utilisateurs les autorisations de restauration FSx des volumes ONTAP <code>fsx:DescribeVolumes</code> , <code>fsx:CreateVolumeFromBackup</code> <code>fsx:DeleteVolume</code> , et <code>fsx:UntagResource</code> .	27 avril 2022
AWSBackupServiceRolePolicyForS3Backup — Mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour autoriser l'utilisateur à recevoir des notifications de modifications apportées à ses compartiments Amazon S3 lors des opérations de sauvegarde : <code>s3:GetBucketNotification</code> et <code>s3:PutBucketNotification</code> .	25 février 2022

Modifier	Description	Date
AWSBackupServiceRolePolicyForS3Backup — Nouvelle politique	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses compartiments Amazon S3 : s3:GetInventoryConfiguration s3:PutInventoryConfiguration ,s3:ListBucketVersions ,s3:ListBucket ,s3:GetBucketTagging ,s3:GetBucketVersioning , s3:GetBucketNotification s3:GetBucketLocation ,et s3:ListAllMyBuckets Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses objets Amazon S3 : s3:GetObject s3GetObjectAcl ,s3:GetObjectVersionTagging ,s3:GetObjectVersionAcl ,s3:GetObjectTagging , ets3:GetObjectVersion . Les actions suivantes ont été ajoutées pour accorder	17 février 2022

Modifier	Description	Date
	à l'utilisateur l'autorisation de sauvegarder ses données Amazon S3 chiffrées : kms:Decrypt et kms:DescribeKey . Les actions suivantes ont été ajoutées pour autoriser l'utilisateur à effectuer des sauvegardes incrémentielles de ses données Amazon S3 en utilisant EventBridge les règles Amazon : events:DescribeRule events:EnableRule events:PutRule ,events:DeleteRule ,events:PutTargets ,events:RemoveTargets ,events:ListTargetsByRule ,events:DisableRule cloudwatch:GetMetricData ,events:ListRules .	

Modifier	Description	Date
AWSBackupServiceRolePolicyForS3Restore — Nouvelle politique	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de restaurer ses compartiments Amazon S3 : s3:CreateBucket s3:ListBucketVersion s3:ListBucket s3:GetBucketVersion s3:GetBucketLocation , s3:PutBucketVersion . Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de restaurer ses compartiments Amazon S3 : s3:GetObject s3:GetObjectVersion s3:DeleteObject ,s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging ,s3:PutObjectTagging ,s3:GetObjectAcl , s3:PutObjectAcl s3:PutObject , s3:ListMultipartUploadParts . Les actions suivantes ont été ajoutées pour autoriser	17 février 2022

Modifier	Description	Date
	l'utilisateur à chiffrer ses données Amazon S3 restaurées :kms:Decrypt ,kms:DescribeKey , et kms:GenerateDataKey .	
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajouté s3:ListAllMyBuckets pour autoriser l'utilisateur à consulter la liste de ses compartiments et à choisir ceux à attribuer à un plan de sauvegarde.	14 février 2022
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajouté backup-gateway:ListVirtualMachines pour accorder à l'utilisateur l'autorisation de consulter la liste de ses machines virtuelles et de choisir celles à attribuer à un plan de sauvegarde. Ajouté backup-gateway:ListTagsForResource pour accorder à l'utilisateur l'autorisation de répertorier les balises de ses machines virtuelles.	30 novembre 2021

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Ajouté backup-gateway:Backup pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs sauvegardes de machines virtuelles. AWS Backup également ajouté backup-gateway:ListTagsForResource pour accorder à l'utilisateur l'autorisation de répertorier les balises attribuées à ses sauvegardes de machines virtuelles.	30 novembre 2021
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajouté backup-gateway:Restore pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs sauvegardes de machines virtuelles.	30 novembre 2021

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	Ajout des actions suivantes pour autoriser les utilisateurs à utiliser AWS Backup Gateway pour sauvegarder, restaurer et gérer leurs machines virtuelles : <code>backup-gateway:AssociateGatewayToServer</code> , <code>backup-gateway:CreateGateway</code> , <code>backup-gateway:DeleteGateway</code> , <code>backup-gateway:DeleteHypervisor</code> , <code>backup-gateway:DissociateGatewayFromServer</code> , <code>backup-gateway:ImportHypervisorConfiguration</code> , <code>backup-gateway:ListGateways</code> , <code>backup-gateway:ListHypervisors</code> , <code>backup-gateway:ListTagsForResource</code> , <code>backup-gateway:ListVirtualMachines</code> , <code>backup-gateway:PutMaintenanceStartTime</code> , <code>backup-gateway:TagResource</code> , <code>backup-gateway:TestHypervisorConfiguration</code> , <code>backup-gateway:UntagResource</code>	30 novembre 2021

Modifier	Description	Date
	e ,backup-gateway:UpdateGatewayInformation ,etbackup-gateway:UpdateHypervisor .	
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses machines virtuelles : backup-gateway:ListGateways backup-gateway:ListHypervisors ,backup-gateway:ListTagsForResource ,etbackup-gateway:ListVirtualMachines .	30 novembre 2021
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajouté dynamodb:ListTagsOfResource pour accorder à l'utilisateur l'autorisation de répertorier les balises de ses tables DynamoDB à sauvegarder à l'aide des fonctionnalités de sauvegarde avancées AWS Backup de DynamoDB.	23 novembre 2021

Modifier	Description	Date
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Ajouté dynamodb : <code>StartAwsBackupJob</code> pour accorder à l'utilisateur l'autorisation de sauvegarder ses tables DynamoDB à l'aide de fonctionnalités de sauvegarde avancées. Ajouté dynamodb : <code>ListTagsOfResource</code> pour accorder à l'utilisateur l'autorisation de copier des balises depuis ses tables DynamoDB source vers ses sauvegardes.	23 novembre 2021
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajouté dynamodb : <code>RestoreTableFromAwsBackup</code> pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs tables DynamoDB sauvegardées à l'aide des fonctionnalités AWS Backup de sauvegarde avancées de DynamoDB.	23 novembre 2021

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajouté dynamodb : RestoreTableFromAWSBackup pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs tables DynamoDB sauvegardées à l'aide des fonctionnalités AWS Backup de sauvegarde avancées de DynamoDB.	23 novembre 2021
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les actions ont été supprimées backup:GetRecoveryPointRestoreMetadata et rds:DescribeDBSnapshots parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux backup:GetRecoveryPointRestoreMetadata et backup:Get* dans le cadre deAWSBackupOperatorAccess . De plus, AWS Backup ne n'avait pas besoin des deux rds:DescribeDBSnapshots et dans rds:describeDBSnapshots le cadre deAWSBackupOperatorAccess .	23 novembre 2021

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout des nouvelles actions <code>elasticfilesystem:DescribeFileSystems</code>, <code>dynamodb:ListTables</code>, <code>storagegateway:ListVolumes</code>, <code>ec2:DescribeVolumes</code>, <code>ec2:DescribeInstances</code>, <code>rds:DescribeDBInstances</code>, <code>rds:DescribeDBClusters</code>, et <code>fsx:DescribeFileSystems</code> pour permettre aux clients de consulter et de choisir parmi une liste de leurs ressources AWS Backup prises en charge lors de la sélection des ressources à affecter à un plan de sauvegarde.	10 novembre 2021
AWSBackupAuditAccess : nouvelle politique	Ajouté <code>AWSBackupAuditAccess</code> pour accorder à l'utilisateur l'autorisation d'utiliser AWS Backup Audit Manager. Les autorisations incluent la possibilité de configurer des frameworks de conformité et de générer des rapports.	24 août 2021

Modifier	Description	Date
AWSServiceRolePolicyForBackupReports : nouvelle politique	Ajouté <code>AWSServiceRolePolicyForBackupReports</code> pour accorder des autorisations pour un rôle lié à un service afin d'automatiser la surveillance des paramètres de sauvegarde, des tâches et des ressources afin de garantir la conformité avec les frameworks configurés par l'utilisateur.	24 août 2021
AWSBackupFullAccess : mise à jour d'une politique existante	Ajouté <code>iam:CreateServiceLinkedRole</code> pour créer un rôle lié à un service (dans la mesure du possible) afin d'automatiser la suppression des points de récupération expirés pour vous. Sans ce rôle lié au service, il est AWS Backup impossible de supprimer les points de récupération expirés une fois que les clients ont supprimé le rôle IAM d'origine qu'ils ont utilisé pour créer leurs points de récupération.	5 juillet 2021

Modifier	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout de la nouvelle action permettant d' <code>dynamodb:DeleteBackupDeleteRecoveryPoint</code> autoriser l'automatisation de la suppression des points de restauration DynamoDB expirés en fonction des paramètres du cycle de vie de votre plan de sauvegarde.	5 juillet 2021
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les actions ont été supprimées <code>backup:GetRecoveryPointRestoreMetadata</code> et <code>rds:DescribeDBSnapshots</code> parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux <code>backup:GetRecoveryPointRestoreMetadata</code> et, dans <code>backup:Get*</code> le cadre de <code>AWSBackupOperatorAccess</code>. Also, AWS Backup n'avait pas besoin des deux <code>rds:DescribeDBSnapshots</code> et dans <code>rds:describeDBSnapshots</code> le cadre de <code>AWSBackupOperatorAccess</code>.	25 mai 2021

Modifier	Description	Date
AWSBackupOperatorAccess : mise à jour d'une politique existante	Les actions ont été supprimées <code>backup:GetRecoveryPointRestoreMetadata</code> et <code>rds:DescribeDBSnapshots</code> parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux <code>backup:GetRecoveryPointRestoreMetadata</code> et <code>backup:Get*</code> dans le cadre de <code>AWSBackupOperatorAccess</code>. De plus, AWS Backup ne n'avait pas besoin des deux <code>rds:DescribeDBSnapshots</code> et dans <code>rds:describeDBSnapshots</code> le cadre de <code>AWSBackupOperatorAccess</code>.	25 mai 2021
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout de la nouvelle action <code>fsx:TagResource</code> permettant d'accorder <code>StartRestoreJob</code> l'autorisation d'appliquer des balises aux systèmes de FSx fichiers Amazon pendant le processus de restauration.	24 mai 2021

Modifier	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Ajout des nouvelles actions <code>ec2:DescribeImages</code> et <code>ec2:DescribeInstances</code> <code>StartRestoreJob</code> autorisation vous permettant de restaurer des EC2 instances Amazon à partir de points de récupération.	24 mai 2021
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Ajout de la nouvelle action <code>fsx:CopyBackup</code> pour accorder <code>StartCopyJob</code> l'autorisation de copier les points de FSx récupération Amazon entre les régions et les comptes.	12 avril 2021
AWSBackupServiceLinkedRolePolicyForBackup : mise à jour d'une politique existante	Ajout de la nouvelle action <code>fsx:CopyBackup</code> pour accorder <code>StartCopyJob</code> l'autorisation de copier les points de FSx récupération Amazon entre les régions et les comptes.	12 avril 2021
AWSBackupServiceRolePolicyForBackup : mise à jour d'une politique existante	Mis à jour pour répondre aux exigences suivantes : AWS Backup Pour créer une sauvegarde d'une table DynamoDB chiffrée, vous devez ajouter les <code>kms:Decrypt</code> autorisations <code>kms:GenerateDataKey</code> et le rôle IAM utilisé pour la sauvegarde.	10 mars 2021

Modifier	Description	Date
AWSBackupFullAccess : mise à jour d'une politique existante	Mis à jour pour répondre aux exigences suivantes : À utiliser AWS Backup pour configurer des sauvegardes continues pour votre base de données Amazon RDS, vérifiez que l'autorisation d'API <code>rds:ModifyDBInstance</code> existe dans le rôle IAM défini par la configuration de votre plan de sauvegarde. Pour restaurer les sauvegardes continues Amazon RDS, vous devez ajouter l'autorisation <code>rds:RestoreDBInstanceToPointInTime</code> au rôle IAM que vous avez soumis pour la tâche de restauration. Dans la AWS Backup console, pour décrire la plage de temps disponible pour la point-in-time restauration, vous devez inclure l'autorisation d'<code>rds:DescribeDBInstanceAutomatedBackups</code> API dans votre politique gérée par IAM.	10 mars 2021

Modifier	Description	Date
AWS Backup a commencé à suivre les modifications	AWS Backup a commencé à suivre les modifications apportées à ses politiques AWS gérées.	10 mars 2021

Utilisation des rôles liés à un service pour AWS Backup

AWS Backup utilise des Gestion des identités et des accès AWS rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Rubriques

- [Utilisation de rôles pour sauvegarder et copier](#)
- [Utilisation des rôles pour AWS Backup Audit Manager](#)
- [Utilisation des rôles pour les tests de la restauration](#)

Utilisation de rôles pour sauvegarder et copier

AWS Backup utilise des Gestion des identités et des accès AWS rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#) et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé `AWSServiceRoleForBackup` pour créer et supprimer des sauvegardes de vos AWS ressources en votre nom.

Le rôle `AWSService RoleForBackup` lié à un service fait confiance aux services suivants pour assumer le rôle :

- `backup.amazonaws.com`

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSBackupServiceLinkedRolePolicyforBackup](#) à la référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous listez des ressources à sauvegarder, que vous configurez une sauvegarde entre comptes ou que vous effectuez des sauvegardes dans le AWS Management Console AWS CLI, le ou l' AWS API, vous AWS Backup créez le rôle lié au service pour vous.

Important

Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter [Un nouveau rôle est apparu dans mon compte IAM](#).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous listez des ressources à sauvegarder, que vous configurez une sauvegarde entre comptes ou que vous effectuez des sauvegardes, vous AWS Backup créez à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle AWSService RoleForBackup lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Tout d'abord, vous devez supprimer tous vos points de récupération. Ensuite, vous devez supprimer tous vos coffres-forts de sauvegarde.

Note

Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSService RoleForBackup (console)

1. Pour supprimer tous vos points de restauration et coffres-forts de sauvegarde (à l'exception de votre coffre-fort par défaut), suivez la procédure décrite dans [Supprimer un coffre-fort](#).
2. Pour supprimer votre coffre-fort par défaut, utilisez la commande suivante dans l' AWS CLI :

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

Pour supprimer AWS Backup les ressources utilisées par le AWSService RoleForBackup (AWS CLI)

1. Pour supprimer tous vos points de récupération, utilisez [delete-recovery-point](#).

2. Pour supprimer tous vos coffres-forts de sauvegarde, utilisez [delete-backup-vault](#).

Pour supprimer AWS Backup les ressources utilisées par AWSService RoleForBackup (API)

1. Pour supprimer tous vos points de récupération, utilisez [DeleteRecoveryPoint](#).
2. Pour supprimer tous vos coffres-forts de sauvegarde, utilisez [DeleteBackupVault](#).

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSService RoleForBackup service. Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Fonctionnalités et régions prises en charge par AWS Backup](#).

Utilisation des rôles pour AWS Backup Audit Manager

AWS Backup utilise des Gestion des identités et des accès AWS rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#) et recherchez les services avec un Oui dans la

colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé `AWSServiceRoleForBackupReports`— Permet de créer AWS Backup des contrôles, des cadres et des rapports.

Le rôle `AWSService RoleForBackupReports` lié à un service fait confiance aux services suivants pour assumer le rôle :

- `reports.backup.amazonaws.com`

Pour voir les autorisations de cette stratégie, consultez [AWSServiceRolePolicyForBackupReports](#) dans le AWS Guide de référence des stratégies gérées par.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un framework ou un plan de rapport dans le AWS Management Console, le AWS CLI ou l' AWS API, vous AWS Backup créez le rôle lié au service pour vous.

Important

Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter [Un nouveau rôle est apparu dans mon compte IAM](#).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un framework ou un plan de rapport, AWS Backup crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle `AWSService RoleForBackupReports` lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car

plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, voir [Modifier la description d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Vous devez supprimer tous les frameworks et plans de rapports.

Note

Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSService RoleForBackupReports (console)

1. Pour supprimer tous les frameworks, consultez [Suppression des cadres](#).
2. Pour supprimer tous les plans de rapport, consultez [Suppression de plans de rapport](#).

Pour supprimer AWS Backup les ressources utilisées par le AWSService RoleForBackupReports (AWS CLI)

1. Pour supprimer tous les cadres, utilisez [delete-framework](#).
2. Pour supprimer tous les plans de rapport, utilisez [delete-report-plan](#).

Pour supprimer AWS Backup les ressources utilisées par AWSService RoleForBackupReports (API)

1. Pour supprimer tous les frameworks, utilisez [DeleteFramework](#).
2. Pour supprimer tous les plans de rapport, utilisez [DeleteReportPlan](#).

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForBackupReports service. Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Fonctionnalités et régions prises en charge par AWS Backup](#).

Utilisation des rôles pour les tests de la restauration

AWS Backup utilise des Gestion des identités et des accès AWS rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#) et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé AWSServiceRoleForBackupRestoreTesting— Fournit des autorisations de sauvegarde pour effectuer des tests de restauration.

Le rôle lié à un service AWSServiceRoleForBackupRestoreTesting approuve les services suivants pour endosser le rôle :

- `restore-testing.backup.amazonaws.com`

Pour voir les autorisations de cette stratégie, consultez

[AWSServiceRolePolicyForBackupRestoreTesting](#) dans le AWS Guide de référence des stratégies gérées par.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous effectuez des tests de restauration dans le AWS Management Console AWS CLI, le ou l' AWS API, vous AWS Backup créez le rôle lié au service pour vous.

Important

Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter [Un nouveau rôle est apparu dans mon compte IAM](#).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous effectuez un test de restauration, AWS Backup crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle `AWSService RoleForBackupRestoreTesting` lié au service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez la section [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité

inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Vous devez supprimer tous les plans de test de la restauration.

Note

Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSService
RoleForBackupRestoreTesting (console)

- Pour supprimer tous les plans de test de la restauration, consultez [Tests de restauration](#).

Pour supprimer AWS Backup les ressources utilisées par le AWSService
RoleForBackupRestoreTesting (AWS CLI)

- Pour supprimer les plans de test de la restauration, utilisez `delete-restore-testing-plan`.

Pour supprimer AWS Backup les ressources utilisées par AWSService
RoleForBackupRestoreTesting (API)

- Pour supprimer les plans de test de la restauration, utilisez `DeleteRestoreTestingPlan`.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au
AWSServiceRoleForBackupRestoreTestingservice. Pour plus d'informations, consultez la section
[Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Fonctionnalités et régions prises en charge par AWS Backup](#).

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé à accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services auprès des principaux fournisseurs de services qui ont obtenu l'accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition [aws:SourceAccount](#) globale [aws:SourceArn](#) et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS Backup accordent un autre service à la ressource. Si vous utilisez les deux clés de contexte de condition globale, la valeur `aws:SourceAccount` et le compte de la valeur `aws:SourceArn` doit utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de stratégie.

La valeur de `aws:SourceArn` doit être un AWS Backup coffre-fort lorsque vous l'utilisez AWS Backup pour publier des sujets Amazon SNS en votre nom.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws::servicename::123456789012:*`.

L'exemple de politique suivant montre comment vous pouvez utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale AWS Backup pour éviter le problème de confusion des adjoints. Cette politique accorde au principal de service `backup-storage.amazonaws.com` la capacité d'effectuer des actions KMS uniquement lorsque le principal de service agit pour le compte 123456789012 sur les coffres-forts de sauvegarde : AWS

Sécurité de l'infrastructure dans AWS Backup

En tant que service géré, AWS Backup il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière AWS dont l'infrastructure est protégée, consultez [AWS Cloud Security](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Backup via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Intégrité des données dans AWS Backup

AWS Backup objectif d'intégrité des données

AWS Backup cherche à maintenir l'intégrité lors de la transmission, du stockage et du traitement de vos données. AWS Backup traite les données des ressources stockées comme des informations critiques indépendantes du contenu, dans la mesure où nous offrons le même niveau élevé de sécurité aux clients, quel que soit le type de données que vous stockez. Nous sommes vigilants quant à la sécurité de nos clients et avons mis en place des mesures techniques et physiques sophistiquées contre les accès non autorisés. Vous gardez le contrôle total sur la manière dont vos données sont classées, sur les régions dans lesquelles vous les stockez et sur la manière dont vous contrôlez, archivez et protégez vos données contre toute divulgation.

AWS Backup implémentation de l'intégrité des données

AWS Backup travaille de concert avec d'autres services AWS et Amazon pour préserver l'intégrité des données qu'il stocke et avec lesquelles il interagit. Les outils utilisés peuvent varier et peuvent inclure (sans s'y limiter) :

- Validation continue des objets par rapport au total de contrôle pour empêcher la corruption des objets
- Taux de contrôle internes pour confirmer l'intégrité des données en transit et au repos
- Taux de contrôle calculés sur les données contenues dans les sauvegardes créées à partir du magasin principal
- Tentative automatique de restauration des niveaux normaux de redondance du stockage d'objets en cas de corruption du disque ou de détection d'une défaillance de l'appareil
- Stockage redondant des données sur plusieurs sites physiques
- Amélioration de la durabilité des objets sur plusieurs zones de disponibilité lors de l'écriture initiale, associée à une réplication ultérieure en cas d'indisponibilité de l'appareil ou de détection d'une corruption des bits
- Taux de contrôle sur l'ensemble du trafic réseau pour détecter la corruption des paquets de données lors du stockage ou de la récupération de données

AWS Backup stocke nativement les données pour Amazon DynamoDB avec des fonctionnalités avancées, Amazon EFS, Amazon S3, Amazon Timestream et les machines virtuelles exécutées avec Connected via la passerelle Backup. VMware AWS Backup facilite les sauvegardes des données stockées avec d'autres services, notamment Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon, Amazon pour Windows File Server, EC2 FSx Amazon pour Lustre, Amazon pour OpenZFS, FSx FSx Amazon pour FSx ONTAP NetApp , Amazon Neptune, Amazon RDS et Amazon Redshift.

Confirmation objective et audit de l'intégrité des données AWS Backup

Les données stockées directement par AWS Backup et celles stockées en partenariat avec les autres AWS services avec lesquels ils AWS Backup interagissent sont soumises au processus rigoureux d'Amazon Simple Storage Service (Amazon S3) qui sous-tend cette intégrité des données. Cette intégrité est confirmée par un auditeur tiers indépendant par le biais d'un rapport d'audit annuel du SOC disponible via [AWS Artifact](#).

Retenues légales et AWS Backup

Vue d'ensemble de la conservation légale

Une conservation légale est un outil administratif qui permet d'empêcher la suppression de sauvegardes pendant une conservation. Tant que la conservation est en place, les sauvegardes

sous conservation ne peuvent pas être supprimées et les politiques de cycle de vie susceptibles de modifier le statut des sauvegardes (comme le passage à un état `Deleted`) sont retardées jusqu'à ce que la conservation légale soit levée.

Des blocages légaux peuvent être appliqués à une ou plusieurs sauvegardes (également appelées points de restauration) créées AWS Backup si leur cycle de vie le permet. Les blocages légaux ne s'appliquent pas aux [sauvegardes continues](#).

Lorsqu'une conservation légale est créée, elle peut prendre en compte des critères de filtrage spécifiques, tels que les types de ressources et les ressources IDs. En outre, vous pouvez définir la plage de dates de création des sauvegardes que vous souhaitez inclure dans une conservation légale.

Les conservations légales ne s'appliquent qu'à la sauvegarde d'origine sur laquelle elles sont placées. Lorsqu'une sauvegarde est copiée entre régions ou comptes (si la ressource la prend en charge), elle n'est pas conservée ni conservée légalement. Une conservation légale, comme d'autres ressources, possède un ARN (Amazon Resource Name) unique qui lui est associé. Seuls les points de récupération créés par AWS Backup peuvent faire partie d'une détention légale.

Notez que si [AWS Backup Vault Lock](#) fournit des protections et une immuabilité supplémentaires à un coffre-fort, une conservation légale fournit une protection supplémentaire contre la suppression de sauvegardes individuelles (points de restauration). La conservation légale n'expire pas et les données de la sauvegarde sont conservées indéfiniment. La suspension reste active jusqu'à ce qu'elle soit levée par un utilisateur disposant des autorisations suffisantes.

Maintenances légales multiples

Une sauvegarde peut avoir plusieurs conservations légales. Les mises en attente légales et les sauvegardes sont liées à plusieurs, ce qui signifie qu'une sauvegarde peut avoir plus qu'une conservation légale et qu'une conservation légale peut inclure plusieurs sauvegardes.

Une sauvegarde ne peut pas être supprimée tant qu'elle est légalement conservée. Une fois toutes les restrictions légales sur une sauvegarde supprimées, celle-ci est soumise à ses propriétés de cycle de conservation. Maintenez au moins un blocage légal pour empêcher la suppression des sauvegardes. Des blocages légaux peuvent être appliqués à un point de restauration conservé après sa date de conservation du cycle de vie de sauvegarde (en raison d'un blocage légal existant).

Chaque compte peut avoir un maximum de 50 conservations légales actives à un moment donné.

Création d'une conservation légale

Une sauvegarde légale peut être ajoutée à une sauvegarde existante (point de restauration).

Les sauvegardes (points de récupération) dont le statut est EXPIRED ou DELETING ne seront pas incluses dans la conservation légale. Les points de récupération (sauvegardes) dont le statut est CREATING peuvent ne pas être inclus dans la conservation légale, selon le moment où ils sont terminés.

Des blocages légaux peuvent être ajoutés par les utilisateurs disposant des autorisations IAM requises.

Création d'une conservation légale juridique à l'aide de la console

Pour créer une conservation légale

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le tableau de bord situé à gauche de la console, trouvez Mon compte. Choisissez Legal Holds.
3. Choisissez Ajouter une conservation légale.
4. Trois panneaux s'affichent : Détails de la conservation légale, étendue de la conservation légale et balises de conservation légales.
 - a. Sous Détails relatifs à la conservation légale, entrez le titre de la conservation légale et une description de la conservation dans les zones de texte prévues à cet effet.
 - b. Dans le panneau Portée de la conservation légale, choisissez la manière dont vous souhaitez sélectionner la ressource à inclure dans la conservation légale. Lorsque vous créez une suspension, vous choisissez la méthode utilisée pour sélectionner les ressources relevant de la retenue légale. Vous pouvez choisir d'inclure l'une des méthodes suivantes :
 - types de ressources spécifiques et IDs
 - Sélectionnez les coffres-forts de sauvegarde
 - Tous les types de ressources ou tous les coffres-forts de sauvegarde de votre compte
 - c. Spécifiez la plage de dates de votre conservation légale. Entrez les dates au format YYYY:MM:DD (les dates sont inclusives).
 - d. Vous pouvez éventuellement ajouter des balises pour la mise en attente sous Balises de conservation légales. Les balises peuvent aider à classer la conservation pour une référence et une organisation futures. Vous pouvez ajouter jusqu'à 50 balises au total.

5. Lorsque vous êtes satisfait de la configuration de votre nouvelle conservation légale, cliquez sur le bouton Ajouter une nouvelle conservation.

Créez une conservation légale à l'aide du AWS CLI

Vous pouvez créer une suspension légale à l'aide de la [create-legal-hold](#) commande.

```
aws backup create-legal-hold --title "my title" \  
  --description "my description" \  
  --recovery-point-selection  
  "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Affichage des conservations légales

Vous pouvez consulter les informations relatives à la conservation légale dans la AWS Backup console ou par programmation.

Afficher les réservations légales à l'aide de la console

Pour consulter toutes les conservations légales d'un compte à l'aide de la console Backup,

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans la partie gauche du tableau de bord, sous Mon compte, cliquez sur Conservations légales.
3. La table conservation légale affiche le titre, le statut, la description, l'ID et la date de création des conservations existantes. Cliquez sur le carat (flèche vers le bas) à côté de l'en-tête de la table pour filtrer la table en fonction de la colonne sélectionnée.

Affichage des conservations légales par programmation

Pour afficher tous les blocages légaux par programmation, vous pouvez utiliser les appels d'API suivants : [ListLegalHoldset](#). [GetLegalHold](#)

Le modèle JSON suivant peut être utilisé pour `GetLegalHold`.

```
GET /legal-holds/{legalHoldId} HTTP/1.1
```

Request

empty body

Response

```
{
  Title: string,
  Status: LegalHoldStatus,
  Description: string, // 280 chars max
  CancelDescription: string, // this is provided during cancel // 280 chars max
  LegalHoldId: string,
  LegalHoldArn: string,
  CreatedTime: number,
  CanceledTime: number,

  ResourceSelection: {
    VaultArns: [ string ]
    Resources: [ string ]
  },
  ResourceFilters: {
    DateRange: {
      FromDate: number,
      ToDate: number
    }
  }
}
```

Le modèle JSON suivant peut être utilisé pour `ListLegalHolds`.

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken
```

Request

empty body

url params:

```
MaxResults: number // optional,
NextToken: string // optional
```

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING

maxResults: 1-1000

Response

```
{
  NextToken: token,
  LegalHold: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]
}
```

Les valeurs d'état possibles sont les suivantes.

Status	Description
CRÉATION	Les points de récupération demandés sont en cours de conservation et les demandes de suppression de ces points de récupération peuvent réussir puisque la création de la conservation n'est pas terminée.
ACTIF	La conservation légale a été créée. Tous les points de récupération répertoriés dans le cadre de cette conservation légale sont conservés.
ANNULATION	Les conservations légales sont en cours de suppression et les demandes de suppression des points de récupération conservés peuvent aboutir.

Status	Description
ANNULÉE	La conservation légale est entièrement libérée et n'a plus aucun effet. Les points de récupération peuvent être supprimés.

Libération d'une conservation légale

Les blocages légaux restent en vigueur jusqu'à ce qu'ils soient supprimés par un utilisateur disposant des autorisations suffisantes. La suppression d'une conservation légale est également connue sous le nom d'annulation, de suppression ou de libération d'une conservation légale. La suppression d'une conservation légale l'élimine de toutes les sauvegardes auxquelles elle était attachée. Toutes les sauvegardes qui ont expiré pendant la période de conservation légale sont supprimées dans les 24 heures suivant la levée de la suspension légale.

Libération d'une conservation légale à l'aide de la console

Pour relâcher un blocage à l'aide de la console

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Entrez la description que vous souhaitez associer à la version.
3. Vérifiez les détails, puis cliquez sur Lever la conservation.
4. Lorsque la boîte de dialogue Lever la conservation apparaît, confirmez votre intention de lever la conservation en saisissant `confirm` dans la zone de texte.
 - Cochez la case indiquant que vous annulez la conservation.

Sur la page Conservations légales, vous pouvez voir toutes vos conservations. Si la libération est réussie, le statut de cette conservation sera affiché comme `Released`.

Libérer une suspension légale par le biais d'un programme

Pour supprimer une conservation par programmation, utilisez l'appel d'API [CancelLegalHold](#).

Utilisez le modèle JSON suivant.

```
DELETE /legal-holds/{legalHoldId}
```

Request

```
{
  CancelDescription: String
  DeleteAfterDays: number // optional
}
```

DeleteAfterDays: optional.

Defaults to 180 days. how long to keep legal hold record after canceled.

This applies to the actual legal hold record only.

Recovery points are unlocked as soon as cancelation processes and are not subject to this date.

Response

Empty body

200 if successful

other standard codes

Protection contre les logiciels malveillants dans AWS Backup

L'analyse des programmes malveillants de vos sauvegardes est assurée par Amazon GuardDuty Malware Protection. L'utilisation d'Amazon GuardDuty Malware Protection pour vos AWS Backup permet d'automatiser l'analyse des points de restauration via les flux de travail de sauvegarde existants ou de lancer des analyses à la demande de sauvegardes créées précédemment. Cette solution AWS native permet de garantir que vos sauvegardes sont exemptes de logiciels malveillants potentiels, ce qui vous permet de répondre aux exigences de conformité et de répondre plus rapidement aux incidents malveillants en garantissant la restauration de données propres.

Pour consulter la liste des types de ressources et des régions pris en charge, consultez la [page de disponibilité des fonctionnalités](#).

Rubriques

- [Intégration avec Amazon GuardDuty](#)
- [Backup des autorisations d'accès instantanées](#)
- [Comment utiliser l'analyse des logiciels malveillants](#)
- [Accès](#)

- [Analyses incrémentielles ou complètes](#)
- [Surveillance de vos analyses de malwares](#)
- [Comprendre les résultats du scan](#)
- [Résolution des problèmes de numérisation](#)
- [Mesure](#)
- [Quotas](#)
- [Étapes d'utilisation de la console et de la CLI pour les types d'analyse des programmes malveillants](#)

Intégration avec Amazon GuardDuty

AWS Backup s'intègre à Amazon GuardDuty Malware Protection pour détecter les menaces pour vos points de récupération. Lorsque vous lancez une analyse des programmes malveillants, l'`StartMalwareScanAPI` d'Amazon GuardDuty est AWS Backup automatiquement appelée une fois chaque sauvegarde terminée, en transmettant les détails du point de restauration et les informations d'identification de votre rôle de scanner. Amazon commence GuardDuty ensuite à lire, déchiffrer et analyser tous les fichiers et objets contenus dans la sauvegarde.

Lorsque Amazon GuardDuty accède à vos données de sauvegarde, cet accès est connecté AWS CloudTrail pour des raisons de visibilité.

Pour plus d'informations sur cette intégration, consultez la [documentation Amazon GuardDuty Malware Protection](#).

Backup des autorisations d'accès instantanées

Lorsque vous utilisez Amazon GuardDuty Malware Protection for AWS Backup avec des sauvegardes S3, Amazon GuardDuty accède à vos sauvegardes S3 par trois APIs moyens : `CreateBackupAccessPoint`, `DescribeBackupAccessPoint`, et `DeleteBackupAccessPoint`.

Amazon GuardDuty utilise `CreateBackupAccessPoint` pour accéder à vos données de sauvegarde cryptées. Au cours de la tâche de numérisation, GuardDuty permet `DescribeBackupAccessPoint` de vérifier la réussite de la création du point d'accès. Une fois l'analyse terminée, GuardDuty des appels `DeleteBackupAccessPoint` lui demandent de supprimer son accès à votre sauvegarde.

Ce flux de travail s'applique à la fois aux sauvegardes S3 et aux sauvegardes EC2 /EBS stockées dans un coffre-fort à espacement logique.

Comment utiliser l'analyse des logiciels malveillants

Lorsque vous utilisez Amazon GuardDuty Malware Protection avec AWS Backup, vous pouvez analyser automatiquement vos sauvegardes pour détecter la présence de logiciels malveillants. Cette intégration vous permet de détecter le code malveillant dans vos sauvegardes et d'identifier des points de restauration propres pour les opérations de restauration.

Amazon GuardDuty Malware Protection prend en charge deux flux de travail principaux pour analyser vos sauvegardes :

- **Analyse automatique des programmes malveillants via des plans de sauvegarde** : activez l'analyse des logiciels malveillants dans les plans de sauvegarde pour automatiser la détection des logiciels malveillants avec AWS Backup. Lorsque cette option est activée, lance AWS Backup automatiquement un GuardDuty scan Amazon après chaque sauvegarde réussie. Vous pouvez configurer une analyse complète ou incrémentielle pour des règles de plan de sauvegarde spécifiques, qui déterminent la fréquence d'analyse de vos sauvegardes. Pour plus d'informations sur les types de numérisation, voir [the section called “Analyses incrémentielles ou complètes”](#) ci-dessous. AWS Backup recommande d'activer l'analyse automatique des programmes malveillants dans les plans de sauvegarde pour une détection proactive des menaces après la création de la sauvegarde.
- **Analyses à la demande** : exécutez des analyses à la demande pour analyser manuellement les sauvegardes existantes, en choisissant entre des types d'analyse complets ou incrémentiels. AWS Backup recommande d'utiliser des analyses à la demande pour identifier votre dernière sauvegarde propre. Lorsque vous effectuez une analyse avant une opération de restauration, utilisez une analyse complète pour examiner l'intégralité de la sauvegarde à l'aide du dernier modèle de détection des menaces.

Accès

Avant de commencer à utiliser la protection contre les logiciels malveillants, votre compte doit disposer des autorisations requises pour les opérations.

AWS Backup l'analyse des programmes malveillants nécessite deux rôles IAM pour analyser vos points de récupération à la recherche de logiciels malveillants potentiels :

- Tout d'abord, la politique `AWSBackupServiceRolePolicyForScans` gérée doit être attachée à votre rôle de sauvegarde existant ou nouveau. Il s'agit du même rôle que celui que l'on trouve dans l'attribution des ressources pour votre plan de sauvegarde dans la console ou via l'[BackupSelection](#)

[API](#). Cette politique gérée permet de AWS Backup lancer des analyses de malwares avec Amazon GuardDuty.

- Ensuite, un nouveau rôle de scanner est requis avec une politique `AWSBackupGuardDutyRolePolicyForScans` gérée qui fait confiance `malware-protection.guarddduty.amazonaws.com`. Il s'agit du même rôle que celui que l'on trouve dans la section de protection contre les programmes malveillants de votre plan de sauvegarde dans la console ou dans les paramètres d'analyse de votre [BackupPlan API](#). Ce rôle est transmis AWS Backup à Amazon GuardDuty lorsqu'une analyse est lancée, ce qui permet d'accéder aux sauvegardes.

Analyses incrémentielles ou complètes

Avec l'analyse des programmes malveillants, vous avez le choix entre des analyses incrémentielles ou complètes en fonction de vos exigences en matière de sécurité et de considérations financières.

Les scans incrémentiels analysent uniquement les données modifiées entre le point de récupération cible et le point de récupération de base. Ces analyses sont plus rapides et plus économiques pour les analyses régulières, ce qui les rend idéales pour les sauvegardes périodiques fréquentes où vous souhaitez analyser des données récemment sauvegardées.

Même lorsque l'analyse incrémentielle est sélectionnée, AWS Backup effectue une analyse complète dans les situations suivantes :

- **Analyses initiales** : l'analyse initiale d'une ressource est toujours une analyse complète, ce qui permet GuardDuty à Amazon d'établir une base de référence des menaces potentielles. Les scans suivants seront alors incrémentiels.
- **Base de référence expirée** : si votre point de récupération de référence a été scanné il y a plus de 90 jours, une analyse complète est effectuée. Amazon ne GuardDuty conservant les informations de recherche que pendant 90 jours, une nouvelle base de référence doit être établie pour garantir des résultats d'analyse précis.
- **Base de référence supprimée** : si votre point de récupération de base est supprimé avant le début de votre prochaine analyse incrémentielle, une analyse complète est automatiquement effectuée.

Les scans complets examinent l'intégralité du point de restauration, indépendamment des scans précédents. Bien que ces analyses fournissent une couverture complète, elles prennent plus de temps et entraînent des coûts plus élevés. Vous pouvez exécuter des analyses complètes à la

demande ou les planifier via vos plans de sauvegarde. AWS Backup recommande de configurer des analyses complètes périodiques dans vos plans de sauvegarde à des intervalles prolongés afin de garantir que l'ensemble de vos données de sauvegarde est régulièrement scanné avec le dernier modèle de signature de logiciel malveillant.

Pour une sécurité optimale par rapport à une gestion des coûts, tenez compte de la fréquence de vos sauvegardes lorsque vous choisissez les types de scan.

Note

L'analyse des programmes malveillants n'est actuellement pas prise en charge pour les points de restauration continue Amazon S3. Pour analyser les sauvegardes continues d'Amazon S3, configurez des sauvegardes périodiques pour vos ressources Amazon S3 et activez l'analyse des programmes malveillants sur ces sauvegardes périodiques. Vous pouvez utiliser une [combinaison de sauvegardes continues et périodiques](#) pour vos compartiments Amazon S3.

Note

L'analyse incrémentielle des programmes malveillants n'est pas prise en charge pour les points de EC2 récupération Amazon situés dans un coffre-fort [isolé de manière logique ou pour les points de](#) récupération Amazon copiés. EC2

Surveillance de vos analyses de malwares

Une fois la numérisation activée, Amazon AWS Backup et Amazon GuardDuty fournissent des mécanismes de surveillance et de notification que vous pouvez utiliser pour suivre vos résultats :

- **AWS Backup Console** : La AWS Backup console est alimentée par `ListScanJobs` et `DescribeScanJob` APIs. Vous pouvez consulter la section Protection contre les logiciels malveillants pour consulter la liste des tâches d'analyse, représentant l'état des tâches et les résultats de l'analyse. AWS Backup supporte également une `ListScanJobSummaries` API, bien qu'elle ne soit pas disponible dans la console.
- **AWS Backup Audit Manager** : vous pouvez configurer un rapport d'analyse pour afficher toutes les tâches d'analyse des programmes malveillants AWS Backup lancées au cours des dernières 24 heures.

- Amazon GuardDuty Console : si Amazon de base GuardDuty est activé, vous pouvez consulter les détails dans les résultats du Malware Scan et étudier les malwares sur la page des GuardDuty résultats d'Amazon. Vous pouvez consulter des informations telles que la menace et le nom du fichier, le chemin du fichier, objects/files le nombre d'octets scannés, etc. Notez que ces informations détaillées sur les menaces ne sont pas disponibles via AWS Backup et que vous devez disposer des GuardDuty autorisations Amazon appropriées pour consulter ces informations.
- Amazon EventBridge : Amazon AWS Backup et Amazon GuardDuty émettent EventBridge des événements, ce qui permet aux administrateurs de sauvegarde et de sécurité d'être alertés de manière synchrone. Vous pouvez configurer des règles personnalisées pour recevoir des notifications lorsque les analyses sont terminées ou qu'un logiciel malveillant est détecté.
- AWS CloudTrail: Amazon AWS Backup et Amazon GuardDuty émettent CloudTrail des événements, ce qui vous permet de surveiller l'accès aux API.

Comprendre les résultats du scan

Vos tâches de numérisation AWS Backup auront un état de numérisation et un résultat de numérisation.

États de numérisation

L'état de numérisation indique l'état de la tâche et peut prendre les valeurs suivantes : `CREATED`, `COMPLETED`, `COMPLETED_WITH_ISSUES`, `RUNNING`, `FAILED`, ou `CANCELED`.

Il existe plusieurs situations dans lesquelles votre tâche de numérisation se terminera avec l'état `COMPLETED_WITH_ISSUES` :

Pour les sauvegardes Amazon S3, il existe des `size/type` limitations relatives aux objets qui empêcheront l'analyse des objets. Lorsqu'au moins un objet est ignoré dans une analyse, la tâche de numérisation correspondante est marquée comme `COMPLETED_WITH_ISSUES`. Pour les sauvegardes Amazon EC2 /Amazon EBS, il existe des `size/quantity` limites de volume qui se traduisent par des volumes ignorés lors de la numérisation. Ces situations entraîneront la création d'une tâche de sauvegarde EC2 Amazon /Amazon EBS. `COMPLETED_WITH_ISSUES`

Si votre tâche se termine par un état `COMPLETED_WITH_ISSUES` et que vous avez besoin d'informations supplémentaires sur les raisons, vous devrez obtenir ces informations auprès de la tâche de numérisation correspondante via Amazon GuardDuty.

 Note

Les tâches d'analyse incrémentielle analysent uniquement la différence de données entre deux sauvegardes. Par conséquent, si une tâche d'analyse incrémentielle ne rencontre aucune des situations décrites ci-dessus, elle se terminera en état COMPLETE et n'héritera pas du point COMPLETED_WITH_ISSUES de récupération de base.

Dans de rares cas, Amazon GuardDuty peut rencontrer des problèmes internes lors de la numérisation de fichiers et d'objets, et les tentatives de nouvelle tentative peuvent être vaines. Dans ce cas, la tâche de numérisation apparaît comme FAILED dans AWS Backup et COMPLETED_WITH_ISSUES dans Amazon GuardDuty. Cette différence de statut vous permet de consulter les résultats de scan disponibles sur Amazon GuardDuty tout en indiquant que tous les fichiers et objets pris en charge n'ont pas été scannés avec succès.

Résultats du scan

Les résultats du scan indiquent un résultat agrégé provenant d'Amazon GuardDuty et peuvent avoir les valeurs suivantes :THREATS_FOUND, ouNO_THREATS_FOUND.

Les résultats de l'analyse indiquent si un logiciel malveillant potentiel a été détecté dans vos points de récupération. Un NO_THREATS_FOUND statut signifie qu'aucun logiciel malveillant potentiel n'a été détecté, tandis qu'THREATS_FOUNDun logiciel malveillant potentiel a été découvert. Pour obtenir des informations détaillées sur les menaces, accédez aux GuardDuty résultats complets d'Amazon via la GuardDuty console Amazon ou APIs. Les résultats du scan sont également disponibles par le biais d'EventBridge événements, ce qui vous permet de créer des flux de travail automatisés qui répondent aux sauvegardes infectées.

Amazon GuardDuty conserve les résultats pendant 90 jours, en suivant les fichiers ou les objets dans le cadre d'analyses incrémentielles afin de vérifier si les menaces sont supprimées ou si les signatures des logiciels malveillants changent. Par exemple, si un logiciel malveillant est détecté dans la sauvegarde 2, le résultat de l'analyse s'afficheTHREATS_FOUND. Lorsque vous effectuez une analyse incrémentielle sur la sauvegarde 3 en utilisant la sauvegarde 2 comme base, le résultat de l'analyse est conservé THREATS_FOUND sauf si la menace a été supprimée des données.

Résolution des problèmes de numérisation

Les échecs de scan courants incluent des autorisations IAM insuffisantes, des limites de service et des problèmes d'accès aux ressources.

Des erreurs d'autorisation se produisent lorsque le rôle de sauvegarde ne dispose pas d'`AWSBackupServiceRolePolicyForScans` autorisations ou lorsque le rôle de scanner n'`AWSBackupGuardDutyRolePolicyForScans` entretient pas de relations de confiance appropriées.

Des erreurs de limite de service se produisent lorsque vous dépassez les 150 analyses simultanées par compte ou 5 analyses simultanées par type de ressource. Les tâches de numérisation resteront en cours jusqu'à ce que la capacité soit disponible.

Les erreurs d'accès refusé peuvent indiquer des points de récupération chiffrés sans AWS KMS les autorisations appropriées ou des points de récupération parents supprimés pour des analyses incrémentielles.

Les délais d'expiration peuvent survenir avec de très grands points de restauration ou pendant des périodes de GuardDuty chargement Amazon élevées.

Pour résoudre le problème, vérifiez l'état de la tâche d'analyse à l'aide de `DescribeScanJobAPI`, vérifiez les configurations des rôles IAM, assurez-vous que les points de récupération existent et sont accessibles, et envisagez de passer aux analyses complètes si des références parentes de scan incrémentielles sont manquantes.

Surveillez votre utilisation simultanée des scans et implémentez l'instabilité dans les flux de travail automatisés afin d'éviter d'atteindre les limites de service.

Mesure

La protection contre les malwares est fournie et facturée par Amazon GuardDuty. Vous ne verrez aucun AWS Backup frais lié à l'utilisation de cette fonctionnalité. Toutes les utilisations peuvent être consultées sur la page GuardDuty de facturation d'Amazon. Pour en savoir plus, consultez la page [GuardDuty des tarifs Amazon](#).

Quotas

Amazon AWS Backup et Amazon GuardDuty ont tous deux fixé des limites de quotas pour Amazon GuardDuty Malware Protection pour AWS Backup.

Pour plus d'informations, consultez les pages [AWS Backup Quotas](#) et [Amazon GuardDuty Quotas](#).

Étapes d'utilisation de la console et de la CLI pour les types d'analyse des programmes malveillants

Les sections suivantes présentent les étapes de configuration des différents types de scan de programmes malveillants à l'aide de la console et AWS CLI.

Comment configurer les analyses de logiciels malveillants

Console

1. Accédez à la AWS Backup console → Plans de sauvegarde
2. Créez un nouveau plan de sauvegarde ou sélectionnez un plan existant
3. Activer le bouton de protection contre les logiciels malveillants
4. Sélectionnez le rôle de scanner pour choisir un nouveau rôle de scanner. Assurez-vous que le rôle de sauvegarde et le rôle de scanner disposent des autorisations appropriées, comme indiqué dans [the section called “Accès”](#).
5. Sélectionnez les types de ressources scannables. Cela filtrera l'analyse des logiciels malveillants en fonction des critères de sélection des ressources que vous avez choisis. Par exemple, si le type de ressource scannable que vous avez sélectionné est Amazon EBS, mais que la sélection de ressources de votre plan inclut Amazon EBS et Amazon S3, seules les analyses de malwares Amazon EBS auront lieu.
6. Définissez le type de scan pour chaque règle de sauvegarde. Vous pouvez choisir entre un scan complet, un scan incrémentiel ou un scan sans scan. La sélection du type de scan signifie que le scan aura lieu à la fréquence planifiée de la règle de sauvegarde associée.
7. Enregistrer le plan de sauvegarde

AWS CLI

CreateBackupPlan

Vous pouvez créer un plan de sauvegarde avec l'analyse des programmes malveillants activée à l'aide de la [create-backup-plan](#) commande.

```
aws backup create-backup-plan \  
  --region us-west-2 \  
  --cli-input-json '{
```

```

"BackupPlan": {
  "BackupPlanName": "scan-initial-test-demo",
  "Rules": [
    {
      "RuleName": "full",
      "TargetBackupVaultName": "Default",
      "ScheduleExpression": "cron(0 * * * ? *)",
      "StartWindowMinutes": 120,
      "CompletionWindowMinutes": 6000,
      "Lifecycle": {
        "DeleteAfterDays": 3,
        "OptInToArchiveForSupportedResources": true
      },
      "RecoveryPointTags": {
        "key1": "foo",
        "key2": "foo"
      },
      "EnableContinuousBackup": true,
      "ScanActions": [
        {
          "MalwareScanner": "GUARDDUTY",
          "ScanMode": "FULL_SCAN"
        }
      ]
    },
    {
      "RuleName": "incremental",
      "TargetBackupVaultName": "Default",
      "ScheduleExpression": "cron(30 * * * ? *)",
      "StartWindowMinutes": 100,
      "CompletionWindowMinutes": 5000,
      "Lifecycle": {
        "DeleteAfterDays": 2,
        "OptInToArchiveForSupportedResources": true
      },
      "RecoveryPointTags": {
        "key1": "foo",
        "key2": "foo"
      },
      "EnableContinuousBackup": true,
      "ScanActions": [
        {
          "MalwareScanner": "GUARDDUTY",
          "ScanMode": "INCREMENTAL_SCAN"
        }
      ]
    }
  ]
}

```

```

        }
      ]
    }
  ],
  "ScanSettings": [
    {
      "MalwareScanner": "GUARDDUTY",
      "ResourceTypes": ["EBS", "EC2", "S3"],
      "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
    }
  ]
}
}'

```

UpdateBackupPlan

Vous pouvez mettre à jour un plan de sauvegarde en activant l'analyse des programmes malveillants à l'aide de la [update-backup-plan](#) commande.

```

aws backup update-backup-plan \
  --region us-west-2 \
  --cli-input-json '{
    "BackupPlanId": "d1391282-68cf-4fce-93ad-e08bc5178bac",
    "BackupPlan": {
      "BackupPlanName": "scan-initial-test-demo",
      "Rules":
      [
        {"RuleName": "full",
          "TargetBackupVaultName": "Default",
          "ScheduleExpression": "cron(0 * * * ? *)",
          "StartWindowMinutes": 60,
          "CompletionWindowMinutes": 3000,
          "Lifecycle":
            {
              "DeleteAfterDays": 6,
              "OptInToArchiveForSupportedResources": false},
          "RecoveryPointTags":
            {"key1": "foo",
             "key2": "foo"},
          "EnableContinuousBackup": false,
          "ScanActions":
            [

```

```

        {"MalwareScanner": "GUARDDUTY",
         "ScanMode": "FULL_SCAN"}
    ],
    {
        "RuleName": "incremental",
        "TargetBackupVaultName": "Default",
        "ScheduleExpression": "cron(30 * * * ? *)",
        "StartWindowMinutes": 120,
        "CompletionWindowMinutes": 6000,
        "Lifecycle": {
            "DeleteAfterDays": 9,
            "OptInToArchiveForSupportedResources": false},
        "RecoveryPointTags": {
            "key1": "foo",
            "key2": "foo"},
        "EnableContinuousBackup": false,
        "ScanActions": [
            {
                "MalwareScanner": "GUARDDUTY",
                "ScanMode": "INCREMENTAL_SCAN"
            }
        ]
    }
],
"ScanSettings": [
    {
        "MalwareScanner": "GUARDDUTY",
        "ResourceTypes": ["ALL", "EBS"],
        "ScannerRoleArn": "arn:aws:iam::300949271314:role/
TestBackupScannerRole"
    }
]
}'

```

Remarques clés

- La saisie de l'ARN cible est requise avant que les options de scan ne soient activées (console)

- Le rôle IAM de sauvegarde et le rôle IAM de scanner sont requis pour toutes les configurations
- `aws backup list-scan-jobs` À utiliser pour afficher toutes les tâches de numérisation (AWS CLI)
- Les implications financières varient selon le type de numérisation (incrémentiel ou complet) et la fréquence

AWS CLI Remarques clés

- `aws backup list-scan-jobs` À utiliser pour afficher toutes les tâches de numérisation (AWS CLI)
- Résultats du scan disponibles via `describe-recovery-point` API avec `ScanResults` champ
- Le rôle IAM de sauvegarde et le rôle IAM de scanner sont requis pour toutes les configurations
- La structure du plan de sauvegarde JSON inclut `ScanSettings` au niveau du plan et `ScanActions` dans les règles

Résilience dans AWS Backup

AWS Backup prend très au sérieux sa résilience et la sécurité de vos données.

AWS Backup stocke vos sauvegardes avec au moins autant de résilience et de durabilité que le AWS service d'origine de votre ressource vous offrirait, si vous les sauvegardiez sur place.

AWS Backup est conçu pour utiliser l'infrastructure AWS mondiale afin de répliquer vos sauvegardes sur plusieurs zones de disponibilité pour une durabilité de 99,999999999 % (11 neuf) par année, à condition que vous respectiez la documentation en vigueur. AWS Backup

AWS Backup chiffre vos plans de sauvegarde au repos et les sauvegarde en permanence.

Vous pouvez également restreindre l'accès à vos plans de sauvegarde à l'aide des informations d'identification et des politiques Gestion des identités et des accès AWS (IAM). Pour plus d'informations, consultez [Authentification](#), [Contrôle d'accès](#) et [Bonnes pratiques de sécurité dans IAM](#).

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. AWS Backup stocke vos sauvegardes dans toutes les zones de disponibilité. Les zones de disponibilité sont davantage

disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données. Pour plus d'informations, consultez [Contrat de niveau de service \(SLA\)AWS Backup](#).

En outre, il AWS Backup vous permet de copier vos sauvegardes d'une région à l'autre pour une résilience encore plus grande. Pour plus d'informations sur la fonctionnalité de copie AWS Backup entre régions, voir [Création d'une copie de sauvegarde](#).

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

AWS Backup quotas

Les quotas suivants s'appliquent lorsque vous travaillez avec AWS Backup.

Quotas

- [Sauvegarde](#)
- [Index de sauvegarde et quotas de recherche](#)
- [Quotas de politiques](#)
- [Quotas d'analyse des logiciels](#)
- [Quotas de ressources Amazon Timestream](#)
- [AWS Backup Quotas d'Audit Manager](#)
- [Rétablir les quotas du plan de test](#)
- [AWS Backup gateway quotas](#)
- [Quotas Amazon EKS](#)
- [Quotas de coffre répartis de manière logique](#)
- [Quotas associés](#)

Sauvegarde

Name	Par défaut	Ajustable
Nombre total de coffres-forts (de sauvegarde et ventilés de manière logique) par région et par compte	300	Oui
Points de restauration par coffre-fort de sauvegarde	1 000 000	Oui
Plans de sauvegarde par région et par compte	300	Oui
Versions par plan de sauvegarde	2 000	Oui

Name	Par défaut	Ajustable
Affectations de ressources par plan de sauvegarde	100	Non
Compartiments Amazon S3 par compte	100	Oui
Tâches de copie interrégionales simultanées par compte dans la région de destination	100 ²	Non
Tâches de copie interrégionales supplémentaires par coffre-fort dans une région de destination une fois que la limite indiquée dans la ligne au-dessus de l'entrée a été atteinte. ¹	5 ²	Non
Copies multicomptes simultanées pouvant être réalisées de la même ressource vers la même région de destination	30	Non
Tâches de sauvegarde et de copie simultanées par ressource	1	Non
Tags par sélection de ressources dans une politique de sauvegarde entre comptes	30	Non Incluez des balises supplémentaires à l'aide de plusieurs affectations de ressources ou de plans de sauvegarde.
Hyperviseurs	20	Non

Name	Par défaut	Ajustable
Retenues légales par compte	50	Non
Couches de sauvegarde imbriquées dans les piles d'applications	10	Non

¹ La limite pour les tâches de copie simultanées d'une région à l'autre est de 100 par compte et par région. Une fois cette limite atteinte, si un coffre-fort spécifique de la région de destination comporte moins de 5 tâches de copie simultanées, de nouvelles tâches de copie peuvent commencer, jusqu'à un maximum de 5 simultanément.

² La limite s'applique uniquement aux types de ressources [entièrement gérés par AWS Backup](#).

Index de sauvegarde et quotas de recherche

Name	Par défaut	Ajustable
Tâches d'indexation simultanées en compte (la plupart Régions AWS)	40	Oui
Des emplois indexés simultanés sont pris en compte en Asie-Pacifique (Malaisie), au Canada (centre), en Asie-Pacifique (Thaïlande) et au Mexique (centre). Régions AWS	10	Oui
Tâches d'indexation simultanées pour chaque ressource	5	Non
Tâche d'indexation simultanée à la demande	1	Non

Name	Par défaut	Ajustable
Recherche simultanée d'emplois dans le compte	10	
Tâches d'exportation simultanées	5	
Nombre de points de récupération inclus dans la tâche de recherche	20	
Tâches de restauration simultanées au niveau des fichiers Amazon EBS (la plupart Régions AWS)	25	
Tâches de restauration simultanées au niveau des fichiers Amazon EBS en Asie-Pacifique (Malaisie), au Canada (centre), en Asie-Pacifique (Thaïlande) et au Mexique (centre). Régions AWS	5	

Quotas de politiques

Name	Par défaut	Ajustable
Affectations de ressources par plan de sauvegarde	100	Non
Tags dans une sélection de ressources	30	Non

Name	Par défaut	Ajustable
Sélections de ressources utilisant des balises dans un plan	10	Non
Règles du plan de sauvegarde dans un plan	10	Non
Balises ajoutées à un point de récupération	10	Non
Actions de copie par règle de sauvegarde	5	Non
Conditions d'attribution de ressources dans un plan de sauvegarde	30	Non

Quotas d'analyse des logiciels

Le tableau suivant répertorie les quotas pour l'analyse des AWS Backup programmes malveillants avec Amazon GuardDuty.

Name	Par défaut	Ajustable
Exécution de tâches de scan par ressource et par compte	5	Oui
Exécution de tâches de scan par point de restauration et par compte	1	Non
Exécution de tâches de scan par compte	150	Oui

Name	Par défaut	Ajustable
Tâches de numérisation créées par ressource et par compte	10	Non
Contrainte de base de numérisation incrémentielle	1	Non

Lorsque vous atteignez la limite de tâches de numérisation que vous avez créées par ressource et par compte, nous échouons à la tâche la plus ancienne en file d'attente.

Vous pouvez également rencontrer des quotas imposés par Amazon GuardDuty. Pour plus d'informations, consultez la section [GuardDuty Quotas Amazon](#) dans le Références générales AWS.

Quotas de ressources Amazon Timestream

Name	Par défaut	Ajustable
Tâches de sauvegarde Timestream simultanées par compte	4	Oui
Tâches de restauration Timestream simultanées par compte	1	Oui

AWS Backup Quotas d'Audit Manager

Name	Par défaut	Ajustable
Cadres par compte et par région	15	Oui
Contrôles par compte et par région	50	Oui

Name	Par défaut	Ajustable
Déclarer les plans par compte	20	Oui
Cadres par plan de rapport	1 000	Non
[Nombre de comptes] multiplié par [nombre de régions dans un plan de rapport]	300	Non
[Nombre de comptes] multiplié par [nombre de régions dans un plan de rapport] multiplié par [nombre d'emplois quotidiens plus évaluations dans un plan de rapport]	100 000	Non

Rétablir les quotas du plan de test

Name	Par défaut	Ajustable
Plans de tests de la restauration	100	Non
Tags par plan	50	Non
Sélections par plan	30	Non
ARNs par sélection de tests de restauration	30	Non
Conditions par sélection (à la fois <code>StringEquals</code> et <code>StringNotEquals</code>)	30	Non

Name	Par défaut	Ajustable
Sélecteurs de coffre-fort par sélection de tests de la restauration	30	Non
Valeur maximale (en jours) de la fenêtre de sélection	365 jours	Non
Limites des heures de la fenêtre de démarrage	Minimum : 1 heure ; maximum : 168 heures	Non
Nombre maximal de caractères pour le nom du plan de tests de la restauration	50 caractères (alphanumériques et traits de soulignement, pas d'espaces blancs)	Non
Nombre maximal de caractères pour le nom de la sélection de tests de la restauration	50 caractères (alphanumériques et traits de soulignement, pas d'espaces blancs)	Non

Chaque type de ressource limite le nombre de tâches de restauration simultanées pouvant exister simultanément pour les tâches de restauration créées dans le cadre d'un plan de test de restauration. Une fois cette limite atteinte, aucune nouvelle tâche de restauration pour ce type de ressource ne sera créée tant qu'une tâche en état de RUNNING transition vers COMPLETED.

Si une tâche de restauration planifiée n'a pas démarré en raison de ce quota, cette tâche se traduira par un FAILED statut avec le message d'état "Restore job was unable to start within the specified start window. Try increasing your start window.". Si vous recevez un message d'échec avec ce message d'état, la meilleure pratique consiste à augmenter d'abord votre fenêtre de démarrage suffisamment longtemps pour permettre aux tâches de se terminer. Réessayez ensuite les tâches.

Notez que les quotas ne s'appliquent pas aux tâches de restauration à la demande, mais aux tâches de restauration créées par un [plan de test de restauration](#). Pour certains types de ressources, vous pouvez demander une augmentation de la limite de quota.

Name	Par défaut	Ajustable
Amazon Aurora	40	Oui
Amazon DocumentDB	40	Oui
Amazon DynamoDB	40	Non
Amazon EBS	100	Oui
Amazon EC2	100	Oui
Amazon EFS	30	Oui
Amazon FSx	40	Oui
Amazon Neptune	40	Oui
Amazon RDS	40	Oui
Amazon S3	30	Oui

AWS Backup gateway quotas

Name	Par défaut	Ajustable
Tâches de sauvegarde ou de restauration par passerelle	4	Non Créez d'autres passerelles et connectez-les à votre hyperviseur.

Quotas Amazon EKS

Name	Par défaut	Ajustable
Espaces de noms par sauvegarde de cluster EKS	1 000	Oui

Name	Par défaut	Ajustable
Sauvegardes de stockage persistantes par sauvegarde de cluster EKS	1 000	Oui
Tâches de restauration par cluster EKS cible	1	Non
Tâches EKS Restore par compte	5	Oui

Quotas de coffre répartis de manière logique

Type de ressource	Nombre maximum de copies simultanées
EC2	La limite de copies simultanées EBS s'applique à tous les instantanés copié dans le cadre d'une copie de l'AMI.
EBS	20
Aurora	20
DocumentDB	20
Neptune	20
Storage Gateway	5
FSx	5

Quotas associés

Il existe [des quotas pour une seule attribution de ressource](#) dans une seule règle de sauvegarde. Vous pouvez créer un plan de sauvegarde avec plusieurs règles de sauvegarde.

Lorsque vous gérez des sauvegardes sur plusieurs comptes à l'aide de AWS Organizations, vous pouvez être confronté à des quotas qui s' AWS Organizations imposent. Pour ces quotas, consultez [Quotas pour AWS Organizations](#) dans le Guide de l'utilisateur AWS Organizations .

Vous pouvez également être confronté à des quotas imposés par un service AWS Backup pris en charge, notamment les suivants :

- [Amazon Elastic File System](#)
- [Amazon Elastic Block Store](#)
- [Amazon RDS](#)
- [Amazon Aurora](#)
- [Amazon EC2](#)
- [AWS Storage Gateway](#)
- [Amazon DynamoDB](#)
- [Amazon FSx pour Lustre](#)
- [Serveur FSx de fichiers Amazon pour Windows](#)
- [Amazon DocumentDB](#)
- [Amazon Neptune](#)
- [Amazon Simple Storage Service](#)
- [Amazon Timestream](#)

Surveillance AWS Backup

AWS Backup fonctionne avec d'autres AWS outils pour vous permettre de surveiller ses charges de travail. Ces outils incluent :

- [AWS Backup tableaux de bord de console](#)
 - Le tableau de bord des tâches permet de surveiller l'état de la tâche ; vous pouvez consulter les métriques indiquant les réussites et les échecs des tâches, filtrés par motif, compte, région et type de ressource.
 - Le tableau de bord des jobs est disponible dans les régions où AWS Backup Audit Manager est pris en charge. Consultez [Disponibilité des fonctionnalités par Région AWS](#) pour ces régions. Toutes les autres régions pourront accéder au [CloudWatch Tableau de bord](#).
- Amazon CloudWatch et Amazon EventBridge pour surveiller AWS Backup les processus.
 - Vous pouvez l'utiliser CloudWatch pour suivre les métriques, créer des alarmes et consulter des tableaux de bord.
 - Vous pouvez l'utiliser EventBridge pour afficher et surveiller les AWS Backup événements.

Pour plus d'informations, consultez [Surveillance des AWS Backup événements à l'aide d'Amazon EventBridge](#) et .

- AWS CloudTrail pour surveiller les appels AWS Backup d'API. Vous pouvez identifier l'heure, l'adresse IP source, les utilisateurs et les comptes qui effectuent ces appels. Pour de plus amples informations, veuillez consulter [Journalisation des appels d' AWS Backup API avec CloudTrail](#).
- Amazon Simple Notification Service (Amazon SNS) pour vous abonner à des sujets AWS Backup connexes tels que les événements de sauvegarde, de restauration et de copie. Pour de plus amples informations, veuillez consulter [Options de notification avec AWS Backup](#).

AWS Backup tableaux de bord de console

Note

Le tableau de bord des jobs est disponible dans toutes les régions où AWS Backup Audit Manager est pris en charge. Consultez [Disponibilité des fonctionnalités par Région AWS](#) pour ces régions. Toutes les autres régions pourront accéder au [CloudWatch Tableau de bord](#).

Rubriques

- [Présentation des tableaux de bord de sauvegarde](#)
- [Affichage du tableau de bord des tâches](#)
- [Motifs de tâches problématiques](#)
- [Obtention des données du tableau de bord via AWS CLI](#)

Présentation des tableaux de bord de sauvegarde

AWS Backup fournit un tableau de bord des tâches dans la console pour vous aider à surveiller l'état de vos tâches de sauvegarde, de copie et de restauration. Les mêmes données affichées visuellement dans la console peuvent être récupérées dans la ligne de commande via AWS CLI.

Le tableau de bord des tâches peut être utilisé pour identifier les problèmes liés aux tâches de sauvegarde, de copie et de restauration par le biais d'une surveillance au niveau de l'organisation ou d'un compte membre. Grâce à ces informations, vous pouvez identifier et diagnostiquer les événements et les problèmes éventuels afin de garantir la fidélité de vos activités.

Le tableau de bord des tâches peut afficher deux périodes. Par défaut, les données des 14 derniers jours sont affichées, mais vous pouvez modifier la vue pour afficher les 7 derniers jours. Si vous modifiez la période, les données seront mises à jour pour refléter le nouvel intervalle de temps.

Notez que le tableau de bord affiche les données jusqu'à la date la plus récente à minuit (UTC), c'est-à-dire que les données du jour en cours ne sont pas incluses. Le tableau de bord est mis à jour quotidiennement entre 1 h 30 et 2 h 30 (UTC) environ.

Affichage du tableau de bord des tâches

Pour consulter le tableau de bord des tâches, [connectez-vous à la AWS Backup console](#) et sélectionnez Tableaux de bord des tâches dans la barre de navigation de gauche.

Sur la page du tableau de bord des tâches, vous pouvez sélectionner une tâche de sauvegarde, de copie ou de restauration.

La présentation du tableau de bord des tâches affiche une vue agrégée de la période spécifiée d'activité des tâches, y compris les tâches terminées, terminées avec des problèmes, expirées et ayant échoué. Par défaut, les données des 14 derniers jours sont affichées, mais vous pouvez modifier la vue pour afficher 7 jours.

Note

`Completed with issues` est le statut d'une tâche affiché dans la console qui indique qu'une tâche est terminée avec un message de statut.

État de la tâche

Le diagramme linéaire affiche les courbes de taux de réussite et d'échec des tâches au fil du temps. La courbe du taux de réussite indique une agrégation des tâches terminées et des tâches terminées avec problèmes. La courbe du taux d'échec indique la somme des tâches ayant échoué et expirées en fonction de la plage de temps spécifiée.

Les tâches non terminées ou n'ayant pas échoué (tâches avec un statut créées, en attente, en cours, abandonnées, abandonnées ou partielles) ne sont pas incluses ; les pourcentages totaux peuvent ne pas être égaux à 100 %.

Statut de la tâche au fil du temps

Avec le diagramme à barres, vous pouvez générer un diagramme à barres personnalisé qui indique le nombre de tâches dans chaque catégorie (terminées, terminées avec problèmes, ayant échoué et expirées), réparties par jours.

À l'aide des menus déroulants, choisissez le ou les statuts, les types de ressources et AWS les régions que vous souhaitez voir apparaître dans le graphique. Si vous souhaitez approfondir votre sélection, sélectionnez **Afficher les tâches** pour afficher une partie préfiltrée de la page de surveillance des tâches/entre comptes.

Vous pouvez placer le pointeur de la souris sur une barre pour afficher une fenêtre contextuelle qui affiche les données de tâches détaillées pour la date sélectionnée.

Tâches problématiques

Une tâche problématique est une tâche dont le statut est **Échoué**, **Expiré** ou **Terminé** avec des problèmes. Chaque diagramme affiche la métrique correspondante qui contient les comptes, les types de ressources ou les principales raisons qui contiennent le plus grand nombre de tâches problématiques.

L'affichage par défaut trie le widget du tableau de bord en fonction de la métrique spécifiée par ordre décroissant, en commençant par la métrique contenant le plus grand nombre de tâches problématiques associées à la métrique.

L'affichage des comptes les plus problématiques ne sera visible que dans les comptes qui y ont accès via Organizations, tels que les comptes administratifs et les comptes d'administrateur délégué. S'il est visible, vous pouvez survoler un compte pour afficher le nombre de tâches problématiques associées au compte choisi.

Vous pouvez sélectionner une barre dans le diagramme pour ouvrir une fenêtre contextuelle. Dans cette fenêtre, vous pouvez sélectionner un statut de tâche pour ouvrir un tableau de surveillance des tâches/entre comptes filtré en fonction du statut sélectionné.

Motifs de tâches problématiques

Le widget Principaux motifs problématiques indique la catégorie de code de message à laquelle appartiennent les messages d'erreur. Cependant, la catégorie peut ne pas expliquer les problèmes rencontrés par une tâche. Développez les catégories de codes de message ci-dessous pour plus de détails sur les messages ou les erreurs spécifiques que vos tâches peuvent rencontrer.

« ERREUR_VSS »

- « La tentative de sauvegarde Windows VSS a échoué car l'état de l'instance ou de l'agent SSM n'est pas valide ou les privilèges sont insuffisants. »
- « La tentative de sauvegarde Windows VSS a échoué en raison de privilèges insuffisants pour effectuer cette opération. »
- « La tentative de sauvegarde Windows VSS a échoué car le fichier ec2-vss-agent.exe n'est pas installé dans l'instance. »
- « Une erreur liée à la tâche de sauvegarde Windows VSS s'est produite lors d'une tentative de sauvegarde normale. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'un délai d'attente lors de la création d'instantanés compatible avec VSS. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'une version de Windows Server non prise en charge. Vous pouvez utiliser Windows Server 2012 ou une version ultérieure. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'un délai d'attente lors de la création d'instantanés compatible avec VSS. »

« LIMITE_DÉPASSÉE »

- « Limite d'abonnés dépassée : vous avez atteint le nombre maximal de sauvegardes simultanées, qui est de 300. Attendez que les autres tâches se terminent et réessayez. Vous pouvez également nous contacter pour Support demander une augmentation de quota. »
- « Le nombre maximum autorisé d'instantanés en cours pour un seul volume est dépassé. »
- « Le nombre maximum autorisé d'instantanés actifs est dépassé. »
- « Impossible de créer plus de 20 instantanés utilisateur »
- « Le jeu de balises résultant ne doit pas comporter plus de 50 balises utilisateur. »
- « Vous avez atteint le maximum de sauvegardes prises en charge pour votre compte/base de données. Consultez Quotas dans le Guide du développeur Timestream pour plus d'informations. »
- « Vous avez atteint votre quota de 50 000 pour le nombre d'images publiques et privées autorisées dans cette région. Désenregistrez les images inutilisées ou demandez une augmentation de votre quota d'AMI. »
- « Votre sauvegarde a réussi, mais nous n'avons pas pu conserver NetworkInterfaces les métadonnées car leur taille dépassait nos limites internes. »
- « REGEX#limite d'abonnés dépassée »
- « REGEX#Plus de 50 balises spécifiées »
- « REGEX#peut avoir au maximum »

« ACCÈS_REFUSÉ »

- « Vous n'êtes pas autorisé à effectuer cette opération. »
- « Accès refusé en essayant d'appeler le AWS Backup service »
- « Les images de AWS Marketplace ne peuvent pas être copiées vers un autre AWS compte. »
- « La tâche de copie a échoué car le coffre-fort de sauvegarde de destination est chiffré avec la clé gérée par le service de sauvegarde par défaut. Le contenu de ce coffre-fort ne peut pas être copié. Seul le contenu d'un coffre-fort Backup chiffré par une AWS KMS clé peut être copié.
- Les instantanés chiffrés avec le ne Clé gérée par AWS peuvent pas être partagés. Spécifiez un autre instantané.
- « Les instantanés chiffrés avec la clé par défaut d'Amazon EBS ne peuvent pas être partagés
- « La tâche de copie a échoué. Les comptes source et de destination doivent être membres de la même organisation. »

- « REGEX#access refusé »
- « REGEX#non autorisé à »
- « REGEX #cannot » doit être assumé par AWS Backup
- « REGEX#n'a pas l'autorisation »
- « REGEX#autorisation manquante »

« TÂCHE_SIMULTANÉE »

- « La tâche de sauvegarde a échoué car une tâche était en cours d'exécution pour la même ressource. »

« FONCTIONNALITÉ_NON_ACTIVÉE »

- « La tâche de copie a échoué. La fonctionnalité de copie entre comptes n'est pas activée pour l'organisation actuelle. »

« TÂCHE_EXPIRÉE »

- « La tâche de sauvegarde a expiré avant d'être terminée. »

« CYCLE_DE_VIE_NON_VALIDE »

- « La tâche de copie a échoué. La rétention spécifiée dans la tâche ne se situe pas dans la plage spécifiée pour le coffre-fort de sauvegarde cible. »
- « REGEX#ne pourrait pas démarrer car il se trouve soit à l'intérieur, soit trop près de la fenêtre de maintenance hebdomadaire configurée »
- « REGEX#ne pourrait pas démarrer car il se trouve soit à l'intérieur, soit trop près de la fenêtre de sauvegarde automatisée »

« ÉTAT_INVALIDE »

- « REGEX#L'instance n'est pas dans l'état »
- « REGEX#pas dans l'état disponible »
- « REGEX#pas dans un état disponible »
- « REGEX#Volume d'instantané impossible »

« ERREUR_CLÉ_KMS »

- « La clé KMS est désactivée ou en attente de suppression ou l'accès à la clé KMS est refusé »
- « L'ID de clé donné n'est pas accessible »
- « La copie de l'instantané de l'AMI a échoué avec une erreur : l'ID de clé donné n'est pas accessible. Vous devez avoir des DescribeKey autorisations sur la clé par défaut. »
- « REGEX#clé kms »

« ERREUR_CLÉ_ACCÈS »

- « L'ID de clé d' AWS accès nécessite un abonnement au service »

« HYPERVISEUR_HORS-LIGNE »

- « Cette opération n'est pas valide pour l'hyperviseur spécifié car il n'est pas en ligne »

« RESSOURCE_INTROUVABLE »

- « Le volume spécifié est introuvable. »
- « La machine virtuelle est introuvable. »
- « L'ID de clé donné n'existe pas »
- « REGEX#n'existe pas »
- « REGEX#Impossible de trouver la ressource »
- « REGEX#Impossible de trouver le cryopode »
- « REGEX#Impossible de trouver un point de récupération »
- « REGEX#resource introuvable »
- « REGEX#plus disponible »
- « REGEX#non valide »

« RESSOURCE_NON_PRISE_EN_CHARGE »

- « REGEX#type de ressource non pris en charge »
- « REGEX#Type de ressource non pris en charge »

« ERREUR_COPIE_BALISE »

- « Nous ne sommes pas en mesure de copier les balises de ressources vers votre sauvegarde en raison d'un échec interne. »
- « Nous ne sommes pas en mesure de copier les balises de ressources vers votre sauvegarde car le point de récupération source ou de destination n'est pas disponible »

« JETON_EXPIRÉ »

- « Jeton expiré. Réessayez. »

« OPÉRATION_NON_PRISE_EN_CHARGE »

- « CreateSnapshot méthode non prise en charge sur l'hyperviseur lors de la création d'un instantané. Tâche de sauvegarde interrompue. »
- « UnsupportedOperation : Les copies de sauvegarde de Storage Gateway nécessitent un coffre-fort de sauvegarde créé par l'utilisateur et une clé à destination. »
- « REGEX#Fonctionnalité non prise en charge pour le type de ressource fourni. »

« ERREUR_FATALE »

- « Une erreur interne s'est produite. »
- « La tâche de copie a rencontré une erreur fatale. Veuillez contacter le AWS Support pour obtenir de l'aide supplémentaire. »
- « La tâche de copie a rencontré une erreur fatale. »
- « REGEX#La tâche de sauvegarde a rencontré une erreur fatale »

Obtention des données du tableau de bord via AWS CLI

Vous pouvez utiliser la ligne de commande pour récupérer les mêmes données qui apparaissent dans la console. Utilisez l'une des commandes d'interface de ligne de commande suivantes :

- [list-backup-job-summaries](#)
- [list-copy-job-summaries](#)
- [list-restore-job-summaries](#)

Voici les paramètres valides que vous pouvez inclure dans chaque commande :

```
BackupJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
  MessageCategory (string),
  AggregationPeriod: (string),
  NextToken (string),
  MaxResults (number)
```

```
CopyJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
  MessageCategory (string),
  AggregationPeriod: (string),
  NextToken (string),
  MaxResults (number)
```

```
RestoreJobSummaries (list)
  Region (string),
  Account (string),
  State (string),
  ResourceType (string),
  AggregationPeriod: (string),
  NextToken (string)
```

Cet exemple montre un exemple de demande dans lequel un utilisateur a une entrée `list-backup-job-summaries` dans laquelle la demande veut renvoyer tous les comptes disponibles dont l'état est `FAILED` au cours des 14 derniers jours :

```
GET /audit/backup-job-summaries/
  ?accountId=ANY
  &state=FAILED
  &aggregationPeriod=FOURTEEN_DAYS
```

Pour obtenir le nombre de tâches dont le statut est `completed with issues`, soustrayez le nombre de tâches `COMPLETED` avec une `MessageCategory SUCCESS` du nombre `COMPLETED` total.

Surveillance des AWS Backup événements à l'aide d'Amazon EventBridge

AWS Backup envoie des événements à Amazon EventBridge lorsque l'état d'une tâche de sauvegarde ou de copie change. Vous pouvez l'utiliser EventBridge pour surveiller les AWS Backup événements. Par exemple, vous pouvez recevoir une alarme en cas d'échec d'une tâche de sauvegarde. AWS Backup émet des événements de la meilleure EventBridge manière possible toutes les 5 minutes.

Pour suivre les événements à l'aide de EventBridge, consultez les rubriques suivantes :

- [Création d'une règle réagissant aux événements](#) (Amazon EventBridge User Guide)
- [Amazon CloudWatch Events and Metrics pour AWS Backup](#) (blog - voir Configurer AWS Backup les événements à envoyer à Amazon EventBridge)

Certains événements indiquent `status: COMPLETED` alors que d'autres événements indiquent `state: COMPLETED`. Cela est conforme à l' AWS Backup API. Certains statuts sont spécifiques à la AWS Backup console : le `Completed with issues` statut est une représentation des `Completed` tâches avec des messages de statut. Pour surveiller les événements `Completed with issues`, surveillez les tâches `COMPLETED` comportant un message de statut. Veuillez noter que cela ne concerne que les tâches de sauvegarde.

Vous pouvez également utiliser l'API de AWS Backup notification pour suivre les AWS Backup événements avec Amazon Simple Notification Service (Amazon SNS). Toutefois, elle EventBridge suit un plus grand nombre de modifications que l'API de notification, notamment les modifications apportées aux coffres-forts de sauvegarde, à l'état des tâches de copie, aux paramètres régionaux et au nombre de points de restauration froids ou chauds.

Événements

- [Événements Backup Job](#)
- [Événements du Backup Plan](#)
- [Événements Backup Vault](#)
- [Événements Copy Job](#)
- [Événements de Recovery Point](#)
- [Événements relatifs aux paramètres régionaux](#)

- [Événements Restore Job](#)
- [Événements d'indexation des points de restauration](#)
- [Malware Scan Job Events](#)

Événements Backup Job

Voici des exemples d'événements.

State

- [État : ÉCHEC](#)
- [État : TERMINÉ](#)
- [État : COURSE À PIED](#)
- [État : AVORTÉ](#)
- [État : EXPIRÉ](#)
- [État : EN ATTENTE](#)
- [État : CRÉÉ](#)

État : ÉCHEC

```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
```



```

    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.\"",
    "startBy": "2020-07-30T04:13:07.392Z",
    "percentDone": 0,
    "retryCount": 3
  }
}

```

État : TERMINÉ

```

{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}

```

État : COURSE À PIED

```
{
  "version": "0",
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLTNmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```

État : AVORTÉ

```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
```

```

"account": "1112233445566",
"time": "2020-07-15T21:33:16Z",
"region": "us-west-2",
"resources": [],
"detail": {
  "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
  "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffc-d-2538-4bbe-8343-1c60dae27c27",
  "backupVaultName": "f59bffc-d-2538-4bbe-8343-1c60dae27c27",
  "bytesTransferred": "0",
  "creationDate": "2020-07-15T21:33:00.803Z",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
  "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
  "resourceType": "type",
  "state": "ABORTED",
  "statusMessage": "\"Backup job was stopped by user.\",
  "completionDate": "2020-07-15T21:33:01.621Z",
  "startBy": "2020-07-16T05:33:00.803Z",
  "percentDone": 0
}
}

```

État : EXPIRÉ

```

{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",

```

```

    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
resource.\",
    \"completionDate\": \"2020-07-29T13:02:15.234Z\",
    \"startBy\": \"2020-07-29T13:00:00Z\",
    \"percentDone\": 0,
    \"createdBy\": {
      \"backupPlanId\": \"aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b\",
      \"backupPlanArn\": \"arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b\",
      \"backupPlanVersion\": \"NjBjOTUzZjYtYzZiNi00Njh1LWlzMTEtNWRjOWY0YTNjN2Vj\",
      \"backupPlanRuleId\": \"3eb0017c-f262-4211-a802-302cebb11dc2\"
    }
  }
}

```

État : EN ATTENTE

```

{
  \"version\": \"0\",
  \"id\": \"64dd1897-f863-31a3-9ee5-b05e306d81ff\",
  \"detail-type\": \"Backup Job State Change\",
  \"source\": \"aws.backup\",
  \"account\": \"1112233445566\",
  \"time\": \"2020-07-29T20:03:30Z\",
  \"region\": \"us-west-2\",
  \"resources\": [],
  \"detail\": {
    \"backupJobId\": \"2cfffdb68-d6ed-485f-9f9b-8b530749f1c2\",
    \"backupVaultArn\": \"arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975\",
    \"backupVaultName\": \"ed1f2661-5587-48bf-8a98-fadb977bf975\",
    \"bytesTransferred\": \"0\",
    \"creationDate\": \"2020-07-29T20:01:06.224Z\",
    \"iamRoleArn\": \"arn:aws:iam::1112233445566:role/MockRCBackupTestRole\",
    \"resourceArn\": \"arn:aws:service:us-west-2:1112233445566:resource-type/resource-id\",
    \"resourceType\": \"type\",
    \"state\": \"PENDING\",
    \"statusMessage\": \"\",
    \"startBy\": \"2020-07-30T04:01:06.224Z\",
    \"percentDone\": 0
  }
}

```

État : CRÉÉ

```
{
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```

Événements du Backup Plan

Voici des exemples d'événements.

State

- [État : MODIFIÉ](#)
- [État : SUPPRIMÉ](#)
- [État : CRÉÉ](#)

État : MODIFIÉ

```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de"
  ]
}
```

```

    ],
    "detail": {
      "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
      "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
      "modifiedAt": "2020-06-24T23:18:19.168Z",
      "state": "MODIFIED"
    }
  }
}

```

État : SUPPRIMÉ

```

{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}

```

État : CRÉÉ

```

{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [

```

```

    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
    "versionId": "N2Q40TczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}

```

Événements Backup Vault

Voici des exemples d'événements.

State

- [État : CRÉÉ](#)
- [État : MODIFIÉ](#)
- [État : SUPPRIMÉ](#)

État : CRÉÉ

```

{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}

```

État : MODIFIÉ

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

État : SUPPRIMÉ

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```


Événements Copy Job

Voici des exemples d'événements.

State

- [État : ÉCHEC](#)
- [État : COURSE À PIED](#)
- [État : TERMINÉ](#)
- [État : CRÉÉ](#)

État : ÉCHEC

```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2:image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```

```
}
```

État : COURSE À PIED

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

État : TERMINÉ

```
{
  "version": "0",
```

```

    "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
    "detail-type": "Copy Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T22:08:04Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
    ],
    "detail": {
      "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
      "backupSizeInBytes": 3221225472,
      "creationDate": "2020-07-15T22:06:27.234Z",
      "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
      "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
      "resourceType": "EBS",
      "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
      "state": "COMPLETED",
      "completionDate": "2020-07-15T22:07:58.111Z",
      "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:846869de-4589-45c3-ab60-4fbbabcbdd3ec",
      "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/snap-0726fe70935586180",
      "createdBy": {
        "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
      }
    }
  }
}

```

État : CRÉÉ

```

{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",

```

```

"region": "us-west-2",
"resources": [
  "arn:aws:ec2:us-west-2:image/ami-0888b126e2170b98e"
],
"detail": {
  "creationDate": "2020-06-22T21:06:25.754Z",
  "state": "CREATED",
  "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
  "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
}
}

```

Événements de Recovery Point

Voici les événements.

State

- [TERMINÉ](#)
- PARTIAL
- SUPPRESSION
- EXPIRÉ
- DISPONIBLE
- STOPPED
- CREAtioN

État : TERMINÉ

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [

```

```

    "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
  ],
  "detail": {
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceType": "Aurora",
    "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
    "status": "COMPLETED",
    "isEncrypted": "false",
    "storageClass": "WARM",
    "completionDate": "2020-07-15T21:39:05.689Z",
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLTNmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    },
    "lifecycle": {
      "deleteAfterDays": 100
    },
    "calculatedLifeCycle": {
      "deleteAt": "2020-10-23T21:38:31.152Z"
    }
  }
}

```

Événements relatifs aux paramètres régionaux

Voici un exemple d'événement.

```

{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dba9cfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",

```

```
"resources": [],
"detail": {
  "modifiedAt": "2020-06-24T22:54:57.161Z",
  "ResourceTypeOptInPreference": {
    "Aurora": true
  },
  "state": "MODIFIED"
}
```

Événements Restore Job

Voici des exemples d'événements. Notez que votre cas d'utilisation d'une tâche de restauration déterminera les paramètres obligatoires et facultatifs à inclure. Par exemple, si votre tâche de restauration fait partie d'un plan de test de restauration, le paramètre `restoreTestingPlanArn` est inclus. Voir `DescribeRestoreJob` pour les paramètres possibles.

State

- [État : ÉCHEC](#)
- [État : COURSE À PIED](#)
- [État : TERMINÉ](#)
- [État : EN ATTENTE](#)
- [État : CRÉÉ](#)

État : ÉCHEC

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
```

```

    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
EC2 instance. Please restore using the backed up instance profile."
  }
}

```

État : COURSE À PIED

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}

```

État : TERMINÉ

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",

```

```

"account": "1112233445566",
"time": "2020-07-15T03:14:58Z",
"region": "us-west-2",
"resources": [
  "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
],
"detail": {
  "restoreJobId": "AB123456-78C9-0123-456D-789012E34567",
  "backupSizeInBytes": "0",
  "creationDate": "2020-07-15T03:10:01.742Z",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
  "percentDone": 0,
  "resourceType": "RDS",
  "status": "COMPLETED",
  "createdResourceArn": "arn:aws:rds:us-west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
  "completionDate": "2020-07-15T03:14:53.128Z"
}
}

```

État : EN ATTENTE

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}

```



```
}  
}
```

État : CRÉÉ

```
{  
  "version": "0",  
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",  
  "detail-type": "Restore Job State Change",  
  "source": "aws.backup",  
  "account": "1112233445566",  
  "time": "2020-06-22T18:50:49Z",  
  "region": "us-west-2",  
  "resources": [  
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-efgh939ij32k"  
  ],  
  "detail": {  
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",  
    "creationDate": "2020-06-22T18:50:46.407Z",  
    "state": "CREATED"  
  }  
}
```

Événements d'indexation des points de restauration

Voici des exemples d'événements.

State

- [État : ACTIF](#)
- [État : SUPPRIMÉ](#)
- [État : ÉCHEC](#)

État : ACTIF

```
{  
  "version": "0",  
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",  
  "detail-type": "Recovery Point Index State Change",
```

```

"source": "aws.backup",
"account": "1112233445566",
"time": "2023-12-15T21:39:07Z",
"region": "us-west-2",
"resources": [
  "arn": "aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
],
"detail": {
  "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
  "accountId": "1112233445566",
  "indexStatus": "ACTIVE",
  "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
  "resourceType": "EBS",
  "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
  "indexCreationTime": "2025-05-25T21:38:31.152Z",
  "isIndexingContinuous": false,
  "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-01234567890abcdef",
  "backupCreationTime": "2023-12-15T21:38:00.000Z",
  "indexStatusMessage": "An AWS Backup recovery point index was successfully completed. Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
  "indexCompletionTime": "2025-05-25T21:39:05.689Z",
}
}

```

État : SUPPRIMÉ

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point Index State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2023-12-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn": "aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {

```

```

    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId": "1112233445566",
    "indexStatus": "DELETED",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/
vol-01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index was deleted.
Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "indexDeletionTime": "2025-05-27T22:39:05.689Z",
  }
}

```

État : ÉCHEC

```

{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Recovery Point Index State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2023-12-15T21:39:07Z",
  "region": "us-west-2",
  "resources": [
    "arn": "aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "accountId": "1112233445566",
    "indexStatus": "FAILED",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/BackupIndexRole",
    "resourceType": "EBS",
    "backupVaultArn": "arn:aws:cryo:us-west-2:1112233445566:pod/backup-pod-12345",
    "indexCreationTime": "2025-05-25T21:38:31.152Z",
    "isIndexingContinuous": false,
  }
}

```

```

    "sourceResourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/01234567890abcdef",
    "backupCreationTime": "2023-12-15T21:38:00.000Z",
    "indexStatusMessage": "An AWS Backup recovery point index failed to create.
Indexed recovery point arn : arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
  }
}

```

Malware Scan Job Events

Voici des exemples d'événements.

State

- [État : CRÉÉ](#)
- [État : COURSE À PIED](#)
- [État : TERMINÉ](#)
- [État : TERMINÉ AVEC DES PROBLÈMES](#)
- [État : ÉCHEC](#)
- [État : ANNULÉ](#)

État : CRÉÉ

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
    abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
    vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "createdBy": {

```

```

      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "CREATED"
  }
}

```

État : COURSE À PIED

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",

```

```

    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "RUNNING"
  }
}

```

État : TERMINÉ

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",

```

```

    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
        "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
        "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
        "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/
RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "scanResult": {
        "scanResultStatus": "THREATS_FOUND"
    },
    "state": "COMPLETED",
    "statusMessage": "An AWS Backup scan job was successful completed."
}
}

```

État : TERMINÉ AVEC DES PROBLÈMES

```

{
    "version": "0",
    "id": "60ce181d-67c7-496b-90fb-69636b42daee",
    "detail-type": "Scan Job State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2025-12-12T12:12:12Z",

```

```

    "region": "us-west-2",
    "resources": [
        "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-
        abcdef123456"
    ],
    "detail": {
        "accountId": "1112233445566",
        "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
        vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
        "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
        "completionDate": "2025-12-12T12:12:12Z",
        "createdBy": {
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
            plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
            "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
            "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
            "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
        },
        "creationDate": "2025-12-12T12:12:00Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/
        RoleForEc2BackupWithNoDescribeTagsPermissions",
        "scannerRoleArn": "arn:aws:iam::1112233445566:role/
        RoleForAwsBackupGuarddutyScanner",
        "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
        point:abcd1234-5678-abcd-9012-abcdef123456",
        "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/
        i-0515aee7de03f58e1",
        "resourceType": "EC2",
        "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
        "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
        "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
        point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
        "malwareScanner": "GUARDDUTY",
        "scanResult": {
            "scanResultStatus": "NO_THREATS_FOUND"
        },
        "state": "COMPLETED_WITH_ISSUES",
        "statusMessage": "Scan job partially completed. View more details in Amazon
        GuardDuty"
    }
}

```


État : ÉCHEC

```
{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMtYWY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
    "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
    "malwareScanner": "GUARDDUTY",
    "state": "FAILED",
  }
}
```

```

    "statusMessage": "<failure reason>"
  }
}

```

État : ANNULÉ

```

{
  "version": "0",
  "id": "60ce181d-67c7-496b-90fb-69636b42daee",
  "detail-type": "Scan Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2025-12-12T12:12:12Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"
  ],
  "detail": {
    "accountId": "1112233445566",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "completionDate": "2025-12-12T12:12:12Z",
    "createdBy": {
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanId": "5d5a14cc-4ee2-4b9f-beb6-4afa998bb98f",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMtY2IwMTY4NWQ4",
      "backupRuleId": "256ad167-f523-4cb9-93f3-f0c933efd97f"
    },
    "creationDate": "2025-12-12T12:12:00Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RoleForEc2BackupWithNoDescribeTagsPermissions",
    "scannerRoleArn": "arn:aws:iam::1112233445566:role/RoleForAwsBackupGuarddutyScanner",
    "recoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "scanId": "43bc14a6-03e0-436a-abf5-8825d3aa6835",
    "scanJobId": "4d5fc12e-7e33-4336-a981-bbe43c300298",
  }
}

```

```
{
  "scanBaseRecoveryPointArn": "arn:aws:backup:us-west-2:1112233445566:recovery-
point:46bd3edb-a499-4db1-8f8f-269a2ff76fab",
  "malwareScanner": "GUARDDUTY",
  "state": "CANCELED",
  "statusMessage": "Scan job was stopped by user."
}
```

AWS Backup statistiques avec Amazon CloudWatch

Rubriques

- [CloudWatch Tableau de bord](#)
- [Métriques avec CloudWatch](#)

CloudWatch Tableau de bord

Note

Le tableau de bord de la console dépend de la région qui accède à la console. Consultez [Disponibilité des fonctionnalités par Région AWS](#) pour savoir quelles régions ont accès au tableau de bord des tâches. Les régions non répertoriées pourront accéder au CloudWatch tableau de bord.

Votre AWS Backup console inclut un tableau de bord permettant de consulter les statistiques relatives aux tâches de sauvegarde, de copie et de restauration terminées ou échouées. Dans ce tableau de bord, vous pouvez afficher le statut de la tâche par période, personnalisée en fonction de la période que vous souhaitez.

POUR ACCÉDER AU TABLEAU DE BORD

1. Ouvrez la AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.
2. Dans le volet de navigation de gauche, sélectionnez Tableau de bord.

AFFICHAGE ET COMPRÉHENSION DU TABLEAU DE BORD

Le CloudWatch tableau de bord affiche plusieurs widgets. Chaque widget affiche les métriques des tâches par nombre. Chaque widget affiche plusieurs graphiques linéaires. Chaque ligne correspond à une ressource protégée (si aucune ressource attendue ne s'affiche, assurez-vous que la ressource est activée dans Paramètres). Les affichages n'indiquent pas les tâches en cours.

L'axe des Y (valeurs verticales) indique le nombre. L'axe des X (valeurs horizontales) indique des points dans le temps. S'il n'y a aucun point de données à visualiser dans le statut de la tâche sélectionnée, la valeur sera définie sur 0 avec une ligne horizontale sur l'axe des X. La légende indiquant les ressources sera toujours visible.

Les métriques affichent des informations spécifiques au compte et à la région relatives à la connexion actuelle. Pour voir d'autres comptes ou régions, vous devez vous connecter sous le compte choisi.

PERSONNALISATION DU TABLEAU DE BORD

Par défaut, le délai affiché est d'une semaine. Dans le menu supérieur, vous trouverez des options permettant de redéfinir la période affichée. Vous pouvez choisir entre 1 heure, 3 heures, 12 heures, 1 jour, 3 jours et 1 semaine. En outre, vous pouvez sélectionner Personnalisé pour spécifier une valeur différente. La personnalisation modifiera temporairement l'affichage actuel selon vos spécifications.

Vous pouvez survoler un widget, qui affichera un bouton Agrandir en haut à droite du widget. Cliquez sur Agrandir pour ouvrir le widget en mode plein écran. En plein écran, d'autres options permettent de personnaliser l'affichage du graphique, telles que la modification de la période (le délai entre chaque point de données). Aucune modification ne sera conservée une fois l'affichage en plein écran fermé.

Pour afficher un seul type de ressource à la fois, cliquez sur le texte de l'étiquette du type de ressource que vous souhaitez afficher dans la légende du graphique. Cela désélectionnera tous les autres types de ressources. Pour inverser cette étape, cliquez sur la case de couleur d'un type de ressource dans la légende. Pour revenir à l'affichage par défaut de tous les types de ressources avec toutes les étiquettes sélectionnées, cliquez à nouveau sur le texte de l'étiquette de n'importe quel type de ressource sélectionné.

Cliquez sur les trois points verticaux dans le coin supérieur droit d'un widget pour ouvrir un menu déroulant contenant des options permettant d'actualiser, d'agrandir, d'afficher les métriques et d'afficher les journaux. « Afficher dans les métriques » ouvre la métrique utilisée dans le widget dans la CloudWatch console. Vous pouvez y apporter toutes les modifications nécessaires et ajouter le widget à un tableau de bord personnalisé dans le tableau CloudWatch de bord. Les modifications que

vous apportez au CloudWatch tableau de bord ne seront pas reflétées dans le tableau de bord de AWS Backup la console. « Afficher sous forme de journaux » ouvre la page d'affichage des journaux dans CloudWatch la console.

Pour ajouter des widgets affichés à votre tableau de CloudWatch bord personnalisé, cliquez sur le bouton Ajouter au tableau de bord situé en haut à droite du tableau de bord. Cela ouvrira la CloudWatch console dans laquelle vous pourrez sélectionner dans quel tableau de bord personnalisé ajouter les six widgets.

Pour plus d'informations, consultez la section [Utilisation CloudWatch des métriques Amazon](#).

Métriques avec CloudWatch

Vous pouvez l'utiliser CloudWatch pour surveiller AWS Backup les métriques. L'espace de AWS/Backup noms vous permet de suivre les métriques suivantes. AWS Backup émet des métriques mises à jour CloudWatch toutes les 5 minutes.

Le but de cette page de documentation est de vous fournir les matériaux de référence à utiliser CloudWatch pour surveiller AWS Backup. Pour savoir comment surveiller une métrique à l'aide d'un service unique CloudWatch, consultez le blog [Amazon CloudWatch Events and Metrics for AWS Backup](#) ou [concentrez-vous sur les métriques et les alarmes dans un seul AWS service](#) dans le guide de CloudWatch l'utilisateur. Pour configurer les alarmes, consultez la section [Utilisation d'Amazon CloudWatch Alarms](#) dans le guide de CloudWatch l'utilisateur.

Catégorie	Métriques	Exemple de dimensions	Exemple de cas d'utilisation
Tâches	Nombre de tâches de sauvegarde, de restauration et de copie dans chaque état, y compris CREATED, PENDING, RUNNING, ABORTED, COMPLETED , FAILED et EXPIRED.	Type de ressource, nom du coffre-fort. Le nom du coffre-fort des tâches de copie est celui du coffre-fort de destination.	Surveillez le nombre de tâches de sauvegarde ayant échoué dans un ou plusieurs coffres-forts de sauvegarde spécifiques. Lorsque plus de cinq tâches ont échoué en une heure, envoyez un e-mail ou un SMS

Catégorie	Métriques	Exemple de dimensions	Exemple de cas d'utilisation
	Les différents types de tâches ont différents états disponibles.		via Amazon SNS ou ouvrez un ticket pour que l'équipe d'ingénierie enquête. Critères de notification : il existe une valeur différente de zéro
Points de récupération	Nombre de points de récupération à chaud et à froid dans chaque état : MODIFIED, COMPLETED, PARTIAL, EXPIRED, DELETED.	Type de ressource, nom du coffre-fort.	Suivez le nombre de points de récupération supprimés pour vos volumes Amazon EBS et suivez séparément le nombre de points de récupération à chaud et à froid dans chaque coffre-fort de sauvegarde. Critères de notification : il existe une valeur différente de zéro

Note

L'état de la tâche de Completed with issues est spécifique à la AWS Backup console uniquement ; il ne peut pas être suivi via CloudWatch.

Le tableau suivant répertorie toutes les métriques disponibles.

Métrique	Description
NumberOfBackupJobsCreated	Le nombre de tâches de sauvegarde AWS Backup créées.
NumberOfBackupJobsPending	Nombre de tâches de sauvegarde sur le point d'être exécutées dans AWS Backup.
NumberOfBackupJobsRunning	Nombre de tâches de sauvegarde en cours d'exécution AWS Backup.
NumberOfBackupJobsAborted	Nombre de tâches de sauvegarde annulées par l'utilisateur.
NumberOfBackupJobsCompleted	Nombre de tâches de sauvegarde AWS Backup terminées.
NumberOfBackupJobsFailed	Nombre de tâches de sauvegarde dont le statut est Failed. Cela est souvent dû à la planification d'une tâche de sauvegarde pendant ou 1 heure avant une ressource de base de données ou 4 heures avant ou pendant une fenêtre de FSx maintenance ou une fenêtre de sauvegarde automatique d'Amazon, sans pour autant l'utiliser AWS Backup pour effectuer une sauvegarde continue pour les point-in-time restaurations. Consultez Point-in-Time la section Restauration pour obtenir une liste des services pris en charge et des instructions sur la façon de AWS Backup les utiliser pour effectuer des sauvegardes continues ou pour replanifier vos tâches de sauvegarde.
NumberOfBackupJobsExpired	Le nombre de tâches de sauvegarde dont le statut est deEXPIRED. Le statut d'une tâche de sauvegarde passe CREATED à celui d'EXPIREDune tâche de

Métrique	Description
	sauvegarde qui ne peut pas démarrer dans le délai imparti.
NumberOfCopyJobsCreated	Nombre de tâches de copie entre comptes et entre régions créées par AWS Backup .
NumberOfCopyJobsRunning	Nombre de tâches de copie entre comptes et entre régions en cours d'exécution dans AWS Backup.
NumberOfCopyJobsCompleted	Nombre de tâches de copie entre comptes et entre régions finies par AWS Backup .
NumberOfCopyJobsFailed	Nombre de tâches de copie entre comptes et entre régions qui AWS Backup ont été tentées mais n'ont pas pu être effectuées.
NumberOfRestoreJobsPending	Nombre de tâches de restauration sur le point d'être exécutées dans AWS Backup.
NumberOfRestoreJobsRunning	Le nombre de tâches de restauration en cours d'exécution AWS Backup.
NumberOfRestoreJobsCompleted	Le nombre de tâches de restauration AWS Backup terminées.
NumberOfRestoreJobsFailed	Nombre de tâches de restauration qui ont été AWS Backup tentées mais qui n'ont pas pu être effectuées.
NumberOfRecoveryPointsCompleted	Le nombre de points de récupération AWS Backup créés.

Métrique	Description
NumberOfRecoveryPointsPartial	Nombre de points de restauration qui AWS Backup ont commencé à être créés mais qui n'ont pas pu être terminés. AWS réessaie le processus ultérieurement, mais comme la nouvelle tentative a lieu ultérieurement, le point de récupération partiel est conservé.
NumberOfRecoveryPointsExpired	Nombre de points de restauration qui AWS Backup ont tenté de supprimer en fonction du cycle de conservation des sauvegardes, mais qui n'ont pas pu être supprimés. Le stockage consommé par les sauvegardes expirées vous est facturé et vous devriez les supprimer manuellement.
NumberOfRecoveryPointsDeleting	Le nombre de points de récupération qui AWS Backup sont supprimés.
NumberOfRecoveryPointsCold	Le nombre de points de récupération associés AWS Backup à une chambre froide.

D'autres dimensions sont disponibles en plus de celles indiquées dans le tableau. Pour afficher toutes les dimensions d'une métrique, tapez le nom de cette métrique dans l'AWS/Backupspace de noms de la section Metrics de la CloudWatch console.

Journalisation des appels d' AWS Backup API avec CloudTrail

AWS Backup est intégré à [AWS CloudTrail](#) un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service de service. CloudTrail capture tous les appels d'API AWS Backup sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Backup console et des appels de code vers les opérations de l' AWS Backup API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Backup, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section [Utilisation de l'historique des CloudTrail événements](#) dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou [CloudTrailLake](#).

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez [Créez un journal de suivi dans vos Compte AWS](#) et [Création d'un journal de suivi pour une organisation](#) dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section [AWS CloudTrail Tarification](#). Pour obtenir des informations sur la tarification Amazon S3, consultez [Tarification Amazon S3](#).

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format [Apache ORC](#). ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des [sélecteurs d'événements avancés](#). Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section [Travailler avec AWS CloudTrail Lake](#) dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'[option de tarification](#) que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section [AWS CloudTrail Tarification](#).

AWS Backup événements à CloudTrail

AWS Backup génère ces CloudTrail événements lorsqu'il effectue des sauvegardes, des restaurations, des copies, des scans ou des notifications. Ces événements ne sont pas nécessairement générés par l'utilisation du AWS Backup public APIs. Pour plus d'informations, consultez les [événements AWS de service](#) dans le guide de AWS CloudTrail l'utilisateur.

- AssociateBackupVaultMpaApprovalTeamCompleted
- AssociateBackupVaultMpaApprovalTeamFailed
- BackupDeleted
- BackupJobCompleted
- BackupJobStarted
- BackupSelectionDeletedDueToSLRDeletion
- BackupTransitionedToCold
- CopyJobCompleted
- CopyJobStarted
- CreateRestoreAccessBackupVaultFailed

- DisassociateBackupVaultMpaApprovalTeamFailed
- PutBackupVaultNotifications
- RecoveryPointCreated
- ReportJobCompleted
- ReportJobStarted
- RestoreAccessBackupVaultDeleted
- RestoreCompleted
- RestoreStarted
- RevokeRestoreAccessBackupVaultFailed
- ScanJobCompleted
- ScanJobCreated
- ScanJobFailed
- ScanJobStarted

Comprendre les entrées du fichier AWS Backup journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre les DeleteRecoveryPoint actions StartBackupJobStartRestoreJob, et ainsi que l'BackupJobCompletedévénement.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
```

```

        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2019-01-10T12:24:50Z"
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    }
}

```

```

    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddd-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",

```

```

    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",

```

```
    "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-  
vault:BackupVault",  
    "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",  
    "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/  
vol-06692095a6a421233",  
    "creationDate": {  
        "seconds": 1547101638,  
        "nanos": 272000000  
    },  
    "backupSizeInBytes": 8589934592,  
    "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",  
    "resourceType": "EBS"  
  }  
}
```

Journalisation des événements de gestion entre comptes

Avec AWS Backup, vous pouvez gérer vos sauvegardes dans Comptes AWS l'ensemble de votre [AWS Organizations](#) structure. AWS Backup génère ces CloudTrail événements dans votre compte membre lorsque vous créez, mettez à jour ou supprimez une politique de AWS Organizations sauvegarde (qui applique des plans de sauvegarde à vos comptes de membre) ou lorsqu'un plan de sauvegarde d'organisation n'est pas valide :

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationBackupPlan`

Exemple : entrées de fichier AWS Backup journal pour la gestion entre comptes

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'CreateOrganizationalBackupPlanaction.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "backup.amazonaws.com"},
  "eventTime": "2020-06-02T00:34:00Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "CreateOrganizationalBackupPlan",
  "awsRegion": "ca-central-1",
  "sourceIPAddress": "backup.amazonaws.com",
  "userAgent": "backup.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "account-id",
  "serviceEventDetails": {
    "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ0ThmNzRj",
    "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanName": "mybackupplan",
    "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
    \"name\":\"hourly\", \"description\":null, \"cryopodArn\":\"arn:aws:backup:ca-central-1:123456789012:backup-vault:ControllerCAMTestBackupVault\", \"scheduleExpression\":\"cron(0 0/1 ? * * *)\", \"startWindow\":\"PT1H\", \"completionWindow\":\"PT2H\", \"lifecycle\":{\"moveToColdStorageAfterDays\":null, \"deleteAfterDays\":\"7\"}, \"tags\":null, \"copyActions\":[]}]",
    "backupSelections": "[{\"name\":\"selectiondatatype\", \"arn\":\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-a075ea715686\", \"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\", \"resources\":[], \"notResources\":[], \"conditions\":[{\"type\":\"STRINGEQUALS\", \"key\":\"dataType\", \"value\":\"PII\"}, {\"type\":\"STRINGEQUALS\", \"key\":\"dataType\", \"value\":\"RED\"}], \"creationDate\":\"2020-06-02T00:34:00.695Z\", \"creatorRequestId\":null}]",
    "creationDate": {
      "seconds": 1591058040,
      "nanos": 695000000
    }
  },
}
```

```

    "organizationId": "org-id",
    "accountId": "123456789012"
  }
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`DeleteOrganizationalBackupPlan` action.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2020-06-02T00:34:25Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "DeleteOrganizationalBackupPlan",
  "awsRegion": "ca-central-1",
  "sourceIPAddress": "backup.amazonaws.com",
  "userAgent": "backup.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "account-id",
  "serviceEventDetails": {
    "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
    "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
    "backupPlanName": "mybackupplan",
    "deletionDate": {
      "seconds": 1591058065,
      "nanos": 519000000
    },
    "organizationId": "org-id",
    "accountId": "123456789012"
  }
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'événement `InvalidOrganizationBackupPlan`, qui est envoyé lorsque vous AWS Backup recevez un plan de sauvegarde non valide de la part d'Organizations.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "backup.amazonaws.com"
  },
  "eventTime": "2022-06-11T13:29:23Z",
  "eventSource": "backup.amazonaws.com",
  "eventName": "InvalidOrganizationBackupPlan",
  "awsRegion": "Region",
  "sourceIPAddress": "backup.amazonaws.com",
  "userAgent": "backup.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "987654321098",
  "serviceEventDetails": {
    "effectivePolicyVersion": 7,
    "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
    "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
    "policyType": "BACKUP_POLICY",
    "effectiveBackupPlan": {
      "logicalName": "logical-name",
      "regions": [
        "Region"
      ],
      "rules": [
        {
          "name": "test-orgs",
          "targetBackupVaultName": "vault-name",
          "ruleLifecycle": {
            "deleteAfterDays": 100
          },
          "copyActions": [],
          "enableContinuousBackup": true
        }
      ]
    }
  }
}
```

```

    ],
    "selections": {
      "tagSelections": [
        {
          "selectionName": "selection-name",
          "iamRoleArn": "arn:aws:iam::$account:role/role",
          "targetedTags": [
            {
              "tagKey": "key",
              "tagValue": "value"
            }
          ]
        }
      ]
    },
    "backupPlanTags": {
      "key": "value"
    }
  },
  "organizationId": "org-id",
  "accountId": "123456789012"
},
"eventCategory": "Management"
}

```

Options de notification avec AWS Backup

Il existe deux manières de recevoir des notifications concernant AWS Backup :

- Notifications des utilisateurs peut envoyer des notifications, y compris des CloudWatch alarmes Amazon AWS Support, et des notifications relatives à d'autres services.
- Amazon Simple Notification Service peut vous informer des AWS Backup événements.

Notifications des utilisateurs et AWS Backup

AWS Backup prend en charge la gestion de vos notifications de sauvegarde depuis la [Notifications des utilisateurs console](#). Vous pouvez ainsi consulter la progression de vos tâches de sauvegarde, de copie et de restauration ainsi que les modifications apportées à vos politiques de sauvegarde, à vos coffres-forts, à vos points de restauration et à vos paramètres à partir du centre de notification des notifications utilisateur. [Notifications des utilisateurs](#)

Amazon CloudWatch, les EventBridge alarmes Amazon et les mises à jour de AWS Support cas font partie des autres types de notifications que vous pouvez gérer depuis la console. En outre, vous pouvez configurer plusieurs options de livraison, notamment le courrier électronique, les notifications Amazon Q Developer dans les applications de chat et les notifications AWS Console Mobile Application push.

Amazon SNS et événements AWS Backup

AWS Backup tire parti des notifications robustes fournies par Amazon Simple Notification Service (Amazon SNS). Vous pouvez configurer Amazon SNS pour qu'il vous informe des AWS Backup événements depuis la console Amazon SNS.

Limitations

- Bien que le service Amazon SNS autorise les notifications entre comptes, il ne prend actuellement AWS Backup pas en charge cette fonctionnalité. Vous devez spécifier votre propre identifiant de AWS compte et l'ARN de la ressource de votre rubrique.
- AWS Backup prend en charge les rubriques standard pour la déduplication optimale via SNS, mais AWS Backup ne prend actuellement pas en charge les rubriques SNS FIFO pour la déduplication stricte.

Cas d'utilisation courants

- Configurez les notifications pour les tâches de sauvegarde ayant échoué en suivant les étapes décrites dans [Comment puis-je recevoir des notifications pour les AWS Backup tâches qui ont échoué ?](#) auprès de AWS Premium Support.
- Consultez un exemple de notification Amazon SNS JSONs pour les tâches de sauvegarde terminées, échouées ou expirées dans le tableau des exemples d'événements ci-dessous.

Pour plus d'informations sur Amazon SNS de façon générale, consultez [Démarrage avec Amazon SNS](#) dans le Guide du développeur Amazon Simple Notification Service.

AWS Backup notification APIs

Après avoir créé vos rubriques à l'aide de la console Amazon SNS ou AWS Command Line Interface (AWS CLI), vous pouvez utiliser les opérations d' AWS Backup API suivantes pour gérer vos notifications de sauvegarde.

- [DeleteBackupVaultNotifications](#) : supprime les notifications d'événement SNS pour le coffre-fort de sauvegarde spécifié.
- [GetBackupVaultNotifications](#) : répertorie toutes les notifications d'événement SNS pour le coffre-fort de sauvegarde spécifié.
- [PutBackupVaultNotifications](#) : active les notifications pour la rubrique et les événements spécifiés.

AWS Backup prend en charge les événements suivants :

Type de tâche	Événement
Tâche de sauvegarde	BACKUP_JOB_STARTED BACKUP_JOB_COMPLETED CONTINUOUS_BACKUP_INTERRUPTED
Tâche de copie	COPY_JOB_STARTED COPY_JOB_SUCCESSFUL COPY_JOB_FAILED
Tâche de restauration	RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
Point de récupération	RECOVERY_POINT_MODIFIED
Indexation des points de récupération	RECOVERY_POINT_INDEX_COMPLETED RECOVERY_POINT_INDEX_DELETED RECOVERY_POINT_INDEXING_FAILED

AWS Backup for S3 prend en charge deux événements supplémentaires :

- `S3_BACKUP_OBJECT_FAILED` vous informe de tout échec de la sauvegarde d'un objet S3 lors d'une tâche de sauvegarde avec AWS Backup .
- `S3_RESTORE_OBJECT_FAILED` vous informe de tout échec de la restauration d'un objet S3 lors d'une tâche de restauration avec AWS Backup .

AWS Backup for EKS prend en charge deux événements supplémentaires :

- **EKS_RESTORE_OBJECT_FAILED** vous informe de l' AWS Backup échec de la restauration d'objets EKS au cours d'une tâche de restauration.
- **EKS_RESTORE_OBJECT_SKIPPED** vous informe de tous les objets EKS qui ont été AWS Backup ignorés lors d'une tâche de restauration.

Exemples d'événements

Exemple Exemple : tâche de sauvegarde terminée

```
{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup job was completed successfully. Recovery point  
ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :  
arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :  
1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
      "Timestamp": "2019-08-02T18:46:02.788Z",
      ...
      "MessageAttributes": {
        "EventType": {"Type": "String", "Value": "BACKUP_JOB"},
        "State": {"Type": "String", "Value": "COMPLETED"},
        "AccountId": {"Type": "String", "Value": "123456789012"},
        "Id": {"Type": "String", "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime": {"Type": "String", "Value": "2019-09-02T13:48:52.226Z"}
      }
    }
  ]
}
```

Exemple Exemple : échec de la tâche de sauvegarde

```
{
  "Records": [{
```

```

    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
      "Timestamp": "2019-08-02T18:46:02.788Z",
      ...
      "MessageAttributes": {
        "EventType": {"Type": "String", "Value": "BACKUP_JOB"},
        "State": {"Type": "String", "Value": "FAILED"},
        "AccountId": {"Type": "String", "Value": "123456789012"},
        "Id": {"Type": "String", "Value": "1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime": {"Type": "String", "Value": "2019-09-02T13:48:52.226Z"}
      }
    }
  ]
}

```

Exemple Exemple : la tâche de sauvegarde n'a pas pu être terminée pendant la fenêtre de sauvegarde

```

{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup job failed to complete in time. Resource ARN : arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
      "Timestamp": "2019-08-02T18:46:02.788Z",
      ...
      "MessageAttributes" : {

```



```

        "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
        "State" : {"Type":"String","Value":"EXPIRED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
        "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
    }
}
]]
}

```

Exemple Exemple : indexation des points de récupération terminée

```

{
  "Records": [{
    "EventSource": "aws:sns",
    "EventVersion": "1.0",
    "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
    "Sns": {
      "Type": "Notification",
      "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
      "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
      "Subject": "Notification from AWS Backup",
      "Message": "An AWS Backup backup index job was completed. Indexed recovery
point arn: arn:aws:backup:us-west-2:1112233445566:recovery-point:abcd1234-5678-
abcd-9012-abcdef123456",
      "Timestamp": "2025-05-25T18:46:02.788Z",
      ...
      "MessageAttributes" : {
        "EventType" :
{"Type":"String","Value":"RECOVERY_POINT_INDEXING_COMPLETED"},
        "AccountId" : {"Type":"String","Value":"123456789012"},
        "IndexStatus" : {"Type":"String","Value":"ACTIVE"},
        "IsIndexingContinuous" : {"Type":"String","Value":"false"},
        "RecoveryPointArn" : {"Type":"String","Value":"arn:aws:backup:us-
west-2:1112233445566:recovery-point:abcd1234-5678-abcd-9012-abcdef123456"}
      }
    }
  ]
}

```

AWS Backup exemples de commandes de notification

Vous pouvez utiliser des AWS CLI commandes pour vous abonner aux notifications Amazon SNS relatives à vos AWS Backup événements, les répertorier et les supprimer.

Exemple de notification de mise en place d'un coffre-fort de sauvegarde

La commande suivante s'abonne à une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié qui vous avertit lorsqu'une tâche de restauration est lancée ou terminée, ou lorsqu'un point de récupération est modifié.

```
aws backup put-backup-vault-notifications
  --backup-vault-name myBackupVault
  --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
  --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
  RECOVERY_POINT_MODIFIED
```

Exemple de notification d'obtention d'un coffre-fort de sauvegarde

La commande suivante répertorie tous les événements actuellement abonnés à une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié.

```
aws backup get-backup-vault-notifications
  --backup-vault-name myVault
```

L'exemple de sortie se présente comme suit :

```
{
  "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
  "BackupVaultEvents": [
    "RESTORE_JOB_STARTED",
    "RESTORE_JOB_COMPLETED",
    "RECOVERY_POINT_MODIFIED"
  ],
  "BackupVaultName": "myVault",
  "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

Exemple de notification de suppression d'un coffre-fort de sauvegarde

La commande suivante se désabonne d'une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié.

```
aws backup delete-backup-vault-notifications
--backup-vault-name myVault
```

Spécification AWS Backup en tant que principal de service

Note

AWS Backup Pour autoriser la publication de sujets SNS en votre nom, vous devez le spécifier AWS Backup en tant que principal de service.

Incluez le code JSON suivant dans la politique d'accès de la rubrique Amazon SNS que vous utilisez pour suivre AWS Backup les événements. Vous devez spécifier l'Amazon Resource Name (ARN) de la ressource de votre rubrique.

```
{
  "Sid": "My-statement-id",
  "Effect": "Allow",
  "Principal": {
    "Service": "backup.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Pour plus d'informations sur la spécification d'un principal de service dans une politique d'accès Amazon SNS, consultez la section [Autoriser la publication d'une AWS ressource dans un sujet](#) dans le guide du développeur Amazon Simple Notification Service.

Note

Si votre sujet est crypté, vous devez inclure des autorisations supplémentaires dans votre politique AWS Backup pour autoriser la publication sur celui-ci. Pour plus d'informations sur la possibilité pour les services de publier sur des sujets chiffrés, consultez la section [Activer la compatibilité entre les sources d'événements AWS des services et les sujets cryptés](#) dans le guide du développeur Amazon Simple Notification Service.

Résolution des problèmes AWS Backup

Lors de l'utilisation AWS Backup, il est possible que vous rencontriez des problèmes. Les sections suivantes peuvent vous aider à résoudre les problèmes courants qui peuvent se poser.

Pour les questions d'ordre général AWS Backup, consultez la [AWS Backup FAQ](#). Vous pouvez également rechercher des réponses et publier des questions dans [AWS re:Post](#).

Rubriques

- [Dépannage de problèmes généraux](#)
- [Résolution des problèmes liés à la création de ressources](#)
- [Résolution des problèmes liés à la suppression de ressources](#)
- [Résolution des problèmes liés à la restauration de ressources](#)
- [Résolution des erreurs de formatage](#)

Dépannage de problèmes généraux

Lorsque vous sauvegardez et restaurez des ressources, vous devez être autorisé à utiliser AWS Backup et à accéder aux ressources que vous souhaitez protéger. Le moyen le plus simple d'obtenir les autorisations appropriées est de choisir le Rôle par défaut lorsque vous [attribuez des ressources à un plan de sauvegarde](#). Pour plus d'informations sur le contrôle d'accès à l'aide de Gestion des identités et des accès AWS (IAM) avec AWS Backup, consultez [Contrôle d'accès](#).

Si vous recevez une AccessDenied erreur lorsque vous tentez d'accéder à une AWS Backup ressource, telle qu'un coffre de sauvegarde, cela signifie que la ressource n'existe pas ou que vous n'êtes pas autorisé à y accéder.

Si vous rencontrez des problèmes avec la sauvegarde et la restauration d'un type de ressource particulier, n'hésitez pas à consulter la rubrique de dépannage des sauvegardes et des restaurations relative à cette ressource. Pour plus d'informations, consultez les liens de la section [Fonctionnement AWS Backup avec les AWS services pris en charge](#).

Si vous AWS Backup ne parvenez pas à créer ou à supprimer une ressource, vous pouvez en savoir plus sur le problème en consultant AWS CloudTrail les messages d'erreur ou les journaux. Pour plus d'informations sur l'utilisation CloudTrail avec AWS Backup, consultez [Journalisation des appels d'AWS Backup API avec CloudTrail](#).

Résolution des problèmes liés à la création de ressources

Les informations suivantes peuvent vous aider à résoudre les problèmes que vous rencontrez lors de la création de sauvegardes.

- En général, les services de base de données AWS ne peuvent pas démarrer les sauvegardes 1 heure avant ou pendant leur fenêtre de maintenance ou leur fenêtre de sauvegarde automatique. Amazon FSx ne peut pas démarrer les sauvegardes 4 heures avant ou pendant la fenêtre de maintenance ou la fenêtre de sauvegarde automatique (Amazon Aurora est exempté de cette restriction de fenêtre de maintenance). Les sauvegardes d'instantanés planifiées pendant ces périodes échoueront. Une exception : lorsque vous choisissez d'utiliser AWS Backup à la fois des sauvegardes instantanées et des sauvegardes continues pour un service pris en charge, vous n'avez plus à vous soucier de ces fenêtres, car AWS Backup nous les planifierons pour vous. Consultez la section [Point-in-Time Recovery](#) pour obtenir une liste des services pris en charge et des instructions sur la manière de les utiliser AWS Backup pour effectuer des sauvegardes continues.
- La création de sauvegardes pour les tables DynamoDB échoue lors de la création de tables. La création d'une table DynamoDB prend généralement quelques minutes.
- La sauvegarde des systèmes de fichiers Amazon EFS peut prendre jusqu'à 7 jours lorsque les systèmes de fichiers sont très volumineux. Une seule sauvegarde simultanée à la fois peut être mise en file d'attente pour un système de fichiers Amazon EFS. Si une sauvegarde ultérieure est mise en file d'attente alors qu'une sauvegarde précédente est toujours en cours, la fenêtre de sauvegarde peut expirer et aucune sauvegarde n'est créée.
- Amazon EBS dispose d'un quota souple de 100 000 sauvegardes Région AWS par compte, et les sauvegardes supplémentaires échouent lorsque ce quota est atteint. Si vous atteignez ce quota, vous pouvez supprimer les sauvegardes excédentaires ou demander une augmentation du quota. Pour de plus amples informations sur la demande d'augmentation de quota, consultez [Quotas de service AWS](#).
- Lorsque vous créez des sauvegardes Amazon Relational Database Service (RDS), tenez compte des points suivants :
 - Si vous ne gérez pas AWS Backup à la fois les instantanés Amazon RDS et les sauvegardes continues avec point-in-time restauration, vos sauvegardes échoueront si elles sont lancées si elles sont planifiées ou effectuées à la demande pendant la fenêtre de sauvegarde quotidienne de 30 minutes configurable par l'utilisateur. Pour plus d'informations sur les sauvegardes Amazon RDS automatiques, consultez [Utilisation des sauvegardes](#) dans le Guide de l'utilisateur

Amazon RDS. Vous pouvez éviter cette limitation en utilisant AWS Backup pour gérer à la fois les instantanés Amazon RDS et les sauvegardes continues avec point-in-time restauration.

- Si vous lancez une tâche de sauvegarde depuis la console Amazon RDS, elle peut entrer en conflit avec une tâche de sauvegarde des clusters Aurora, provoquant l'erreur Backup job expired before completion.. Si cela se produit, configurez une fenêtre de sauvegarde plus longue dans AWS Backup.
- AWS Backup ne transmet actuellement pas le groupe d'options TDE lorsqu'une tâche de copie est créée. Si vous avez l'intention d'utiliser ce groupe d'options pour créer des tâches de copie, vous devez utiliser la console Amazon RDS ou l'API Amazon RDS au lieu d'outils AWS Backup . Consultez [Copie d'un groupe d'options](#) dans le Manuel de l'utilisateur Amazon Relational Database Service pour plus d'informations.
- ERREUR : les sauvegardes à la demande sont terminées mais les sauvegardes planifiées échouent avec l'erreur « La clé KMS de l'instantané source n'existe pas, n'est pas activée ou vous n'êtes pas autorisé à y accéder ». La tâche à la demande est terminée, car elle utilise l'appel d'API CopyDBSnapshot, qui ne nécessite pas d'accès à la clé KMS.

SOLUTION : Ajoutez votre rôle IAM à votre clé KMS.

Résolution des problèmes liés à la suppression de ressources

Les points de restauration créés par AWS Backup ne peuvent pas être supprimés dans la fenêtre de console de la ressource protégée. Vous pouvez les supprimer sur la AWS Backup console en les sélectionnant dans le coffre où ils sont stockés, puis en choisissant Supprimer.

Pour supprimer un point de récupération ou un coffre-fort de sauvegarde, vous avez besoin des autorisations appropriées. Pour plus d'informations sur le contrôle d'accès à l'aide d'IAM avec AWS Backup, consultez [Contrôle d'accès](#).

Résolution des problèmes liés à la restauration de ressources

Restauration à l'aide de l'API

Pour restaurer une sauvegarde par programmation, utilisez l'opération d'API [StartRestoreJob](#).

Pour obtenir les métadonnées de configuration avec lesquelles votre sauvegarde a été créée, vous pouvez appeler [GetRecoveryPointRestoreMetadata](#).

Pour plus d'informations, consultez [Restauration d'une sauvegarde](#).

Restauration avec la console

- [Restauration de données Amazon S3](#)
- [Restauration d'une machine virtuelle](#)
- [Restauration d'un système de FSx fichiers Amazon](#)
- [Restauration d'un volume Amazon EBS](#)
- [Restauration d'un système de fichiers Amazon EFS](#)
- [Restauration d'une table Amazon DynamoDB](#)
- [Restauration d'une base de données Amazon RDS](#)
- [Restauration d'un cluster Aurora](#)
- [Restauration d'une EC2 instance Amazon](#)
- [Restauration d'un volume Storage Gateway](#)
- [Restauration d'un cluster Amazon DocumentDB](#)
- [Restauration d'un cluster Neptune](#)

Résolution des erreurs de formatage

Lorsqu'un caractère générique (*) est inclus pour la valeur d'un paramètre, le caractère générique est traité pour inclure des valeurs autres que des espaces. Les valeurs d'une paire clé-valeur contenant des espaces blancs ne seront pas incluses dans le caractère générique.

AWS Backup API

Outre l'utilisation de la console, vous pouvez utiliser les actions de l' AWS Backup API et les types de données pour configurer AWS Backup et gérer ses ressources par programmation. Cette section décrit les actions et les types de données AWS Backup . Il contient la référence d'API pour AWS Backup.

AWS Backup API

- [AWS Backup Actions](#)
- [AWS Backup Types de données](#)

Actions

Les actions suivantes sont prises en charge par AWS Backup :

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)
- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)

- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)
- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)

- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)
- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)

- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)
- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)

- [UpdateTieringConfiguration](#)

Les actions suivantes sont prises en charge par AWS Backup gateway :

- [AssociateGatewayToServer](#)
- [CreateGateway](#)
- [DeleteGateway](#)
- [DeleteHypervisor](#)
- [DisassociateGatewayFromServer](#)
- [GetBandwidthRateLimitSchedule](#)
- [GetGateway](#)
- [GetHypervisor](#)
- [GetHypervisorPropertyMappings](#)
- [GetVirtualMachine](#)
- [ImportHypervisorConfiguration](#)
- [ListGateways](#)
- [ListHypervisors](#)
- [ListTagsForResource](#)
- [ListVirtualMachines](#)
- [PutBandwidthRateLimitSchedule](#)
- [PutHypervisorPropertyMappings](#)
- [PutMaintenanceStartTime](#)
- [StartVirtualMachinesMetadataSync](#)
- [TagResource](#)
- [TestHypervisorConfiguration](#)
- [UntagResource](#)
- [UpdateGatewayInformation](#)
- [UpdateGatewaySoftwareNow](#)
- [UpdateHypervisor](#)

Les actions suivantes sont prises en charge par AWS Backup :

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)
- [ListTagsForResource](#)
- [StartSearchJob](#)
- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

AWS Backup

Les actions suivantes sont prises en charge par AWS Backup :

- [AssociateBackupVaultMpaApprovalTeam](#)
- [CancelLegalHold](#)
- [CreateBackupPlan](#)
- [CreateBackupSelection](#)
- [CreateBackupVault](#)
- [CreateFramework](#)
- [CreateLegalHold](#)
- [CreateLogicallyAirGappedBackupVault](#)
- [CreateReportPlan](#)
- [CreateRestoreAccessBackupVault](#)
- [CreateRestoreTestingPlan](#)
- [CreateRestoreTestingSelection](#)
- [CreateTieringConfiguration](#)
- [DeleteBackupPlan](#)
- [DeleteBackupSelection](#)

- [DeleteBackupVault](#)
- [DeleteBackupVaultAccessPolicy](#)
- [DeleteBackupVaultLockConfiguration](#)
- [DeleteBackupVaultNotifications](#)
- [DeleteFramework](#)
- [DeleteRecoveryPoint](#)
- [DeleteReportPlan](#)
- [DeleteRestoreTestingPlan](#)
- [DeleteRestoreTestingSelection](#)
- [DeleteTieringConfiguration](#)
- [DescribeBackupJob](#)
- [DescribeBackupVault](#)
- [DescribeCopyJob](#)
- [DescribeFramework](#)
- [DescribeGlobalSettings](#)
- [DescribeProtectedResource](#)
- [DescribeRecoveryPoint](#)
- [DescribeRegionSettings](#)
- [DescribeReportJob](#)
- [DescribeReportPlan](#)
- [DescribeRestoreJob](#)
- [DescribeScanJob](#)
- [DisassociateBackupVaultMpaApprovalTeam](#)
- [DisassociateRecoveryPoint](#)
- [DisassociateRecoveryPointFromParent](#)
- [ExportBackupPlanTemplate](#)
- [GetBackupPlan](#)
- [GetBackupPlanFromJSON](#)
- [GetBackupPlanFromTemplate](#)
- [GetBackupSelection](#)

- [GetBackupVaultAccessPolicy](#)
- [GetBackupVaultNotifications](#)
- [GetLegalHold](#)
- [GetRecoveryPointIndexDetails](#)
- [GetRecoveryPointRestoreMetadata](#)
- [GetRestoreJobMetadata](#)
- [GetRestoreTestingInferredMetadata](#)
- [GetRestoreTestingPlan](#)
- [GetRestoreTestingSelection](#)
- [GetSupportedResourceTypes](#)
- [GetTieringConfiguration](#)
- [ListBackupJobs](#)
- [ListBackupJobSummaries](#)
- [ListBackupPlans](#)
- [ListBackupPlanTemplates](#)
- [ListBackupPlanVersions](#)
- [ListBackupSelections](#)
- [ListBackupVaults](#)
- [ListCopyJobs](#)
- [ListCopyJobSummaries](#)
- [ListFrameworks](#)
- [ListIndexedRecoveryPoints](#)
- [ListLegalHolds](#)
- [ListProtectedResources](#)
- [ListProtectedResourcesByBackupVault](#)
- [ListRecoveryPointsByBackupVault](#)
- [ListRecoveryPointsByLegalHold](#)
- [ListRecoveryPointsByResource](#)
- [ListReportJobs](#)
- [ListReportPlans](#)

- [ListRestoreAccessBackupVaults](#)
- [ListRestoreJobs](#)
- [ListRestoreJobsByProtectedResource](#)
- [ListRestoreJobSummaries](#)
- [ListRestoreTestingPlans](#)
- [ListRestoreTestingSelections](#)
- [ListScanJobs](#)
- [ListScanJobSummaries](#)
- [ListTags](#)
- [ListTieringConfigurations](#)
- [PutBackupVaultAccessPolicy](#)
- [PutBackupVaultLockConfiguration](#)
- [PutBackupVaultNotifications](#)
- [PutRestoreValidationResult](#)
- [RevokeRestoreAccessBackupVault](#)
- [StartBackupJob](#)
- [StartCopyJob](#)
- [StartReportJob](#)
- [StartRestoreJob](#)
- [StartScanJob](#)
- [StopBackupJob](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateBackupPlan](#)
- [UpdateFramework](#)
- [UpdateGlobalSettings](#)
- [UpdateRecoveryPointIndexSettings](#)
- [UpdateRecoveryPointLifecycle](#)
- [UpdateRegionSettings](#)
- [UpdateReportPlan](#)

- [UpdateRestoreTestingPlan](#)
- [UpdateRestoreTestingSelection](#)
- [UpdateTieringConfiguration](#)

AssociateBackupVaultMpaApprovalTeam

Service : AWS Backup

Associe une équipe d'approbation MPA à un coffre-fort de sauvegarde.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/mpaApprovalTeam HTTP/1.1
Content-type: application/json

{
  "MpaApprovalTeamArn": "string",
  "RequesterComment": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom du coffre de sauvegarde à associer à l'équipe d'approbation MPA.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

MpaApprovalTeamArn

Le nom de ressource Amazon (ARN) de l'équipe d'approbation du MPA à associer au coffre de sauvegarde.

Type : String

Obligatoire : oui

RequesterComment

Un commentaire fourni par le demandeur expliquant la demande d'association.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

CancelLegalHold

Service : AWS Backup

Supprime le blocage légal spécifié sur un point de récupération. Cette action ne peut être effectuée que par un utilisateur disposant des autorisations suffisantes.

Syntaxe de la demande

```
DELETE /legal-holds/legalHoldId?  
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

CancelDescription

Chaîne qui décrit le motif de la suppression de la suspension légale.

Obligatoire : oui

legalHoldId

L'identifiant de la retenue légale.

Obligatoire : oui

RetainRecordInDays

Le montant entier, en jours, après lequel la suspension légale doit être supprimée.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 201
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateBackupPlan

Service : AWS Backup

Crée un plan de sauvegarde à l'aide d'un nom de plan de sauvegarde et de règles de sauvegarde. Un plan de sauvegarde est un document qui contient des informations permettant de AWS Backup planifier des tâches qui créent des points de récupération pour les ressources.

Si vous appelez CreateBackupPlan avec un plan qui existe déjà, vous recevez une exception `AlreadyExistsException`.

Syntaxe de la demande

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
          {
            "DestinationBackupVaultArn": "string",
            "Lifecycle": {
              "DeleteAfterDays": number,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
```

```

        "ResourceTypes": [ "string" ]
    },
    ],
    "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
    }
    ],
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string" ],
            "ScannerRoleArn": "string"
        }
    ]
    },
    "BackupPlanTags": {
        "string" : "string"
    },
    "CreatorRequestId": "string"
}

```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupPlan](#)

Le corps d'un plan de secours. Comprend un BackupPlanName et un ou plusieurs ensembles de Rules.

Type : objet [BackupPlanInput](#)

Obligatoire : oui

[BackupPlanTags](#)

Les balises à attribuer au plan de sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

[CreatorRequestId](#)

Identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un CreatorRequestId qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AdvancedBackupSettings": [
    {
      "BackupOptions": {
        "string" : "string"
```

```
    },  
    "ResourceType": "string"  
  }  
],  
"BackupPlanArn": "string",  
"BackupPlanId": "string",  
"CreationDate": number,  
"VersionId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AdvancedBackupSettings](#)

Les paramètres d'un type de ressource. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Type : tableau d'objets [AdvancedBackupSetting](#)

[BackupPlanArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : Chaîne

[BackupPlanId](#)

ID du plan de sauvegarde.

Type : Chaîne

[CreationDate](#)

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Ils ne peuvent pas être modifiés.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

CreateBackupSelection

Service : AWS Backup

Crée un document JSON qui spécifie un ensemble de ressources à attribuer à un plan de sauvegarde. Pour des exemples, consultez [Attribution de ressources par programmation](#).

Syntaxe de la demande

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "BackupSelection": {
    "Conditions": [
      {
        "StringEquals": [
          {
            "ConditionKey": "string",
            "ConditionValue": "string"
          }
        ],
        "StringLike": [
          {
            "ConditionKey": "string",
            "ConditionValue": "string"
          }
        ],
        "StringNotEquals": [
          {
            "ConditionKey": "string",
            "ConditionValue": "string"
          }
        ],
        "StringNotLike": [
          {
            "ConditionKey": "string",
            "ConditionValue": "string"
          }
        ]
      },
      {
        "IamRoleArn": "string",
        "ListOfTags": [
          {
            "ConditionKey": "string",
```



```
    "ConditionType": "string",
    "ConditionValue": "string"
  },
  ],
  "NotResources": [ "string" ],
  "Resources": [ "string" ],
  "SelectionName": "string"
},
"CreatorRequestId": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

ID du plan de sauvegarde.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupSelection

Le corps d'une demande visant à affecter un ensemble de ressources à un plan de sauvegarde.

Type : objet BackupSelection

Obligatoire : oui

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "CreationDate": number,
  "SelectionId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanId](#)

ID du plan de sauvegarde.

Type : String

[CreationDate](#)

Date et heure de création d'une sélection de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[SelectionId](#)

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateBackupVault

Service : AWS Backup

Crée un conteneur logique dans lequel sont stockées les sauvegardes. Une demande CreateBackupVault comprend un nom, éventuellement une ou plusieurs balises de ressource, une clé de chiffrement et un ID de demande.

Note

N'incluez pas de données sensibles, telles que des numéros de passeport, dans le nom d'un coffre-fort de sauvegarde.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json
```

```
{
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés. Ces noms sont composés de lettres, de chiffres et de traits d'union.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupVaultTags](#)

Les balises à attribuer au coffre de sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

[CreatorRequestId](#)

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

[EncryptionKeyArn](#)

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple,

arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés. Ces noms sont composés de lettres minuscules, des chiffres et de traits d'union.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

[CreationDate](#)

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`AlreadyExistsException`

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateFramework

Service : AWS Backup

Crée un cadre avec un ou plusieurs contrôles. Un cadre est un ensemble de contrôles que vous pouvez utiliser pour évaluer vos pratiques de sauvegarde. En utilisant des contrôles personnalisables prédéfinis pour définir vos politiques, vous pouvez évaluer si vos pratiques de sauvegarde sont conformes à vos politiques et quelles ressources ne le sont pas encore.

Syntaxe de la demande

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string" : "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "FrameworkName": "string",
  "FrameworkTags": {
    "string" : "string"
  },
  "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[FrameworkControls](#)

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets [FrameworkControl](#)

Obligatoire : oui

[FrameworkDescription](#)

Une description facultative du framework avec 1 024 caractères au maximum.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : .*\\S.*

Obligatoire : non

[FrameworkName](#)

Le nom unique du framework. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

[FrameworkTags](#)

Les balises à attribuer au framework.

Type : mappage chaîne/chaîne

Obligatoire : non

[IdempotencyToken](#)

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `CreateFrameworkInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "FrameworkArn": "string",
  "FrameworkName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[FrameworkArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : String

[FrameworkName](#)

Le nom unique du framework. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateLegalHold

Service : AWS Backup

Crée un blocage légal sur un point de récupération (sauvegarde). Une conservation légale est une restriction associée à la modification ou à la suppression d'une sauvegarde jusqu'à ce qu'un utilisateur autorisé annule la conservation légale. Toute action visant à supprimer ou dissocier un point de récupération échouera avec une erreur si une ou plusieurs conservations légales actives se trouvent sur le point de récupération.

Syntaxe de la demande

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
  "Description": "string",
  "IdempotencyToken": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
    "VaultNames": [ "string" ]
  },
  "Tags": {
    "string" : "string"
  },
  "Title": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Description

Description de la détention légale.

Type : String

Obligatoire : oui

[IdempotencyToken](#)

Il s'agit d'une chaîne choisie par l'utilisateur utilisée pour faire la distinction entre des appels par ailleurs identiques. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

[RecoveryPointSelection](#)

Les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet [RecoveryPointSelection](#)

Obligatoire : non

[Tags](#)

Balises facultatives à inclure. Une balise est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : /.

Type : mappage chaîne/chaîne

Obligatoire : non

[Title](#)

Titre de la retenue légale.

Type : String

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```


Content-type: application/json

```
{
  "CreationDate": number,
  "Description": "string",
  "LegalHoldArn": "string",
  "LegalHoldId": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
    "VaultNames": [ "string" ]
  },
  "Status": "string",
  "Title": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationDate

Heure à laquelle la mise en attente légale a été créée.

Type : Timestamp

Description

Description de la détention légale.

Type : String

LegalHoldArn

L'Amazon Resource Name (ARN) de la conservation légale.

Type : String

LegalHoldId

L'identifiant de la retenue légale.

Type : String

[RecoveryPointSelection](#)

Les critères à attribuer à un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet [RecoveryPointSelection](#)

[Status](#)

Le statut de la mise en attente légale.

Type : String

Valeurs valides : CREATING | ACTIVE | CANCELING | CANCELED

[Title](#)

Titre de la retenue légale.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

CreateLogicallyAirGappedBackupVault

Service : AWS Backup

Crée un conteneur logique dans lequel les sauvegardes peuvent être copiées.

Cette demande inclut un nom, la région, le nombre maximum de jours de rétention, le nombre minimum de jours de rétention et peut éventuellement inclure des balises et un ID de demande de créateur.

Note

N'incluez pas de données sensibles, telles que des numéros de passeport, dans le nom d'un coffre-fort de sauvegarde.

Syntaxe de la demande

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json
```

```
{
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "MaxRetentionDays": number,
  "MinRetentionDays": number
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde logiquement cloisonnés sont identifiés par des noms uniques au compte utilisé pour les créer et la région dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupVaultTags](#)

Les balises à attribuer au coffre.

Type : mappage chaîne/chaîne

Obligatoire : non

[CreatorRequestId](#)

ID de la demande de création.

Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

[EncryptionKeyArn](#)

L'ARN de la clé KMS gérée par le client à utiliser pour chiffrer le coffre-fort de sauvegarde logiquement isolé. Si ce n'est pas spécifié, le coffre-fort sera chiffré à l'aide d'une clé AWS détenue par AWS Backup.

Type : chaîne

Obligatoire : non

[MaxRetentionDays](#)

Période de conservation maximale pendant laquelle le coffre conserve ses points de récupération.

Type : Long

Obligatoire : oui

[MinRetentionDays](#)

Ce paramètre spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération.

La valeur minimale acceptée est de 7 jours.

Type : Long

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number,
  "VaultState": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

L'ARN (Amazon Resource Name) du coffre.

Type : Chaîne

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde logiquement cloisonnés sont identifiés par des noms uniques au compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

CreationDate

Date et heure de la création du coffre-fort.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VaultState

État actuel du coffre.

Type : Chaîne

Valeurs valides : CREATING | AVAILABLE | FAILED

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateReportPlan

Service : AWS Backup

Crée un plan de rapport. Un plan de rapport est un document qui contient des informations sur le contenu du rapport et sur l'endroit où il AWS Backup sera livré.

Si vous appelez CreateReportPlan avec un plan qui existe déjà, vous recevez une exception `AlreadyExistsException`.

Syntaxe de la demande

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ],
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportPlanName": "string",
  "ReportPlanTags": {
    "string" : "string"
  },
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `CreateReportPlanInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

ReportDeliveryChannel

Une structure qui contient des informations sur où et comment livrer vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet [ReportDeliveryChannel](#)

Obligatoire : oui

ReportPlanDescription

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : Chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

ReportPlanName

Le nom unique du plan de rapport. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (`_`).

Type : Chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

[ReportPlanTags](#)

Les balises à attribuer au plan de rapport.

Type : mappage chaîne/chaîne

Obligatoire : non

[ReportSetting](#)

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT |
SCAN_JOB_REPORT

Si le modèle de rapport est RESOURCE_COMPLIANCE_REPORT ou CONTROL_COMPLIANCE_REPORT, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet [ReportSetting](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "ReportPlanArn": "string",
  "ReportPlanName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : Chaîne

ReportPlanName

Le nom unique du plan de rapport.

Type : Chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateRestoreAccessBackupVault

Service : AWS Backup

Crée un coffre-fort de sauvegarde avec accès à la restauration qui fournit un accès temporaire aux points de restauration dans un coffre de sauvegarde logiquement isolé, sous réserve de l'approbation de la MPA.

Syntaxe de la demande

```
PUT /restore-access-backup-vaults HTTP/1.1
Content-type: application/json

{
  "BackupVaultName": "string",
  "BackupVaultTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string",
  "RequesterComment": "string",
  "SourceBackupVaultArn": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupVaultName

Nom du coffre de sauvegarde à associer à une équipe d'approbation MPA.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

BackupVaultTags

Balises facultatives à attribuer au coffre de sauvegarde de l'accès à la restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

CreatorRequestId

Chaîne unique qui identifie la demande et permet aux demandes ayant échoué d'être réessayées sans risquer d'exécuter l'opération deux fois.

Type : chaîne

Obligatoire : non

RequesterComment

Un commentaire expliquant la raison de la demande d'accès à la restauration du coffre de sauvegarde.

Type : chaîne

Obligatoire : non

SourceBackupVaultArn

L'ARN du coffre de sauvegarde source contenant les points de restauration auxquels un accès temporaire est demandé.

Type : String

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationDate": number,
  "RestoreAccessBackupVaultArn": "string",
  "RestoreAccessBackupVaultName": "string",
  "VaultState": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationDate

>Date et heure de création du coffre de sauvegarde de l'accès à la restauration, au format Unix et en temps universel coordonné

Type : Timestamp

RestoreAccessBackupVaultArn

L'ARN qui identifie de manière unique le coffre de sauvegarde d'accès à la restauration créé.

Type : String

RestoreAccessBackupVaultName

Nom du coffre de sauvegarde créé pour l'accès à la restauration.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

VaultState

État actuel du coffre de sauvegarde de l'accès à la restauration.

Type : String

Valeurs valides : CREATING | AVAILABLE | FAILED

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateRestoreTestingPlan

Service : AWS Backup

Crée un plan de test de restauration.

La première des deux étapes pour créer un plan de test de restauration. Une fois cette demande réussie, terminez la procédure en utilisant CreateRestoreTestingSelection.

Syntaxe de la demande

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
  "CreatorRequestId": "string",
  "RestoreTestingPlan": {
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    },
    "RestoreTestingPlanName": "string",
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowHours": number
  },
  "Tags": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[CreatorRequestId](#)

Il s'agit d'une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

[RestoreTestingPlan](#)

Un plan de tests de la restauration doit contenir une chaîne `RestoreTestingPlanName` unique que vous créez et doit contenir un cron `ScheduleExpression`. Vous pouvez éventuellement inclure un nombre entier `StartWindowHours` et une chaîne `CreatorRequestId`.

`RestoreTestingPlanName` est une chaîne unique qui est le nom du plan de test de la restauration. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : objet [RestoreTestingPlanForCreate](#)

Obligatoire : oui

[Tags](#)

Les balises à attribuer au plan de test de restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string"
}
```


Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique le plan de test de la restauration créé.

Type : String

RestoreTestingPlanName

Cette chaîne unique est le nom du plan de test de la restauration.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateRestoreTestingSelection

Service : AWS Backup

Cette demande peut être envoyée une fois que la CreateRestoreTestingPlan demande a été renvoyée avec succès. Il s'agit de la deuxième partie de la création d'un plan de test des ressources, qui doit être réalisée de manière séquentielle.

Cela comprend RestoreTestingSelectionName, ProtectedResourceType et l'un des éléments suivants :

- ProtectedResourceArns
- ProtectedResourceConditions

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour ProtectedResourceArns avec ProtectedResourceConditions. Vous pouvez également inclure jusqu'à 30 ressources protégées spécifiques ARNs dans ProtectedResourceArns.

Impossible de sélectionner à la fois les types de ressources protégées ET les ressources spécifiques ARNs. La demande échouera si les deux sont inclus.

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "CreatorRequestId": "string",
  "RestoreTestingSelection": {
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
      "StringEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ],
      "StringNotEquals": [
        {
```

```
        "Key": "string",
        "Value": "string"
      }
    ],
    "ProtectedResourceType": "string",
    "RestoreMetadataOverrides": {
      "string": "string"
    },
    "RestoreTestingSelectionName": "string",
    "ValidationWindowHours": number
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Entrez le nom du plan de test de restauration renvoyé par la CreateRestoreTestingPlan demande correspondante.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

CreatorRequestId

Il s'agit d'une chaîne unique facultative qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

RestoreTestingSelection

Cela comprend RestoreTestingSelectionName, ProtectedResourceType et l'un des éléments suivants :

- ProtectedResourceArns
- ProtectedResourceConditions

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour ProtectedResourceArns avec ProtectedResourceConditions. Vous pouvez également inclure jusqu'à 30 ressources protégées spécifiques ARNs dans ProtectedResourceArns.

Type : objet [RestoreTestingSelectionForCreate](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Heure à laquelle la sélection des ressources testées a été créée.

Type : Timestamp

[RestoreTestingPlanArn](#)

L'ARN du plan de test de restauration auquel la sélection de test de restauration est associée.

Type : Chaîne

RestoreTestingPlanName

Nom du plan de test de restauration.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

RestoreTestingSelectionName

Nom de la sélection de test de restauration pour le plan de test de restauration associé.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateTieringConfiguration

Service : AWS Backup

Crée une configuration de hiérarchisation.

Une configuration hiérarchisée permet le transfert automatique des données de sauvegarde vers un niveau de stockage moins coûteux en fonction de l'âge des objets sauvegardés dans le coffre de sauvegarde.

Chaque coffre ne peut avoir qu'une seule configuration hiérarchique spécifique au coffre, en plus de toute configuration globale qui s'applique à tous les coffres-forts.

Syntaxe de la demande

```
PUT /tiering-configurations HTTP/1.1
Content-type: application/json

{
  "CreatorRequestId": "string",
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ],
    "TieringConfigurationName": "string"
  },
  "TieringConfigurationTags": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[CreatorRequestId](#)

Il s'agit d'une chaîne unique qui identifie la demande et permet aux demandes ayant échoué d'être réessayées sans risquer d'exécuter l'opération deux fois. Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

[TieringConfiguration](#)

Une configuration de hiérarchisation doit contenir une `TieringConfigurationName` chaîne unique que vous créez et doit contenir un `BackupVaultName` et `ResourceSelection`. Vous pouvez éventuellement inclure une `CreatorRequestId` chaîne.

`TieringConfigurationName` s'agit d'une chaîne unique qui est le nom de la configuration de hiérarchisation. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : objet [TieringConfigurationInputForCreate](#)

Obligatoire : oui

[TieringConfigurationTags](#)

Les balises à attribuer à la configuration de hiérarchisation.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

TieringConfigurationArn

Un Amazon Resource Name (ARN) qui identifie de manière unique la configuration de hiérarchisation créée.

Type : Chaîne

TieringConfigurationName

Cette chaîne unique est le nom de la configuration de hiérarchisation.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 200.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupPlan

Service : AWS Backup

Supprime un plan de sauvegarde. Un plan de sauvegarde ne peut être supprimé qu'une fois que toutes les sélections de ressources associées ont été supprimées. La suppression d'un plan de sauvegarde supprime la version actuelle d'un plan de sauvegarde. Les versions précédentes, le cas échéant, existeront toujours.

Syntaxe de la demande

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupPlanId](#)

Identifie de façon unique un plan de secours.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "DeletionDate": number,
  "VersionId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : String

[BackupPlanId](#)

Identifie de façon unique un plan de secours.

Type : String

[DeletionDate](#)

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[VersionId](#)

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. La version IDs ne peut pas être modifiée.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupSelection

Service : AWS Backup

Supprime la sélection de ressources associée à un plan de sauvegarde spécifié par l'`SelectionId`.

Syntaxe de la demande

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupPlanId](#)

Identifie de façon unique un plan de secours.

Obligatoire : oui

[selectionId](#)

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupVault

Service : AWS Backup

Supprime le coffre-fort de sauvegarde identifié par son nom. Un coffre-fort ne peut être supprimé que s'il est vide.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupVaultAccessPolicy

Service : AWS Backup

Supprime le document de politique qui gère les autorisations sur un coffre-fort de sauvegarde.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés. Ces noms sont composés de lettres minuscules, des chiffres et de traits d'union.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupVaultLockConfiguration

Service : AWS Backup

Supprime AWS Backup Vault Lock d'un coffre-fort de sauvegarde spécifié par un nom de coffre-fort de sauvegarde.

Si la configuration de Vault Lock est immuable, vous ne pouvez pas supprimer Vault Lock à l'aide des opérations de l'API et vous recevrez une `InvalidRequestException` si vous essayez de le faire. Pour plus d'informations, consultez [Vault Lock](#) dans le guide du AWS Backup développeur.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Nom du coffre-fort de sauvegarde dans lequel vous souhaitez supprimer AWS Backup Vault Lock.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteBackupVaultNotifications

Service : AWS Backup

Supprime les notifications d'événement pour le coffre-fort de sauvegarde spécifié.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteFramework

Service : AWS Backup

Supprime le framework spécifié par un nom de framework.

Syntaxe de la demande

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[frameworkName](#)

Le nom unique d'un cadre.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteRecoveryPoint

Service : AWS Backup

Supprime le point de récupération spécifié par un ID de point de récupération.

Si l'ID du point de récupération appartient à une sauvegarde continue, l'appel de ce point de terminaison supprime la sauvegarde continue existante et arrête la sauvegarde continue future.

Lorsque les autorisations d'un rôle IAM sont insuffisantes pour appeler cette API, le service renvoie une réponse HTTP 200 avec un corps HTTP vide, mais le point de récupération n'est pas supprimé. Au lieu de cela, il entre dans un état EXPIRED.

Les points de récupération EXPIRED peuvent être supprimés avec cette API une fois que le rôle IAM a activé l'action `iam:CreateServiceLinkedRole`. Pour en savoir plus sur l'ajout de ce rôle, consultez [Résolution des problèmes liés aux suppressions manuelles](#).

Si l'utilisateur ou le rôle est supprimé ou si l'autorisation associée au rôle est supprimée, la suppression échouera et entrera dans un état EXPIRED.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

[recoveryPointArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteReportPlan

Service : AWS Backup

Supprime le plan de rapport spécifié par un nom de plan de rapport.

Syntaxe de la demande

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[reportPlanName](#)

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteRestoreTestingPlan

Service : AWS Backup

Cette demande supprime le plan de test de la restauration spécifié.

La suppression ne peut réussir que si toutes les sélections de tests de la restauration associées sont d'abord supprimées.

Syntaxe de la demande

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration que vous souhaitez supprimer.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteRestoreTestingSelection

Service : AWS Backup

Entrez le nom du plan de test de la restauration et le nom de la sélection de tests de la restauration.

Toutes les sélections de tests associées à un plan de test de la restauration doivent être supprimées avant que le plan de test de la restauration ne puisse être supprimé.

Syntaxe de la demande

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration contenant la sélection de tests de la restauration que vous souhaitez supprimer.

Obligatoire : oui

RestoreTestingSelectionName

Nom unique obligatoire de la sélection de tests de la restauration que vous souhaitez supprimer.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

DeleteTieringConfiguration

Service : AWS Backup

Supprime la configuration de hiérarchisation spécifiée par un nom de configuration de hiérarchisation.

Syntaxe de la demande

```
DELETE /tiering-configurations/tieringConfigurationName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[tieringConfigurationName](#)

Nom unique d'une configuration de hiérarchisation.

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeBackupJob

Service : AWS Backup

Renvoie les détails de la tâche de sauvegarde pour l'`BackupJobId` spécifié.

Syntaxe de la demande

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[`backupJobId`](#)

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupJobId": "string",
  "BackupOptions": {
    "string" : "string"
  },
  "BackupSizeInBytes": number,
  "BackupType": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "BytesTransferred": number,
  "ChildJobsInState": {
    "string" : number
  },
}
```

```

"CompletionDate": number,
"CreatedBy": {
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "BackupPlanName": "string",
  "BackupPlanVersion": "string",
  "BackupRuleCron": "string",
  "BackupRuleId": "string",
  "BackupRuleName": "string",
  "BackupRuleTimezone": "string"
},
"CreationDate": number,
"EncryptionKeyArn": "string",
"ExpectedCompletionDate": number,
"IamRoleArn": "string",
"InitiationDate": number,
"IsEncrypted": boolean,
"IsParent": boolean,
"MessageCategory": "string",
"NumberOfChildJobs": number,
"ParentJobId": "string",
"PercentDone": "string",
"RecoveryPointArn": "string",
"RecoveryPointLifecycle": {
  "DeleteAfterDays": number,
  "DeleteAfterEvent": "string",
  "MoveToColdStorageAfterDays": number,
  "OptInToArchiveForSupportedResources": boolean
},
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"StartBy": number,
"State": "string",
"StatusMessage": "string",
"VaultLockState": "string",
"VaultType": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AccountId](#)

Renvoie l'ID de compte du propriétaire de la tâche de sauvegarde.

Type : Chaîne

Modèle : `^[0-9]{12}$`

[BackupJobId](#)

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : Chaîne

[BackupOptions](#)

Représente les options spécifiées dans le cadre du plan de sauvegarde ou de la tâche de sauvegarde à la demande.

Type : mappage chaîne/chaîne

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[BackupSizeInBytes](#)

Taille, en octets, d'une sauvegarde (point de restauration).

Cette valeur peut s'afficher différemment selon le type de ressource, car AWS Backup elle extrait des informations de données provenant d'autres AWS services. Par exemple, la valeur renvoyée peut afficher une valeur de 0, qui peut être différente de la valeur prévue.

Le comportement attendu pour les valeurs par type de ressource est décrit comme suit :

- Amazon Aurora, Amazon DocumentDB et Amazon Neptune n'ont pas cette valeur renseignée à partir de l'opération. `GetBackupJobStatus`
- Pour Amazon DynamoDB doté de fonctionnalités avancées, cette valeur fait référence à la taille du point de restauration (sauvegarde).
- Amazon EC2 et Amazon EBS indiquent la taille du volume (stockage provisionné) renvoyé dans le cadre de cette valeur. Amazon EBS ne renvoie pas d'informations sur la taille de sauvegarde ; la taille de l'instantané aura la même valeur que la ressource d'origine sauvegardée.

- Pour Amazon EFS, cette valeur fait référence aux octets delta transférés lors d'une sauvegarde.
- Amazon FSx ne renseigne pas cette valeur à partir de l'opération `GetBackupJobStatus` pour les systèmes de FSx fichiers.
- Une instance Amazon RDS s'affichera sous la forme 0.
- Pour les machines virtuelles en cours d'exécution VMware, cette valeur est transmise AWS Backup via un flux de travail asynchrone, ce qui peut signifier que la valeur affichée peut sous-représenter la taille réelle de la sauvegarde.

Type : Long

[BackupType](#)

Représente le type de sauvegarde réel sélectionné pour une tâche de sauvegarde. Par exemple, si une sauvegarde Windows Volume Shadow Copy Service (VSS) a bien été effectuée, `BackupType` renvoie "WindowsVSS". Si `BackupType` est vide, le type de sauvegarde était une sauvegarde normale.

Type : Chaîne

[BackupVaultArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

[BytesTransferred](#)

Taille en octets transférée vers un coffre-fort de sauvegarde au moment où le statut de la tâche a été demandé.

Type : Long

[ChildJobsInState](#)

Cela renvoie les statistiques des tâches de sauvegarde enfant (imbriquées) incluses.

Type : mappage chaîne/long

Clés valides : CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

[CompletionDate](#)

Date et heure de fin d'une tâche de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[CreatedBy](#)

Contient des informations d'identification relatives à la création d'une tâche de sauvegarde, dont `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour la créer.

Type : objet [RecoveryPointCreator](#)

[CreationDate](#)

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[EncryptionKeyArn](#)

Le nom de ressource Amazon (ARN) de la clé KMS utilisée pour chiffrer la sauvegarde. Il peut s'agir d'une clé gérée par le client ou d'une clé AWS gérée, selon la configuration du coffre-fort.

Type : Chaîne

[ExpectedCompletionDate](#)

Date et heure de fin attendues d'une tâche de sauvegarde des ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `ExpectedCompletionDate` est précise

en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

InitiationDate

Date à laquelle une tâche de sauvegarde a été initiée.

Type : Timestamp

IsEncrypted

Valeur booléenne indiquant si la sauvegarde est cryptée. Toutes les sauvegardes AWS Backup sont cryptées, mais ce champ indique l'état du chiffrement pour des raisons de transparence.

Type : Boolean

IsParent

Cela renvoie la valeur booléenne indiquant qu'une tâche de sauvegarde est une tâche parent (composite).

Type : Boolean

MessageCategory

Nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `INVALIDPARAMETERS`. Consultez [la section Surveillance](#) pour obtenir la liste des `MessageCategory` chaînes acceptées.

Type : Chaîne

NumberOfChildJobs

Cela renvoie le nombre de tâches de sauvegarde enfant (imbriquées).

Type : Long

ParentJobId

Cela renvoie l'ID de la tâche de sauvegarde de la ressource parent (composite).

Type : Chaîne

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : Chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple,

```
arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.
```

Type : Chaîne

RecoveryPointLifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Type : objet [Lifecycle](#)

ResourceArn

Un ARN qui identifie de façon unique une ressource enregistrée. Le format de l'ARN dépend du type de ressource.

Type : Chaîne

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : Chaîne

ResourceType

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

StartBy

Spécifie l'heure au format Unix et au format UTC (Coordinated Universal Time) quand une tâche de sauvegarde doit être démarrée avant d'être annulée. La valeur est calculée en ajoutant la fenêtre de démarrage à l'heure planifiée. Ainsi, si l'heure prévue était 18 h 00 et que la fenêtre de début était de 2 heures, l'heure `StartBy` serait 20 h 00 à la date spécifiée. La valeur de `StartBy` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

State

L'état actuel d'une tâche de sauvegarde.

Type : Chaîne

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Message détaillé expliquant le statut de la tâche de sauvegarde d'une ressource.

Type : Chaîne

VaultLockState

État de verrouillage du coffre-fort de sauvegarde. Pour les coffres-forts à espacement logique, cela indique si le coffre-fort est verrouillé en mode de conformité. Les valeurs valides sont LOCKED et UNLOCKED.

Type : Chaîne

VaultType

Type de coffre-fort de sauvegarde dans lequel le point de restauration est stocké. Les valeurs valides concernent BACKUP_VAULT les coffres-forts de sauvegarde standard et les coffres-forts LOGICALLY_AIR_GAPPED_BACKUP_VAULT à espacement logique.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

DependencyFailureException

Un AWS service ou une ressource dépendant a renvoyé une erreur au AWS Backup service et l'action ne peut pas être terminée.

Context

Type

Code d'état HTTP : 500

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeBackupVault

Service : AWS Backup

Renvoie les métadonnées relatives à un coffre-fort de sauvegarde spécifié par son nom.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CreationDate": number,
  "CreatorRequestId": "string",
  "EncryptionKeyArn": "string",
  "EncryptionKeyType": "string",
  "LatestMpaApprovalTeamUpdate": {
```

```
    "ExpiryDate": number,
    "InitiationDate": number,
    "MpaSessionArn": "string",
    "Status": "string",
    "StatusMessage": "string"
  },
  "LockDate": number,
  "Locked": boolean,
  "MaxRetentionDays": number,
  "MinRetentionDays": number,
  "MpaApprovalTeamArn": "string",
  "MpaSessionArn": "string",
  "NumberOfRecoveryPoints": number,
  "SourceBackupVaultArn": "string",
  "VaultState": "string",
  "VaultType": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : Chaîne

CreationDate

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[CreatorRequestId](#)

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : Chaîne

[EncryptionKeyArn](#)

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple,
`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : Chaîne

[EncryptionKeyType](#)

Type de clé de chiffrement utilisée pour le coffre de sauvegarde. Les valeurs valides sont `CUSTOMER_MANAGED_KMS_KEY` pour les clés gérées par le client ou `_OWNED_KMS_KEY` pour les clés détenues par le client. AWS AWS

Type : Chaîne

Valeurs valides : `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

[LatestMpaApprovalTeamUpdate](#)

Informations sur la dernière mise à jour de l'association de l'équipe d'approbation MPA pour ce coffre de sauvegarde.

Type : objet [LatestMpaApprovalTeamUpdate](#)

[LockDate](#)

Date et heure auxquelles la configuration de AWS Backup Vault Lock ne peut pas être modifiée ou supprimée.

Si vous avez appliqué Vault Lock à votre coffre-fort sans spécifier de date de verrouillage, vous pouvez modifier les paramètres de Vault Lock ou supprimer complètement Vault Lock du coffre-fort à tout moment.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[Locked](#)

Un booléen qui indique si AWS Backup Vault Lock protège actuellement le coffre-fort de sauvegarde. True signifie que Vault Lock entraîne l'échec des opérations de suppression ou de mise à jour sur les points de récupération stockés dans le coffre-fort.

Type : Boolean

[MaxRetentionDays](#)

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, Vault Lock n'applique pas de période de rétention maximale sur les points de récupération dans le coffre-fort (permettant un stockage indéfini).

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou inférieure à la période de rétention maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : Long

[MinRetentionDays](#)

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'appliquera pas de période de conservation minimale.

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou supérieure à la période de rétention minimale. Si la période de rétention de la tâche est plus courte que cette période de rétention minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : Long

[MpaApprovalTeamArn](#)

L'ARN de l'équipe d'approbation MPA associée à ce coffre de sauvegarde.

Type : Chaîne

[MpaSessionArn](#)

L'ARN de la session MPA associée à ce coffre de sauvegarde.

Type : Chaîne

[NumberOfRecoveryPoints](#)

Nombre de points de récupération stockés dans un coffre-fort de sauvegarde.

La valeur du nombre de points de récupération affichée dans la console peut être approximative. Utilisez l'API [ListRecoveryPointsByBackupVault](#) pour obtenir le nombre exact.

Type : Long

[SourceBackupVaultArn](#)

L'ARN du coffre de sauvegarde source à partir duquel ce coffre de sauvegarde d'accès à la restauration a été créé.

Type : Chaîne

[VaultState](#)

État actuel du coffre. ->

Type : Chaîne

Valeurs valides : CREATING | AVAILABLE | FAILED

[VaultType](#)

Type de coffre décrit.

Type : Chaîne

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeCopyJob

Service : AWS Backup

Renvoie les métadonnées associées à la création d'une copie d'une ressource.

Syntaxe de la demande

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

copyJobId

Identifie de manière unique une tâche de copie.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJob": {
    "AccountId": "string",
    "BackupSizeInBytes": number,
    "ChildJobsInState": {
      "string" : number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
```

```

    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreatedByBackupJobId": "string",
  "CreationDate": number,
  "DestinationBackupVaultArn": "string",
  "DestinationEncryptionKeyArn": "string",
  "DestinationRecoveryPointArn": "string",
  "DestinationRecoveryPointLifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "DestinationVaultLockState": "string",
  "DestinationVaultType": "string",
  "IamRoleArn": "string",
  "IsParent": boolean,
  "MessageCategory": "string",
  "NumberOfChildJobs": number,
  "ParentJobId": "string",
  "ResourceArn": "string",
  "ResourceName": "string",
  "ResourceType": "string",
  "SourceBackupVaultArn": "string",
  "SourceRecoveryPointArn": "string",
  "State": "string",
  "StatusMessage": "string"
}
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CopyJob](#)

Contient des informations détaillées sur une tâche de copie.

Type : objet [CopyJob](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeFramework

Service : AWS Backup

Renvoie les détails du framework pour le paramètre FrameworkName spécifié.

Syntaxe de la demande

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

frameworkName

Le nom unique d'un cadre.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "DeploymentStatus": "string",
  "FrameworkArn": "string",
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ]
    }
  ]
}
```

```

    ],
    "ControlName": "string",
    "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
            "string" : "string"
        }
    }
}
],
"FrameworkDescription": "string",
"FrameworkName": "string",
"FrameworkStatus": "string",
"IdempotencyToken": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, 2020-07-10T15:00:00.000-08:00 représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

DeploymentStatus

Le statut du déploiement d'un framework. Les statuts sont les suivants :

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED
| FAILED

Type : String

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : String

FrameworkControls

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets [FrameworkControl](#)

FrameworkDescription

Description facultative du framework.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : .*\\S.*

FrameworkName

Le nom unique d'un cadre.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

FrameworkStatus

Un cadre est constitué d'un ou plusieurs contrôles. Chaque contrôle régit une ressource, telle que les plans de sauvegarde, les sélections de sauvegarde, les coffres-forts de sauvegarde ou les points de récupération. Vous pouvez également activer ou désactiver AWS Config l'enregistrement pour chaque ressource. Les statuts sont les suivants :

- **ACTIVE** lorsque l'enregistrement est activé pour toutes les ressources que le framework gouverne.
- **PARTIALLY_ACTIVE** lorsque l'enregistrement est désactivé pour au moins une ressource que le framework gouverne.
- **INACTIVE** lorsque l'enregistrement est désactivé pour toutes les ressources que le framework gouverne.
- **UNAVAILABLE** lorsqu'il n'y a pas d'AWS Backup en mesure de valider le statut de l'enregistrement pour le moment.

Type : String

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `DescribeFrameworkOutput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeGlobalSettings

Service : AWS Backup

Décrit si le AWS compte est activé pour la sauvegarde entre comptes. Renvoie une erreur si le compte n'est pas membre d'une organisation Organizations. Exemple : `describe-global-settings --region us-west-2`

Syntaxe de la demande

```
GET /global-settings HTTP/1.1
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "GlobalSettings": {
    "string" : "string"
  },
  "LastUpdateTime": number
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[GlobalSettings](#)

L'état des drapeaux `isCrossAccountBackupEnabled` `isMpaEnabled` (« Mpa » fait référence à une approbation multipartite), `etisDelegatedAdministratorEnabled`.

Type : mappage chaîne/chaîne

LastUpdateTime

Date et heure de la dernière mise à jour de l'indicateur `isCrossAccountBackupEnabled`. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeProtectedResource

Service : AWS Backup

Renvoie des informations sur une ressource enregistrée, notamment la dernière fois qu'elle a été sauvegardée, son Amazon Resource Name (ARN) et le type de AWS service de la ressource enregistrée.

Syntaxe de la demande

```
GET /resources/resourceArn HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[resourceArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "LastBackupTime": number,
  "LastBackupVaultArn": "string",
  "LastRecoveryPointArn": "string",
  "LatestRestoreExecutionTimeMinutes": number,
  "LatestRestoreJobCreationDate": number,
  "LatestRestoreRecoveryPointCreationDate": number,
  "ResourceArn": "string",
  "ResourceName": "string",
  "ResourceType": "string"
}
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LastBackupTime

Date et heure de la dernière sauvegarde d'une ressource, au format Unix et au format UTC (temps universel coordonné). La valeur de LastBackupTime est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

LastBackupVaultArn

L'ARN (Amazon Resource Name) du coffre de sauvegarde qui contient le point de restauration de sauvegarde le plus récent.

Type : String

LastRecoveryPointArn

L'ARN (Amazon Resource Name) du point de récupération le plus récent.

Type : String

LatestRestoreExecutionTimeMinutes

Durée, en minutes, nécessaire à l'exécution de la dernière tâche de restauration.

Type : long

LatestRestoreJobCreationDate

Date de création de la tâche de restauration la plus récente.

Type : Timestamp

LatestRestoreRecoveryPointCreationDate

Date à laquelle le point de récupération le plus récent a été créé.

Type : Timestamp

[ResourceArn](#)

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : String

[ResourceName](#)

Nom de la ressource appartenant à la sauvegarde spécifiée.

Type : String

[ResourceType](#)

Type de AWS ressource enregistrée en tant que point de récupération ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeRecoveryPoint

Service : AWS Backup

Renvoie les métadonnées associées à un point de récupération, notamment l'ID, le statut, le chiffrement et le cycle de vie.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?  
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

Modèle : `^[0-9]{12}$`

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

HTTP/1.1 200

Content-type: application/json

```
{
  "BackupSizeInBytes": number,
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "CompletionDate": number,
  "CompositeMemberIdentifier": "string",
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanName": "string",
    "BackupPlanVersion": "string",
    "BackupRuleCron": "string",
    "BackupRuleId": "string",
    "BackupRuleName": "string",
    "BackupRuleTimezone": "string"
  },
  "CreationDate": number,
  "EncryptionKeyArn": "string",
  "EncryptionKeyType": "string",
  "IamRoleArn": "string",
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "InitiationDate": number,
  "IsEncrypted": boolean,
  "IsParent": boolean,
  "LastRestoreTime": number,
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "ParentRecoveryPointArn": "string",
  "RecoveryPointArn": "string",
  "ResourceArn": "string",
```

```

"ResourceName": "string",
"ResourceType": "string",
"ScanResults": [
  {
    "Findings": [ "string" ],
    "LastScanTimestamp": number,
    "MalwareScanner": "string",
    "ScanJobState": "string"
  }
],
"SourceBackupVaultArn": "string",
"Status": "string",
"StatusMessage": "string",
"StorageClass": "string",
"VaultType": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : Long

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

CalculatedLifecycle

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet [CalculatedLifecycle](#)

CompletionDate

Date et heure de fin d'une tâche de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'[ID logique](#) au sein d'une pile.

Type : Chaîne

CreatedBy

Contient des informations d'identification relatives à la création d'un point de récupération, notamment les valeurs `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour le créer.

Type : objet [RecoveryPointCreator](#)

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

EncryptionKeyArn

Clé de chiffrement côté serveur utilisée pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : Chaîne

EncryptionKeyType

Type de clé de chiffrement utilisée pour le point de récupération. Les valeurs valides sont CUSTOMER_MANAGED_KMS_KEY pour les clés gérées par le client ou _OWNED_KMS_KEY pour les clés détenues par le client. AWS AWS

Type : Chaîne

Valeurs valides : AWS_OWNED_KMS_KEY | CUSTOMER_MANAGED_KMS_KEY

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, arn:aws:iam::123456789012:role/S3Access.

Type : Chaîne

IndexStatus

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : PENDING | ACTIVE | FAILED DELETING

Un point de récupération dont l'index a le statut de ACTIVE peut être inclus dans une recherche.

Type : Chaîne

Valeurs valides : PENDING | ACTIVE | FAILED | DELETING

IndexStatusMessage

Chaîne sous la forme d'un message détaillé expliquant l'état d'un index de sauvegarde associé au point de restauration.

Type : Chaîne

InitiationDate

Date et heure auxquelles la tâche de sauvegarde qui a créé ce point de restauration a été lancée, au format Unix et en temps universel coordonné (UTC).

Type : Timestamp

IsEncrypted

Valeur booléenne renvoyée comme TRUE si le point de récupération spécifié était chiffré ou FALSE s'il n'était pas chiffré.

Type : Boolean

IsParent

Cela renvoie la valeur booléenne indiquant qu'un point de récupération est une tâche parent (composite).

Type : Boolean

LastRestoreTime

Date et heure de la dernière restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de LastRestoreTime est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet [Lifecycle](#)

[ParentRecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération parent (composite) ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

[RecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

[ResourceArn](#)

Un ARN qui identifie de façon unique une ressource enregistrée. Le format de l'ARN dépend du type de ressource.

Type : Chaîne

[ResourceName](#)

Nom de la ressource appartenant à la sauvegarde spécifiée.

Type : Chaîne

[ResourceType](#)

Type de AWS ressource à enregistrer comme point de récupération ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ScanResults](#)

Contient les derniers résultats d'analyse par rapport au point de récupération et inclut actuellement `MalwareScannerScanJobState`, `Findings`, et `LastScanTimestamp`

Type : tableau d'objets [ScanResult](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 5 éléments.

SourceBackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique le coffre-fort source dans lequel la ressource a été initialement sauvegardée ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Si la restauration est rétablie sur le même AWS compte ou la même région, cette valeur sera `null`.

Type : Chaîne

Status

Code de statut spécifiant l'état du point de récupération. Pour plus d'informations, consultez la section [État du point de récupération](#) dans le guide du AWS Backup développeur.

- **CREATING**Le statut indique qu'une AWS Backup tâche a été initiée pour une ressource. Le processus de sauvegarde a démarré et traite activement une tâche de sauvegarde pour le point de restauration associé.
- **AVAILABLE**Le statut indique que la sauvegarde a été créée avec succès pour le point de restauration. Le processus de sauvegarde s'est terminé sans problème et le point de restauration est maintenant prêt à être utilisé.
- **PARTIAL**L'état indique qu'un point de restauration composite possède un ou plusieurs points de restauration imbriqués qui ne figuraient pas dans la sauvegarde.
- **EXPIRED**Le statut indique que le point de restauration a dépassé sa période de rétention, mais qu'il n'est AWS Backup pas autorisé ou qu'il est incapable de le supprimer pour une autre raison. Pour supprimer manuellement ces points de récupération, voir [Étape 3 : Supprimer les points de récupération](#) dans la section Nettoyage des ressources du guide Mise en route.
- Le statut **STOPPED** apparaît lors d'une sauvegarde continue lorsqu'un utilisateur a effectué une action qui entraîne la désactivation de la sauvegarde continue. Cela peut être dû à la suppression des autorisations, à la désactivation de la gestion des versions, à la désactivation des événements envoyés ou à EventBridge la désactivation des EventBridge règles mises en place par AWS Backup Pour les points de restauration des ressources Amazon S3, Amazon RDS et Amazon Aurora, cet état se produit lorsque la période de rétention d'une règle de sauvegarde continue est modifiée.

Pour résoudre le statut **STOPPED**, assurez-vous que toutes les autorisations demandées sont en place et que la gestion des versions est activée sur le compartiment S3. Une fois ces conditions remplies, la prochaine instance d'une règle de sauvegarde exécutée entraînera la

création d'un nouveau point de récupération continue. Les points de récupération ayant le statut ARRÊTÉ n'ont pas besoin d'être supprimés.

Pour SAP HANA on Amazon, le EC2 STOPPED statut est dû à une action de l'utilisateur, à une mauvaise configuration de l'application ou à un échec de sauvegarde. Pour garantir le succès des futures sauvegardes continues, reportez-vous au statut du point de récupération et consultez SAP HANA pour plus de détails.

Type : Chaîne

Valeurs valides : COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

StatusMessage

Message de statut expliquant le statut du point de récupération.

Type : Chaîne

StorageClass

Spécifie la classe de stockage du point de récupération. Les valeurs valides sont WARM ou COLD.

Type : Chaîne

Valeurs valides : WARM | COLD | DELETED

VaultType

Type de coffre-fort dans lequel le point de récupération décrit est stocké.

Type : Chaîne

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT | RESTORE_ACCESS_BACKUP_VAULT

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeRegionSettings

Service : AWS Backup

Renvoie les paramètres actuels d'activation du service pour la région. Si l'opt-in est activé pour un service, AWS Backup essaie de protéger les ressources de ce service dans cette région, lorsque la ressource est incluse dans une sauvegarde à la demande ou un plan de sauvegarde planifiée. Sinon, AWS Backup n'essaie pas de protéger les ressources de ce service dans cette région.

Syntaxe de la demande

```
GET /account-settings HTTP/1.1
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypeManagementPreference": {
    "string" : boolean
  },
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ResourceTypeManagementPreference](#)

Indique si les sauvegardes d'un type de ressource sont AWS Backup entièrement gérées.

Pour connaître les avantages de la AWS Backup gestion complète, consultez la section [AWS Backup Gestion complète](#).

Pour obtenir la liste des types de ressources et savoir si chacun prend en charge AWS Backup la gestion complète, consultez le tableau [Disponibilité des fonctionnalités par ressource](#).

Si "DynamoDB" : false, vous pouvez activer la AWS Backup gestion complète de la sauvegarde DynamoDB en activant les [fonctionnalités avancées AWS Backup de sauvegarde DynamoDB](#).

Type : chaîne vers un mappage booléen

Modèle de clé : ^[a-zA-Z0-9\-_\.\.]{1,50}\$

[ResourceTypeOptInPreference](#)

Les services ainsi que les préférences d'inscription dans la région.

Type : chaîne vers un mappage booléen

Modèle de clé : ^[a-zA-Z0-9\-_\.\.]{1,50}\$

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeReportJob

Service : AWS Backup

Renvoie les détails associés à la création d'un rapport tel que spécifié par son `ReportJobId`.

Syntaxe de la demande

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportJobId

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. L'ID de tâche de rapport ne peut pas être modifié.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportJob": {
    "CompletionTime": number,
    "CreationTime": number,
    "ReportDestination": {
      "S3BucketName": "string",
      "S3Keys": [ "string" ]
    },
    "ReportJobId": "string",
    "ReportPlanArn": "string",
    "ReportTemplate": "string",
    "Status": "string",
```

```
    "StatusMessage": "string"  
  }  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ReportJob](#)

Informations relatives à une tâche de rapport, notamment ses heures d'achèvement et de création, la destination du rapport, l'identifiant unique de la tâche de rapport, le nom de ressource Amazon (ARN), le modèle de rapport, le statut et le message de statut.

Type : objet [ReportJob](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeReportPlan

Service : AWS Backup

Renvoie la liste de tous les plans de rapport pour un Compte AWS et Région AWS.

Syntaxe de la demande

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportPlan": {
    "CreationTime": number,
    "DeploymentStatus": "string",
    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
    }
  }
}
```

```
    },
    "ReportPlanArn": "string",
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
    }
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ReportPlan](#)

Renvoie des informations sur le plan de rapport spécifié par son nom. Ces informations incluent l'Amazon Resource Name (ARN), la description, les paramètres, le canal de livraison, le statut du déploiement, l'heure de création et les dernières tentatives d'exécution du plan de rapport ainsi que celles ayant réussi.

Type : objet [ReportPlan](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeRestoreJob

Service : AWS Backup

Renvoie les métadonnées associées à une tâche de restauration spécifiée par un ID de tâche.

Syntaxe de la demande

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[restoreJobId](#)

Identifie de manière unique la tâche qui restaure un point de récupération.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupSizeInBytes": number,
  "BackupVaultArn": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "RestoreTestingPlanArn": "string"
  },
  "CreatedResourceArn": "string",
  "CreationDate": number,
  "DeletionStatus": "string",
  "DeletionStatusMessage": "string",
  "ExpectedCompletionTimeMinutes": number,
  "IamRoleArn": "string",
```

```
"IsParent": boolean,  
"ParentJobId": "string",  
"PercentDone": "string",  
"RecoveryPointArn": "string",  
"RecoveryPointCreationDate": number,  
"ResourceType": "string",  
"RestoreJobId": "string",  
"SourceResourceArn": "string",  
"Status": "string",  
"StatusMessage": "string",  
"ValidationStatus": "string",  
"ValidationStatusMessage": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccountId

Renvoie l'ID de compte du propriétaire de la tâche de restauration.

Type : Chaîne

Modèle : `^[0-9]{12}$`

BackupSizeInBytes

Taille, en octets, de la ressource restaurée.

Type : Long

BackupVaultArn

Nom de ressource Amazon (ARN) du coffre de sauvegarde contenant le point de restauration. Cela permet d'identifier les politiques et les autorisations d'accès au coffre-fort.

Type : Chaîne

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de CompletionDate est précise en

millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de restauration.

Type : objet [RestoreJobCreator](#)

CreatedResourceArn

Le nom de ressource Amazon (ARN) de la ressource créée par la tâche de restauration.

Le format de l'ARN dépend du type de ressource sauvegardée.

Type : Chaîne

CreationDate

Date et heure de création d'une tâche de restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

DeletionStatus

État des données générées par le test de restauration.

Type : Chaîne

Valeurs valides : DELETING | FAILED | SUCCESSFUL

DeletionStatusMessage

Cela décrit le statut de suppression de la tâche de restauration.

Type : Chaîne

ExpectedCompletionTimeMinutes

Durée en minutes prévue d'une tâche de restauration d'un point de récupération.

Type : Long

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

IsParent

Il s'agit d'une valeur booléenne indiquant si la tâche de restauration est une tâche de restauration parent (composite).

Type : Boolean

ParentJobId

Il s'agit de l'identifiant unique de la tâche de restauration parent pour la tâche de restauration sélectionnée.

Type : Chaîne

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : Chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

RecoveryPointCreationDate

Date de création du point de restauration créé par la tâche de restauration spécifiée.

Type : Timestamp

ResourceType

Renvoie les métadonnées associées à une tâche de restauration répertoriées par type de ressource.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

[RestoreJobId](#)

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : Chaîne

[SourceResourceArn](#)

Le nom de ressource Amazon (ARN) de la ressource d'origine qui a été sauvegardée. Cela fournit un contexte sur la ressource en cours de restauration.

Type : Chaîne

[Status](#)

Code d'état spécifiant l'état de la tâche initiée AWS Backup pour restaurer un point de restauration.

Type : Chaîne

Valeurs valides : PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[StatusMessage](#)

Message indiquant le statut d'une tâche de restauration d'un point de récupération.

Type : Chaîne

[ValidationStatus](#)

État de la validation exécutée sur la tâche de restauration indiquée.

Type : Chaîne

Valeurs valides : FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

[ValidationStatusMessage](#)

Message d'état.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

DependencyFailureException

Un AWS service ou une ressource dépendant a renvoyé une erreur au AWS Backup service et l'action ne peut pas être terminée.

Context

Type

Code d'état HTTP : 500

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DescribeScanJob

Service : AWS Backup

Renvoie les détails de la tâche de numérisation pour l' ScanJobID spécifié.

Syntaxe de la demande

```
GET /scan/jobs/ScanJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ScanJobId

Identifie de manière unique une demande AWS Backup d'analyse d'une ressource.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountId": "string",
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "CompletionDate": number,
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": number,
  "IamRoleArn": "string",
  "MalwareScanner": "string",
```

```

"RecoveryPointArn": "string",
"ResourceArn": "string",
"ResourceName": "string",
"ResourceType": "string",
"ScanBaseRecoveryPointArn": "string",
"ScanId": "string",
"ScanJobId": "string",
"ScanMode": "string",
"ScannerRoleArn": "string",
"ScanResult": {
  "ScanResultStatus": "string"
},
"State": "string",
"StatusMessage": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccountId

Renvoie l'ID du compte auquel appartient la tâche de numérisation.

Modèle : `^[0-9]{12}$`

Type : Chaîne

BackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de manière unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Type : Chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Modèle : `^[a-zA-Z0-9\-\_\.\-]{2,50}$`

Type : Chaîne

CompletionDate

Date et heure de fin de création d'un index de sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche d'analyse, notamment le plan de sauvegarde et la règle à l'origine de l'analyse.

Type : objet [ScanJobCreator](#)

CreationDate

Date et heure de fin de création d'un index de sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IamRoleArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

MalwareScanner

Moteur d'analyse utilisé pour la tâche de numérisation correspondante. Actuellement, seul `GUARDUTY` est pris en charge.

Type : Chaîne

Valeurs valides : `GUARDDUTY`

RecoveryPointArn

Un ARN qui identifie de manière unique le point de récupération cible à scanner. ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

[ResourceArn](#)

Un ARN qui identifie de manière unique la ressource source de l'ARN du point de récupération correspondant.

Type : Chaîne

[ResourceName](#)

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : Chaîne

[ResourceType](#)

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS).

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Type : Chaîne

Valeurs valides : EBS | EC2 | S3

[ScanBaseRecoveryPointArn](#)

Un ARN qui identifie de manière unique le point de récupération de base à scanner. Ce champ ne sera rempli que lorsqu'une tâche de numérisation incrémentielle aura eu lieu.

Type : Chaîne

[ScanId](#)

L'ID de scan généré par Amazon GuardDuty pour la demande d'ID de scan Job correspondante auprès de AWS Backup.

Type : Chaîne

[ScanJobId](#)

L'ID de la tâche de numérisation qui a identifié de manière unique la demande adressée à AWS Backup.

Type : Chaîne

ScanMode

Spécifie le type de numérisation utilisé pour la tâche de numérisation.

Type : Chaîne

Valeurs valides : FULL_SCAN | INCREMENTAL_SCAN

ScannerRoleArn

Spécifie l'ARN du rôle IAM du scanner utilisé pour la tâche de numérisation.

Type : Chaîne

ScanResult

Contient le ScanResultsStatus pour le travail de numérisation et les retours THREATS_FOUND ou NO_THREATS_FOUND pour les travaux terminés.

Type : objet [ScanResultInfo](#)

State

État actuel d'une tâche de numérisation.

Type : Chaîne

Valeurs valides : CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

StatusMessage

Message détaillé expliquant le statut de la tâche de sauvegarde d'une ressource.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DisassociateBackupVaultMpaApprovalTeam

Service : AWS Backup

Supprime l'association entre une équipe d'approbation MPA et un coffre de sauvegarde, désactivant ainsi le flux de travail d'approbation MPA pour les opérations de restauration.

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/mpaApprovalTeam?delete HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "RequesterComment": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom du coffre de sauvegarde duquel dissocier l'équipe d'approbation de la MPA.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

RequesterComment

Un commentaire facultatif expliquant la raison pour laquelle l'équipe d'approbation MPA a été dissociée du coffre de sauvegarde.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DisassociateRecoveryPoint

Service : AWS Backup

Supprime le point de restauration de sauvegarde continue spécifié AWS Backup et confie le contrôle de cette sauvegarde continue au service source, tel qu'Amazon RDS. Le service source continuera à créer et à conserver des sauvegardes continues en utilisant le cycle de vie que vous avez spécifié dans votre plan de sauvegarde d'origine.

Ne prend pas en charge les points de récupération des sauvegardes d'instantanés.

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Nom unique d'un AWS Backup coffre-fort.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

[recoveryPointArn](#)

Un Amazon Resource Name (ARN) qui identifie de manière unique un point AWS Backup de récupération.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DisassociateRecoveryPointFromParent

Service : AWS Backup

Cette action sur un point de récupération enfant (imbriqué) spécifique supprime la relation entre le point de récupération spécifié et son point de récupération parent (composite).

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/parentAssociation HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom d'un conteneur logique dans lequel le point de récupération enfant (imbriqué) est stocké. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

recoveryPointArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique le point de récupération enfant (imbriqué) ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```


Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ExportBackupPlanTemplate

Service : AWS Backup

Renvoie le plan de sauvegarde spécifié par l'ID du plan en tant que modèle de sauvegarde.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupPlanId](#)

Identifie de façon unique un plan de secours.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanTemplateJson": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanTemplateJson](#)

Le corps d'un modèle de plan de sauvegarde au format JSON.

 Note

Il s'agit d'un document JSON signé qui ne peut pas être modifié avant d'être transmis à `GetBackupPlanFromJSON`.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupPlan

Service : AWS Backup

Renvoie les informations BackupPlan pour l'BackupPlanId spécifié. Les informations constituent le corps d'un plan de sauvegarde au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId?  
MaxScheduledRunsPreview=MaxScheduledRunsPreview&versionId=VersionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

MaxScheduledRunsPreview

Nombre de futures sauvegardes planifiées à prévisualiser. Lorsque ce paramètre est défini sur 0 (par défaut), aucun aperçu des courses planifiées n'est inclus dans la réponse. La plage valide est comprise entre 0 et 10.

Plage valide : Valeur minimum de 0. Valeur maximum de 10.

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. La version IDs ne peut pas être modifiée.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json  
  
{
```

```

    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlan": {
      "AdvancedBackupSettings": [
        {
          "BackupOptions": {
            "string" : "string"
          },
          "ResourceType": "string"
        }
      ],
      "BackupPlanName": "string",
      "Rules": [
        {
          "CompletionWindowMinutes": number,
          "CopyActions": [
            {
              "DestinationBackupVaultArn": "string",
              "Lifecycle": {
                "DeleteAfterDays": number,
                "DeleteAfterEvent": "string",
                "MoveToColdStorageAfterDays": number,
                "OptInToArchiveForSupportedResources": boolean
              }
            }
          ],
          "EnableContinuousBackup": boolean,
          "IndexActions": [
            {
              "ResourceTypes": [ "string" ]
            }
          ],
          "Lifecycle": {
            "DeleteAfterDays": number,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ]
    }
  ],

```

```

    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],
    "ScannerRoleArn": "string"
  }
]
},
"BackupPlanArn": "string",
"BackupPlanId": "string",
"CreationDate": number,
"CreatorRequestId": "string",
"DeletionDate": number,
"LastExecutionDate": number,
"ScheduledRunsPreview": [
  {
    "ExecutionTime": number,
    "RuleExecutionType": "string",
    "RuleId": "string"
  }
],
"VersionId": "string"
}

```


Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AdvancedBackupSettings](#)

Contient une liste d'`BackupOptions` pour chaque type de ressource. La liste est renseignée uniquement si l'option avancée est définie pour le plan de sauvegarde.

Type : tableau d'objets [AdvancedBackupSetting](#)

[BackupPlan](#)

Spécifie le corps d'un plan de sauvegarde. Comprend un `BackupPlanName` et un ou plusieurs ensembles de `Rules`.

Type : objet [BackupPlan](#)

[BackupPlanArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : Chaîne

[BackupPlanId](#)

Identifie de façon unique un plan de secours.

Type : Chaîne

[CreationDate](#)

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[CreatorRequestId](#)

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois.

Type : Chaîne

DeletionDate

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

LastExecutionDate

La dernière fois que ce plan de sauvegarde a été exécuté. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ScheduledRunsPreview

Liste des prochaines exécutions de sauvegarde planifiées. Inclus uniquement lorsque `MaxScheduledRunsPreview` le paramètre est supérieur à 0. Contient jusqu'à 10 futures exécutions de sauvegarde avec leurs heures planifiées, leurs types d'exécution et la règle associée IDs.

Type : tableau d'objets [ScheduledPlanExecutionMember](#)

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. La version IDs ne peut pas être modifiée.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupPlanFromJSON

Service : AWS Backup

Renvoie un document JSON valide spécifiant un plan de sauvegarde ou une erreur.

Syntaxe de la demande

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
  "BackupPlanTemplateJson": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupPlanTemplateJson](#)

Document de plan de sauvegarde fourni par le client au format JSON.

Type : Chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ]
  }
}
```

```

    }
  ],
  "BackupPlanName": "string",
  "Rules": [
    {
      "CompletionWindowMinutes": number,
      "CopyActions": [
        {
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
            "DeleteAfterDays": number,
            "DeleteAfterEvent": "string",
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
          }
        }
      ],
      "EnableContinuousBackup": boolean,
      "IndexActions": [
        {
          "ResourceTypes": [ "string" ]
        }
      ],
      "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      },
      "RecoveryPointTags": {
        "string" : "string"
      },
      "RuleId": "string",
      "RuleName": "string",
      "ScanActions": [
        {
          "MalwareScanner": "string",
          "ScanMode": "string"
        }
      ],
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowMinutes": number,
      "TargetBackupVaultName": "string",

```

```

        "TargetLogicallyAirGappedBackupVaultArn": "string"
    },
    ],
    "ScanSettings": [
        {
            "MalwareScanner": "string",
            "ResourceTypes": [ "string " ],
            "ScannerRoleArn": "string"
        }
    ]
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlan](#)

Spécifie le corps d'un plan de sauvegarde. Comprend un BackupPlanName et un ou plusieurs ensembles de Rules.

Type : objet [BackupPlan](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupPlanFromTemplate

Service : AWS Backup

Renvoie le modèle spécifié par son `templateId` en tant que plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[templateId](#)

Identifie de manière unique un modèle de plan de sauvegarde enregistré.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanDocument": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string" : "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
```

```

    {
      "DestinationBackupVaultArn": "string",
      "Lifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
      }
    },
    "EnableContinuousBackup": boolean,
    "IndexActions": [
      {
        "ResourceTypes": [ "string" ]
      }
    ],
    "Lifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
      "string" : "string"
    },
    "RuleId": "string",
    "RuleName": "string",
    "ScanActions": [
      {
        "MalwareScanner": "string",
        "ScanMode": "string"
      }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
  }
],
"ScanSettings": [
  {
    "MalwareScanner": "string",
    "ResourceTypes": [ "string" ],

```

```
        "ScannerRoleArn": "string"  
      }  
    ]  
  }  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanDocument](#)

Renvoie le corps d'un plan de sauvegarde en fonction du modèle cible, y compris le nom, les règles et le coffre-fort de sauvegarde du plan.

Type : objet [BackupPlan](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupSelection

Service : AWS Backup

Renvoie les métadonnées de sélection et un document au format JSON qui spécifie une liste de ressources associées à un plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupPlanId](#)

Identifie de façon unique un plan de secours.

Obligatoire : oui

[selectionId](#)

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanId": "string",
  "BackupSelection": {
    "Conditions": {
      "StringEquals": [
        {
          "ConditionKey": "string",
```

```

        "ConditionValue": "string"
    },
    ],
    "StringLike": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ],
    "StringNotEquals": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ],
    "StringNotLike": [
        {
            "ConditionKey": "string",
            "ConditionValue": "string"
        }
    ]
},
"IamRoleArn": "string",
"ListOfTags": [
    {
        "ConditionKey": "string",
        "ConditionType": "string",
        "ConditionValue": "string"
    }
],
"NotResources": [ "string" ],
"Resources": [ "string" ],
"SelectionName": "string"
},
"CreationDate": number,
"CreatorRequestId": "string",
"SelectionId": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanId](#)

Identifie de façon unique un plan de secours.

Type : String

[BackupSelection](#)

Spécifie le corps d'une demande pour attribuer un ensemble de ressources à un plan de secours.

Type : objet [BackupSelection](#)

[CreationDate](#)

Date et heure de création d'une sélection de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[CreatorRequestId](#)

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois.

Type : String

[SelectionId](#)

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)

- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupVaultAccessPolicy

Service : AWS Backup

Renvoie le document de stratégie d'accès associé au coffre-fort de sauvegarde nommé.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "Policy": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

[Policy](#)

Document de stratégie d'accès au coffre-fort de sauvegarde au format JSON.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBackupVaultNotifications

Service : AWS Backup

Renvoie des notifications d'événement pour le coffre-fort de sauvegarde spécifié.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "BackupVaultEvents": [ "string" ],
  "BackupVaultName": "string",
  "SNSTopicArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

[BackupVaultEvents](#)

Tableau d'événements qui indiquent le statut des tâches de sauvegarde des ressources dans le coffre-fort de sauvegarde.

Type : tableau de chaînes

Valeurs valides : `BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `BACKUP_JOB_SUCCESSFUL` | `BACKUP_JOB_FAILED` | `BACKUP_JOB_EXPIRED` | `RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED` | `RESTORE_JOB_SUCCESSFUL` | `RESTORE_JOB_FAILED` | `COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED` | `RECOVERY_POINT_MODIFIED` | `BACKUP_PLAN_CREATED` | `BACKUP_PLAN_MODIFIED` | `S3_BACKUP_OBJECT_FAILED` | `S3_RESTORE_OBJECT_FAILED` | `CONTINUOUS_BACKUP_INTERRUPTED` | `RECOVERY_POINT_INDEX_COMPLETED` | `RECOVERY_POINT_INDEX_DELETED` | `RECOVERY_POINT_INDEXING_FAILED`

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\ ]{2,50}$`

[SNSTopicArn](#)

ARN qui identifie de façon unique une rubrique Amazon Simple Notification Service (Amazon SNS) ; par exemple, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetLegalHold

Service : AWS Backup

Cette action renvoie les détails d'une conservation légale spécifiée. Les détails constituent le corps d'une conservation légale au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

legalHoldId

L'identifiant de la retenue légale.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CancelDescription": "string",
  "CancellationDate": number,
  "CreationDate": number,
  "Description": "string",
  "LegalHoldArn": "string",
  "LegalHoldId": "string",
  "RecoveryPointSelection": {
    "DateRange": {
      "FromDate": number,
      "ToDate": number
    },
    "ResourceIdentifiers": [ "string" ],
  },
}
```

```
    "VaultNames": [ "string" ]  
  },  
  "RetainRecordUntil": number,  
  "Status": "string",  
  "Title": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CancelDescription](#)

La raison de la levée de la suspension légale.

Type : String

[CancellationDate](#)

Heure à laquelle le blocage légal a été annulé.

Type : Timestamp

[CreationDate](#)

Heure à laquelle la mise en attente légale a été créée.

Type : Timestamp

[Description](#)

Description de la détention légale.

Type : String

[LegalHoldArn](#)

L'ARN du framework pour la conservation légale spécifiée. Le format de l'ARN dépend du type de ressource.

Type : String

[LegalHoldId](#)

L'identifiant de la retenue légale.

Type : String

[RecoveryPointSelection](#)

Les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet [RecoveryPointSelection](#)

[RetainRecordUntil](#)

Date et heure jusqu'à laquelle le dossier de conservation légal est conservé.

Type : Timestamp

[Status](#)

Le statut de la mise en attente légale.

Type : String

Valeurs valides : CREATING | ACTIVE | CANCELING | CANCELED

[Title](#)

Titre de la retenue légale.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetRecoveryPointIndexDetails

Service : AWS Backup

Cette opération renvoie les métadonnées et les détails spécifiques à l'index de sauvegarde associé au point de restauration spécifié.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Les caractères acceptés incluent les lettres minuscules, les chiffres et les traits d'union.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple,

`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```



```
{
  "BackupVaultArn": "string",
  "IndexCompletionDate": number,
  "IndexCreationDate": number,
  "IndexDeletionDate": number,
  "IndexStatus": "string",
  "IndexStatusMessage": "string",
  "RecoveryPointArn": "string",
  "SourceResourceArn": "string",
  "TotalItemsIndexed": number
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Un ARN qui identifie de manière unique le coffre de sauvegarde dans lequel l'index du point de restauration est stocké.

Par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

IndexCompletionDate

Date et heure de fin de création d'un index de sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IndexCreationDate

Date et heure de création d'un index de sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[IndexDeletionDate](#)

Date et heure auxquelles un index de sauvegarde a été supprimé, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[IndexStatus](#)

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : PENDING | ACTIVE | FAILED DELETING

Un point de récupération dont l'index a le statut de ACTIVE peut être inclus dans une recherche.

Type : String

Valeurs valides : PENDING | ACTIVE | FAILED | DELETING

[IndexStatusMessage](#)

Message détaillé expliquant l'état d'un index de sauvegarde associé au point de restauration.

Type : String

[RecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : String

[SourceResourceArn](#)

Chaîne contenant le nom de la ressource Amazon (ARN) qui identifie de manière unique la ressource source.

Type : String

[TotalItemsIndexed](#)

Nombre d'éléments dans l'index de sauvegarde associé au point de restauration.

Type : long

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetRecoveryPointRestoreMetadata

Service : AWS Backup

Renvoie un ensemble de paires clé-valeur de métadonnées qui ont été utilisées pour créer la sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

Modèle : `^[0-9]{12}$`

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "RecoveryPointArn": "string",
  "ResourceType": "string",
  "RestoreMetadata": {
    "string" : "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

[RecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : String

[ResourceType](#)

Type de ressource du point de récupération.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

RestoreMetadata

Ensemble de paires clé-valeur de métadonnées décrivant la configuration d'origine de la ressource sauvegardée. Ces valeurs varient en fonction du service restauré.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetRestoreJobMetadata

Service : AWS Backup

Cette demande renvoie les métadonnées de la tâche de restauration spécifiée.

Syntaxe de la demande

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[restoreJobId](#)

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "Metadata": {
    "string" : "string"
  },
  "RestoreJobId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Metadata

Cela contient les métadonnées de la tâche de sauvegarde spécifiée.

Type : mappage chaîne/chaîne

RestoreJobId

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetRestoreTestingInferredMetadata

Service : AWS Backup

Cette demande renvoie l'ensemble minimal de métadonnées requis pour démarrer une tâche de restauration avec des paramètres par défaut sécurisés. BackupVaultName et RecoveryPointArn sont des paramètres obligatoires. BackupVaultAccountId est un paramètre facultatif.

Syntaxe de la demande

```
GET /restore-testing/inferred-metadata?  
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=RecoveryPointArn  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[BackupVaultAccountId](#)

ID de compte du coffre-fort de sauvegarde spécifié.

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés. Ces noms sont composés de lettres, de chiffres et de traits d'union.

Obligatoire : oui

[RecoveryPointArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "InferredMetadata": {
    "string" : "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[InferredMetadata](#)

Il s'agit d'une carte de chaînes des métadonnées déduites de la demande.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

GetRestoreTestingPlan

Service : AWS Backup

Renvoie les informations RestoreTestingPlan pour l'RestoreTestingPlanName spécifié. Les informations constituent le corps d'un plan de test de la restauration au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreTestingPlan": {
    "CreationTime": number,
    "CreatorRequestId": "string",
    "LastExecutionTime": number,
    "LastUpdateTime": number,
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    }
  }
}
```



```
    },  
    "RestoreTestingPlanArn": "string",  
    "RestoreTestingPlanName": "string",  
    "ScheduleExpression": "string",  
    "ScheduleExpressionTimezone": "string",  
    "StartWindowHours": number  
  }  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[RestoreTestingPlan](#)

Spécifie le corps d'un plan de test de la restauration. Inclut `RestoreTestingPlanName`.

Type : objet [RestoreTestingPlanForGet](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetRestoreTestingSelection

Service : AWS Backup

Renvoie RestoreTestingSelection, qui affiche les ressources et les éléments du plan de test de restauration.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration.

Obligatoire : oui

RestoreTestingSelectionName

Nom unique obligatoire de la sélection de tests de la restauration.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreTestingSelection": {
    "CreationTime": number,
    "CreatorRequestId": "string",
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
```

```

    "StringEquals": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "StringNotEquals": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  "ProtectedResourceType": "string",
  "RestoreMetadataOverrides": {
    "string" : "string"
  },
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string",
  "ValidationWindowHours": number
}
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

RestoreTestingSelection

Nom unique de la sélection de tests de la restauration.

Type : objet RestoreTestingSelectionForGet

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetSupportedResourceTypes

Service : AWS Backup

Renvoie les types de AWS ressources pris en charge par AWS Backup.

Syntaxe de la demande

```
GET /supported-resource-types HTTP/1.1
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ResourceTypes": [ "string" ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ResourceTypes](#)

Contient une chaîne avec les types de AWS ressources pris en charge :

- Aurora pour Amazon Aurora
- CloudFormation pour AWS CloudFormation
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB
- EBS pour Amazon Elastic Block Store

- EC2 pour Amazon Elastic Compute Cloud
- EFS pour Amazon Elastic File System
- FSx pour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- Redshift pour Amazon Redshift
- S3 pour Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- Storage Gateway pour AWS Storage Gateway
- Timestream pour Amazon Timestream
- Virtual Machine pour les machines VMware virtuelles

Type : tableau de chaînes

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetTieringConfiguration

Service : AWS Backup

Renvoie les informations TieringConfiguration pour l'`TieringConfigurationName` spécifié. Les détails constituent le corps d'une configuration de hiérarchisation au format JSON, en plus des métadonnées de configuration.

Syntaxe de la demande

```
GET /tiering-configurations/tieringConfigurationName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

tieringConfigurationName

Nom unique d'une configuration de hiérarchisation.

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "CreationTime": number,
    "CreatorRequestId": "string",
    "LastUpdatedTime": number,
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
```

```
        "TieringDownSettingsInDays": number
      }
    ],
    "TieringConfigurationArn": "string",
    "TieringConfigurationName": "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[TieringConfiguration](#)

Spécifie le corps d'une configuration de hiérarchisation. Inclut `TieringConfigurationName`.

Type : objet [TieringConfiguration](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupJobs

Service : AWS Backup

Renvoie la liste des tâches de sauvegarde existantes pour un compte authentifié au cours des 30 derniers jours. Envisagez d'utiliser ces [outils de surveillance](#) pendant une période plus longue.

Syntaxe de la demande

```
GET /backup-jobs/?  
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByAccountId](#)

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de sauvegarde associées à l'ID de compte spécifié.

S'il est utilisé à partir d'un compte de AWS Organizations gestion, le transfert * renvoie tous les emplois de l'organisation.

Modèle : `^[0-9]{12}$`

[ByBackupVaultName](#)

Renvoie uniquement les tâches de sauvegarde qui seront stockées dans le coffre-fort de sauvegarde spécifié. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

[ByCompleteAfter](#)

Renvoie uniquement les tâches de sauvegarde terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCompleteBefore](#)

Renvoie uniquement les tâches de sauvegarde terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCreatedAfter](#)

Renvoie uniquement les tâches de sauvegarde créées après la date spécifiée.

[ByCreatedBefore](#)

Renvoie uniquement les tâches de sauvegarde créées avant la date spécifiée.

[ByMessageCategory](#)

Il s'agit d'un paramètre facultatif qui peut être utilisé pour filtrer les tâches MessageCategory dont la valeur correspond à la valeur que vous avez saisie.

Les exemples de chaînes peuvent inclure AccessDenied, SUCCESS, AGGREGATE_ALL et InvalidParameters.

Consultez [Surveillance](#)

Le caractère générique () renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

[ByParentJobId](#)

Il s'agit d'un filtre permettant de répertorier les tâches enfants (imbriquées) en fonction de l'ID de tâche parent.

[ByResourceArn](#)

Renvoie uniquement les tâches de sauvegarde qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

[ByResourceType](#)

Renvoie uniquement les tâches de sauvegarde pour les ressources spécifiées :

- Aurora pour Amazon Aurora
- CloudFormation pour AWS CloudFormation
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB
- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud

- EFS pour Amazon Elastic File System
- FSx pour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- Redshift pour Amazon Redshift
- S3 pour Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- Storage Gateway pour AWS Storage Gateway
- Timestream pour Amazon Timestream
- Virtual Machine pour machines VMware virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ByState](#)

Renvoie uniquement les tâches de sauvegarde qui sont dans l'état spécifié.

`Completed with issues` est un statut présent uniquement dans la console AWS Backup . Pour l'API, ce statut fait référence aux tâches avec un état `COMPLETED` et `MessageCategory` avec une valeur différente de `SUCCESS` ; c'est-à-dire que le statut est terminé mais qu'il est accompagné d'un message de statut.

Pour obtenir le nombre de tâches pour `Completed with issues`, exécutez deux requêtes GET et soustrayez le deuxième plus petit nombre :

GET `/backup-jobs/?state=COMPLETED`

GET `/backup-jobs/?messageCategory=SUCCESS&state=COMPLETED`

Valeurs valides : `CREATED` | `PENDING` | `RUNNING` | `ABORTING` | `ABORTED` | `COMPLETED` | `FAILED` | `EXPIRED` | `PARTIAL`

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobs": [
    {
      "AccountId": "string",
      "BackupJobId": "string",
      "BackupOptions": {
        "string" : "string"
      },
      "BackupSizeInBytes": number,
      "BackupType": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "BytesTransferred": number,
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanName": "string",
        "BackupPlanVersion": "string",
        "BackupRuleCron": "string",
        "BackupRuleId": "string",
        "BackupRuleName": "string",
        "BackupRuleTimezone": "string"
      },
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "ExpectedCompletionDate": number,
      "IamRoleArn": "string",
```

```

    "InitiationDate": number,
    "IsEncrypted": boolean,
    "IsParent": boolean,
    "MessageCategory": "string",
    "ParentJobId": "string",
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointLifecycle": {
        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "StartBy": number,
    "State": "string",
    "StatusMessage": "string",
    "VaultLockState": "string",
    "VaultType": "string"
  },
  ],
  "NextToken": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupJobs](#)

Tableau de structures contenant des métadonnées relatives à vos tâches de sauvegarde renvoyées au format JSON.

Type : tableau d'objets [BackupJob](#)

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)

- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupJobSummaries

Service : AWS Backup

Il s'agit d'une demande pour un résumé des tâches de sauvegarde créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/backup-job-summaries?
AccountID=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[AccountId](#)

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

AGGREGATE_ALL agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

[AggregationPeriod](#)

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.

- `FOURTEEN_DAYS`- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : `ONE_DAY` | `SEVEN_DAYS` | `FOURTEEN_DAYS`

MaxResults

Le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

MessageCategory

Ce paramètre renvoie le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes acceptées incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir [Surveillance](#) pour une liste des `MessageCategory` chaînes acceptées.

La valeur `ANY` renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande `GetSupportedResourceTypes` pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur `ANY` renvoie le nombre de tous les types de ressources.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

AGGREGATE_ALL agrège le nombre de tâches pour tous les états et renvoie la somme.

Completed with issues est un statut présent uniquement dans la console AWS Backup . Pour l'API, ce statut fait référence aux tâches avec un état COMPLETED et MessageCategory avec une valeur différente de SUCCESS ; c'est-à-dire que le statut est terminé mais qu'il est accompagné d'un message de statut. Pour obtenir le nombre de tâches pour Completed with issues, exécutez deux requêtes GET et soustrayez le deuxième plus petit nombre :

OBTENIR /audit/ ? backup-job-summaries AggregationPeriod=Quatorteen_days&state=Terminé

OBTENIR /audit/ ? backup-job-summaries AggregationPeriod=QUATORTE_DAYS&=Success&State=Terminé MessageCategory

Valeurs valides : CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "BackupJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MessageCategory": "string",
      "Region": "string",
```

```
    "ResourceType": "string",
    "StartTime": number,
    "State": "string"
  },
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AggregationPeriod](#)

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : String

[BackupJobSummaries](#)

Les informations récapitulatives.

Type : tableau d'objets [BackupJobSummary](#)

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupPlans

Service : AWS Backup

Répertorie les plans de sauvegarde actifs pour le compte.

Syntaxe de la demande

```
GET /backup/plans/?  
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[IncludeDeleted](#)

Une valeur booléenne dont la valeur par défaut est FALSE, qui renvoie les plans de sauvegarde supprimés lorsqu'elle est définie sur TRUE.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json  
  
{  
  "BackupPlansList": [  
    {  
      "AdvancedBackupSettings": [  

```



```

    {
      "BackupOptions": {
        "string" : "string"
      },
      "ResourceType": "string"
    }
  ],
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "BackupPlanName": "string",
  "CreationDate": number,
  "CreatorRequestId": "string",
  "DeletionDate": number,
  "LastExecutionDate": number,
  "VersionId": "string"
}
],
"NextToken": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlansList

Informations sur les plans de sauvegarde.

Type : tableau d'objets [BackupPlansListMember](#)

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupPlanTemplates

Service : AWS Backup

Répertorie les modèles de plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'articles à retourner.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupPlanTemplatesList": [
    {
      "BackupPlanTemplateId": "string",
      "BackupPlanTemplateName": "string"
    }
  ],
  "NextToken": "string"
}
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanTemplatesList](#)

Un tableau d'éléments de liste de modèles contenant des métadonnées relatives à vos modèles enregistrés.

Type : tableau d'objets [BackupPlanTemplatesListMember](#)

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`MissingParameterValueException`

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

ListBackupPlanVersions

Service : AWS Backup

Renvoie les métadonnées de version de vos plans de sauvegarde, notamment les noms des ressources Amazon (ARNs), le plan de sauvegarde IDs, les dates de création et de suppression, les noms des plans et la version IDs.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json
```



```

{
  "BackupPlanVersionsList": [
    {
      "AdvancedBackupSettings": [
        {
          "BackupOptions": {
            "string": "string"
          },
          "ResourceType": "string"
        }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "DeletionDate": number,
      "LastExecutionDate": number,
      "VersionId": "string"
    }
  ],
  "NextToken": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupPlanVersionsList](#)

Un tableau de versions répertorie les éléments contenant des métadonnées relatives à vos plans de sauvegarde.

Type : tableau d'objets [BackupPlansListMember](#)

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupSelections

Service : AWS Backup

Renvoie un tableau contenant les métadonnées des ressources associées au plan de sauvegarde cible.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "BackupSelectionsList": [
    {
      "BackupPlanId": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "SelectionId": "string",
      "SelectionName": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupSelectionsList](#)

Un tableau de sélection de sauvegardes répertorie les éléments contenant des métadonnées relatives à chaque ressource de la liste.

Type : tableau d'objets [BackupSelectionsListMember](#)

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListBackupVaults

Service : AWS Backup

Renvoie une liste des conteneurs de stockage de points de récupération ainsi que des informations les concernant.

Syntaxe de la demande

```
GET /backup-vaults/?  
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByShared](#)

Ce paramètre triera la liste des coffres-forts par coffres-forts partagés.

[ByVaultType](#)

Ce paramètre triera la liste des coffres-forts par type de coffre-fort.

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultList": [
    {
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CreationDate": number,
      "CreatorRequestId": "string",
      "EncryptionKeyArn": "string",
      "EncryptionKeyType": "string",
      "LockDate": number,
      "Locked": boolean,
      "MaxRetentionDays": number,
      "MinRetentionDays": number,
      "NumberOfRecoveryPoints": number,
      "VaultState": "string",
      "VaultType": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultList](#)

Un tableau des membres du coffre-fort de sauvegarde contenant les métadonnées du coffre-fort, notamment l'Amazon Resource Name (ARN), le nom d'affichage, la date de création, le nombre de points de récupération enregistrés et les informations de chiffrement si les ressources enregistrées dans le coffre-fort de sauvegarde sont chiffrées.

Type : tableau d'objets [BackupVaultListMember](#)

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`MissingParameterValueException`

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

`ResourceNotFoundException`

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListCopyJobs

Service : AWS Backup

Renvoie les métadonnées relatives à vos tâches de copie.

Syntaxe de la demande

```
GET /copy-jobs/?  
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&destinationVaultArn=ByDestinationVaultArn  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByAccountId](#)

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de copie associées à l'ID de compte spécifié.

Modèle : `^[0-9]{12}$`

[ByCompleteAfter](#)

Renvoie uniquement les tâches de copie terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCompleteBefore](#)

Renvoie uniquement les tâches de copie terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCreatedAfter](#)

Renvoie uniquement les tâches de copie créées après la date spécifiée.

[ByCreatedBefore](#)

Renvoie uniquement les tâches de copie créées avant la date spécifiée.

[ByDestinationVaultArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde source à partir duquel copier ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Il s'agit d'un paramètre facultatif qui peut être utilisé pour filtrer les tâches MessageCategory dont la valeur correspond à la valeur que vous avez saisie.

Les exemples de chaînes peuvent inclure AccessDenied, SUCCESS, AGGREGATE_ALL et INVALIDPARAMETERS.

Consultez [Surveillance](#) pour obtenir la liste des chaînes acceptées.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

ByParentJobId

Il s'agit d'un filtre permettant de répertorier les tâches enfants (imbriquées) en fonction de l'ID de tâche parent.

ByResourceArn

Renvoie uniquement les tâches de copie qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

ByResourceType

Renvoie uniquement les tâches de sauvegarde pour les ressources spécifiées :

- Aurora pour Amazon Aurora
- CloudFormationpour AWS CloudFormation
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB
- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud
- EFS pour Amazon Elastic File System
- FSxpour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- Redshift pour Amazon Redshift
- S3pour Amazon Simple Storage Service (Amazon S3)

- SAP HANA on Amazon EC2 pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- Storage Gateway pour AWS Storage Gateway
- Timestream pour Amazon Timestream
- Virtual Machine pour les machines VMware virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[BySourceRecoveryPointArn](#)

Les filtres copient les tâches en fonction de l'ARN du point de récupération source spécifié.

[ByState](#)

Renvoie uniquement les tâches de copie qui sont dans l'état spécifié.

Valeurs valides : CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer un MaxResults certain nombre d'articles, cela vous NextToken permet de renvoyer d'autres articles dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobs": [
    {
      "AccountId": "string",
```

```

    "BackupSizeInBytes": number,
    "ChildJobsInState": {
      "string" : number
    },
    "CompletionDate": number,
    "CompositeMemberIdentifier": "string",
    "CopyJobId": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "BackupPlanVersion": "string",
      "BackupRuleCron": "string",
      "BackupRuleId": "string",
      "BackupRuleName": "string",
      "BackupRuleTimezone": "string"
    },
    "CreatedByBackupJobId": "string",
    "CreationDate": number,
    "DestinationBackupVaultArn": "string",
    "DestinationEncryptionKeyArn": "string",
    "DestinationRecoveryPointArn": "string",
    "DestinationRecoveryPointLifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "DestinationVaultLockState": "string",
    "DestinationVaultType": "string",
    "IamRoleArn": "string",
    "IsParent": boolean,
    "MessageCategory": "string",
    "NumberOfChildJobs": number,
    "ParentJobId": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "SourceRecoveryPointArn": "string",
    "State": "string",
    "StatusMessage": "string"
  }
],

```

```
"NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CopyJobs](#)

Tableau de structures contenant des métadonnées relatives à vos tâches de copie renvoyées au format JSON.

Type : tableau d'objets [CopyJob](#)

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer un MaxResults certain nombre d'articles, cela vous NextToken permet de renvoyer d'autres articles dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListCopyJobSummaries

Service : AWS Backup

Cette demande obtient une liste des tâches de copie créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état RestourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/copy-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[AccountId](#)

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

AGGREGATE_ALL agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

[AggregationPeriod](#)

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Ce paramètre définit le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

MessageCategory

Ce paramètre renvoie le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes acceptées incluent AccessDenied, Success et InvalidParameters. Voir [Surveillance](#) pour une liste des MessageCategory chaînes acceptées.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer MaxResults ressources, NextToken vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande GetSupportedResourceTypes pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

AGGREGATE_ALL agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

AGGREGATE_ALL agrège le nombre de tâches pour tous les états et renvoie la somme.

Valeurs valides : CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "CopyJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MessageCategory": "string",
      "Region": "string",
      "ResourceType": "string",
      "StartTime": number,
      "State": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AggregationPeriod](#)

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : String

[CopyJobSummaries](#)

Ce retour affiche un résumé contenant la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Type : tableau d'objets [CopyJobSummary](#)

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer MaxResults ressources, NextToken vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListFrameworks

Service : AWS Backup

Renvoie une liste de tous les frameworks pour un Compte AWS et Région AWS.

Syntaxe de la demande

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "Frameworks": [
    {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "FrameworkArn": "string",
      "FrameworkDescription": "string",
      "FrameworkName": "string",
```

```
    "NumberOfControls": number
  },
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Frameworks](#)

Les frameworks avec les détails de chaque framework, y compris le nom du framework, le nom de ressource Amazon (ARN), la description, le nombre de contrôles, l'heure de création et l'état du déploiement.

Type : tableau d'objets [Framework](#)

[NextToken](#)

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListIndexedRecoveryPoints

Service : AWS Backup

Cette opération renvoie une liste de points de récupération associés à un index appartenant au compte spécifié.

Les paramètres facultatifs que vous pouvez inclure sont les suivants : MaxResults NextToken SourceResourceArns ; CreatedBefore ; CreatedAfter ; ; et ResourceType.

Syntaxe de la demande

```
GET /indexes/recovery-point/?
createdAfter=CreatedAfter&createdBefore=CreatedBefore&indexStatus=IndexStatus&maxResults=MaxRes
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[CreatedAfter](#)

Renvoie uniquement les points de récupération indexés créés après la date spécifiée.

[CreatedBefore](#)

Renvoie uniquement les points de récupération indexés créés avant la date spécifiée.

[IndexStatus](#)

Incluez ce paramètre pour filtrer la liste renvoyée en fonction des statuts indiqués.

Valeurs acceptées : PENDING | ACTIVE | FAILED | DELETING

Un point de récupération dont l'index a le statut de ACTIVE peut être inclus dans une recherche.

Valeurs valides : PENDING | ACTIVE | FAILED | DELETING

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant suivant une liste partielle des points de récupération renvoyés.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de points de récupération indexés, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[ResourceType](#)

Renvoie une liste de points de récupération indexés pour le ou les types de ressources spécifiés.

Les valeurs acceptées incluent :

- EBS pour Amazon Elastic Block Store
- S3 pour Amazon Simple Storage Service (Amazon S3)

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[SourceResourceArn](#)

Chaîne contenant le nom de la ressource Amazon (ARN) qui identifie de manière unique la ressource source.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "IndexedRecoveryPoints": [
    {
      "BackupCreationDate": number,
      "BackupVaultArn": "string",
      "IamRoleArn": "string",
      "IndexCreationDate": number,
      "IndexStatus": "string",
      "IndexStatusMessage": "string",
      "RecoveryPointArn": "string",
      "ResourceType": "string",
      "SourceResourceArn": "string"
    }
  ],
  "NextToken": "string"
}
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[IndexedRecoveryPoints](#)

Il s'agit d'une liste de points de récupération associés à un index appartenant au compte spécifié.

Type : tableau d'objets [IndexedRecoveryPoint](#)

[NextToken](#)

L'élément suivant suivant une liste partielle des points de récupération renvoyés.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de points de récupération indexés, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`ResourceNotFoundException`

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListLegalHolds

Service : AWS Backup

Cette action renvoie des métadonnées concernant les mises en suspens juridiques actives et antérieures.

Syntaxe de la demande

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "LegalHolds": [
    {
      "CancellationDate": number,
      "CreationDate": number,
      "Description": "string",
      "LegalHoldArn": "string",
```

```
    "LegalHoldId": "string",  
    "Status": "string",  
    "Title": "string"  
  },  
],  
"NextToken": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[LegalHolds](#)

Il s'agit d'un ensemble de mises en suspens juridiques retournées, actives et antérieures.

Type : tableau d'objets [LegalHold](#)

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListProtectedResources

Service : AWS Backup

Renvoie un tableau de ressources sauvegardées avec succès AWS Backup, y compris l'heure à laquelle la ressource a été enregistrée, un Amazon Resource Name (ARN) de la ressource et un type de ressource.

Syntaxe de la demande

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
      "LastBackupVaultArn": "string",
```

```
    "LastRecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string"
  }
]
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[Results](#)

Tableau de ressources sauvegardé avec succès en AWS Backup indiquant l'heure à laquelle la ressource a été enregistrée, le nom de ressource Amazon (ARN) de la ressource et un type de ressource.

Type : tableau d'objets [ProtectedResource](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListProtectedResourcesByBackupVault

Service : AWS Backup

Cette demande répertorie les ressources protégées correspondant à chaque coffre-fort de sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/resources/?  
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

La liste des ressources protégées par coffre-fort de sauvegarde dans le ou les coffres que vous spécifiez par identifiant de compte.

Modèle : `^[0-9]{12}$`

backupVaultName

La liste des ressources protégées par coffre-fort de sauvegarde dans le ou les coffres que vous spécifiez par nom.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "LastBackupTime": number,
      "LastBackupVaultArn": "string",
      "LastRecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Results

Il s'agit des résultats renvoyés pour la demande `ListProtectedResourcesByBackupVault`.

Type : tableau d'objets [ProtectedResource](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)

- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRecoveryPointsByBackupVault

Service : AWS Backup

Renvoie des informations détaillées sur les points de récupération stockés dans un coffre-fort de sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/?  
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAfter  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[BackupVaultAccountId](#)

Ce paramètre triera la liste des points de récupération par ID de compte.

Modèle : `^[0-9]{12}$`

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Note

Le nom du coffre-fort de sauvegarde peut ne pas être disponible lorsqu'un service pris en charge crée la sauvegarde.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

[ByBackupPlanId](#)

Renvoie uniquement les points de récupération correspondant à l'ID du plan de sauvegarde spécifié.

[ByCreatedAfter](#)

Renvoie uniquement les points de récupération créés après l'horodatage spécifié.

[ByCreatedBefore](#)

Renvoie uniquement les points de récupération créés après l'horodatage spécifié.

[ByParentRecoveryPointArn](#)

Cela renvoie uniquement les points de récupération qui correspondent au point de récupération parent (composite) spécifié (Amazon Resource Name (ARN)).

[ByResourceArn](#)

Renvoie uniquement les points de récupération qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

[ByResourceType](#)

Renvoie uniquement les points de récupération qui correspondent au(x) type(s) de ressources spécifié(s) :

- Aurora pour Amazon Aurora
- CloudFormationpour AWS CloudFormation
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB
- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud
- EFS pour Amazon Elastic File System
- FSxpour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- Redshift pour Amazon Redshift
- S3pour Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- Storage Gatewaypour AWS Storage Gateway
- Timestream pour Amazon Timestream

- VirtualMachinepour machines VMware virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CalculatedLifecycle": {
        "DeleteAt": number,
        "MoveToColdStorageAt": number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
```

```

    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanName": "string",
      "BackupPlanVersion": "string",
      "BackupRuleCron": "string",
      "BackupRuleId": "string",
      "BackupRuleName": "string",
      "BackupRuleTimezone": "string"
    },
    "CreationDate": number,
    "EncryptionKeyArn": "string",
    "EncryptionKeyType": "string",
    "IamRoleArn": "string",
    "IndexStatus": "string",
    "IndexStatusMessage": "string",
    "InitiationDate": number,
    "IsEncrypted": boolean,
    "IsParent": boolean,
    "LastRestoreTime": number,
    "Lifecycle": {
      "DeleteAfterDays": number,
      "DeleteAfterEvent": "string",
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
    },
    "ParentRecoveryPointArn": "string",
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceName": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "Status": "string",
    "StatusMessage": "string",
    "VaultType": "string"
  }
]
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[RecoveryPoints](#)

Ensemble d'objets contenant des informations détaillées sur les points de récupération enregistrés dans un coffre-fort de sauvegarde.

Type : tableau d'objets [RecoveryPointByBackupVault](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`MissingParameterValueException`

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

`ResourceNotFoundException`

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRecoveryPointsByLegalHold

Service : AWS Backup

Cette action renvoie le point de récupération ARNs (Amazon Resource Names) de la retenue légale spécifiée.

Syntaxe de la demande

```
GET /legal-holds/LegalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[legalHoldId](#)

L'identifiant de la retenue légale.

Obligatoire : oui

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json  
  
{
```

```
"NextToken": "string",
"RecoveryPoints": [
  {
    "BackupVaultName": "string",
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceType": "string"
  }
]
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées.

Type : String

[RecoveryPoints](#)

Les points de récupération.

Type : tableau d'objets [RecoveryPointMember](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRecoveryPointsByResource

Service : AWS Backup

Les informations sur les points de récupération du type spécifié par le nom de ressource Amazon (ARN) d'une ressource.

Note

Pour Amazon EFS et Amazon EC2, cette action répertorie uniquement les points de récupération créés par AWS Backup.

Syntaxe de la demande

```
GET /resources/resourceArn/recovery-points/?  
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ManagedByAWSBackupOnly

Cet attribut filtre les points de récupération en fonction de leur propriétaire.

Si ce paramètre est défini sur `TRUE`, la réponse contiendra les points de récupération associés aux ressources sélectionnées gérées par AWS Backup.

Si ce paramètre est défini sur `FALSE`, la réponse contiendra tous les points de récupération associés à la ressource sélectionnée.

Type : Boolean

MaxResults

Le nombre maximum d'éléments à renvoyer.

Note

Amazon RDS nécessite une valeur d'au moins 20.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[resourceArn](#)

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RecoveryPoints": [
    {
      "AggregatedScanResult": {
        "FailedScan": boolean,
        "Findings": [ "string" ],
        "LastComputed": number
      },
      "BackupSizeBytes": number,
      "BackupVaultName": "string",
      "CreationDate": number,
      "EncryptionKeyArn": "string",
      "EncryptionKeyType": "string",
      "IndexStatus": "string",
      "IndexStatusMessage": "string",
      "IsParent": boolean,
      "ParentRecoveryPointArn": "string",
      "RecoveryPointArn": "string",
      "ResourceName": "string",
```

```
    "Status": "string",  
    "StatusMessage": "string",  
    "VaultType": "string"  
  }  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[RecoveryPoints](#)

Tableau d'objets contenant des informations détaillées sur les points de récupération du type de ressource spécifié.

Note

Seuls les points de EC2 récupération Amazon EFS et Amazon sont renvoyés `BackupVaultName`.

Type : tableau d'objets [RecoveryPointByResource](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListReportJobs

Service : AWS Backup

Renvoie des informations sur vos tâches de rapport.

Syntaxe de la demande

```
GET /audit/report-jobs?  
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByCreationAfter](#)

Renvoie uniquement les tâches de rapport créées après la date et l'heure spécifiées au format Unix et au format UTC (temps universel coordonné). Par exemple, la valeur 1516925490 représente le vendredi 26 janvier 2018 à 00 h 11 m 30 s.

[ByCreationBefore](#)

Renvoie uniquement les tâches de rapport créées avant la date et l'heure spécifiées au format Unix et au format UTC (temps universel coordonné). Par exemple, la valeur 1516925490 représente le vendredi 26 janvier 2018 à 00 h 11 m 30 s.

[ByReportPlanName](#)

Renvoie uniquement les tâches de rapport portant le nom du plan de rapport spécifié.

Contraintes de longueur : longueur minimale de 1 caractère. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

[ByStatus](#)

Renvoie uniquement les tâches de rapport qui sont dans le statut spécifié. Les statuts sont les suivants :

CREATED | RUNNING | COMPLETED | FAILED | COMPLETED_WITH_ISSUES

Veuillez noter que seules les tâches de numérisation se terminent avec un état terminé présentant des problèmes. Pour les tâches de sauvegarde, il s'agit d'une interprétation par console d'une tâche qui se termine à l'état terminé et qui comporte un message d'état.

MaxResults

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ReportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
        "S3BucketName": "string",
        "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : Chaîne

[ReportJobs](#)

Détails de vos tâches de rapports au format JSON.

Type : tableau d'objets [ReportJob](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListReportPlans

Service : AWS Backup

Renvoie une liste de vos plans de rapport. Pour obtenir des informations détaillées sur un plan de rapport unique, utilisez DescribeReportPlan.

Syntaxe de la demande

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ReportPlans": [
    {
      "CreationTime": number,
      "DeploymentStatus": "string",
```

```

    "LastAttemptedExecutionTime": number,
    "LastSuccessfulExecutionTime": number,
    "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
    },
    "ReportPlanArn": "string",
    "ReportPlanDescription": "string",
    "ReportPlanName": "string",
    "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
    }
  }
]
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : String

[ReportPlans](#)

Le rapport planifie avec des informations détaillées pour chaque plan. Ces informations incluent l'Amazon Resource Name (ARN), le nom du plan de rapport, la description, les paramètres, le canal de livraison, le statut du déploiement, l'heure de création et les dernières tentatives d'exécution du plan de rapport ainsi que celles ayant réussi.

Type : tableau d'objets [ReportPlan](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

ListRestoreAccessBackupVaults

Service : AWS Backup

Renvoie une liste des coffres-forts de sauvegarde d'accès à la restauration associés à un coffre-fort de sauvegarde spécifié.

Syntaxe de la demande

```
GET /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/?
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom du coffre de sauvegarde pour lequel répertorier les coffres-forts de sauvegarde associés à l'accès à la restauration.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer dans la réponse.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

Le jeton de pagination issu d'une demande précédente pour récupérer le prochain ensemble de résultats.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "NextToken": "string",
  "RestoreAccessBackupVaults": [
    {
      "ApprovalDate": number,
      "CreationDate": number,
      "LatestRevokeRequest": {
        "ExpiryDate": number,
        "InitiationDate": number,
        "MpaSessionArn": "string",
        "Status": "string",
        "StatusMessage": "string"
      },
      "RestoreAccessBackupVaultArn": "string",
      "VaultState": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

Le jeton de pagination à utiliser dans une demande ultérieure pour récupérer le prochain ensemble de résultats.

Type : String

[RestoreAccessBackupVaults](#)

Liste des coffres-forts de sauvegarde pour accès à la restauration associés au coffre-fort de sauvegarde spécifié.

Type : tableau d'objets [RestoreAccessBackupVaultListMember](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRestoreJobs

Service : AWS Backup

Renvoie la liste des tâches AWS Backup initiées pour restaurer une ressource enregistrée, y compris des détails sur le processus de restauration.

Syntaxe de la demande

```
GET /restore-jobs/?  
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfter=ByCreatedAfter&createdBefore=ByCreatedBefore&parentJobId=ByParentJobId  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByAccountId](#)

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de restauration associées à l'ID de compte spécifié.

Modèle : `^[0-9]{12}$`

[ByCompleteAfter](#)

Renvoie uniquement les tâches de copie terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCompleteBefore](#)

Renvoie uniquement les tâches de copie terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByCreatedAfter](#)

Renvoie uniquement les tâches de restauration créées après la date spécifiée.

[ByCreatedBefore](#)

Renvoie uniquement les tâches de restauration créées avant la date spécifiée.

[ByParentJobId](#)

Il s'agit d'un filtre permettant de répertorier les tâches de restauration enfants (imbriquées) en fonction de l'identifiant de la tâche de restauration parent.

[ByResourceType](#)

Incluez ce paramètre pour renvoyer uniquement les tâches de restauration pour les ressources spécifiées :

- Aurora pour Amazon Aurora
- CloudFormation pour AWS CloudFormation
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB
- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud
- EFS pour Amazon Elastic File System
- FSx pour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- Redshift pour Amazon Redshift
- S3 pour Amazon Simple Storage Service (Amazon S3)
- SAP HANA on Amazon EC2 pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- Storage Gateway pour AWS Storage Gateway
- Timestream pour Amazon Timestream
- VirtualMachine pour les machines VMware virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ByRestoreTestingPlanArn](#)

Cela renvoie uniquement les tâches de test de la restauration qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

[ByStatus](#)

Renvoie uniquement les tâches de restauration associées au statut de tâche spécifié.

Valeurs valides : PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "RecoveryPointCreationDate": number,
      "ResourceType": "string",
      "RestoreJobId": "string",
      "SourceResourceArn": "string",
      "Status": "string",
```

```
    "StatusMessage": "string",  
    "ValidationStatus": "string",  
    "ValidationStatusMessage": "string"  
  }  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[RestoreJobs](#)

Tableau d'objets contenant des informations détaillées sur les tâches de restauration des ressources enregistrées.

Type : tableau d'objets [RestoreJobsListMember](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRestoreJobsByProtectedResource

Service : AWS Backup

Cela renvoie les tâches de restauration contenant la ressource protégée spécifiée.

Vous devez inclure `ResourceArn`. Vous pouvez éventuellement inclure `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` et `ByRecoveryPointCreationDateBefore`.

Syntaxe de la demande

```
GET /resources/resourceArn/restore-jobs/?  
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreationDateAfter  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByRecoveryPointCreationDateAfter](#)

Renvoie uniquement les tâches de restauration des points de récupération créées après la date spécifiée.

[ByRecoveryPointCreationDateBefore](#)

Renvoie uniquement les tâches de restauration des points de récupération créées avant la date spécifiée.

[ByStatus](#)

Renvoie uniquement les tâches de restauration associées au statut de tâche spécifié.

Valeurs valides : PENDING | RUNNING | COMPLETED | ABORTED | FAILED

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[resourceArn](#)

Renvoie uniquement les tâches de restauration qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreJobs": [
    {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "BackupVaultArn": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "RestoreTestingPlanArn": "string"
      },
      "CreatedResourceArn": "string",
      "CreationDate": number,
      "DeletionStatus": "string",
      "DeletionStatusMessage": "string",
      "ExpectedCompletionTimeMinutes": number,
      "IamRoleArn": "string",
      "IsParent": boolean,
      "ParentJobId": "string",
      "PercentDone": "string",
      "RecoveryPointArn": "string",
      "RecoveryPointCreationDate": number,
      "ResourceType": "string",
      "RestoreJobId": "string",
      "SourceResourceArn": "string",
      "Status": "string",
      "StatusMessage": "string",
```

```
    "ValidationStatus": "string",  
    "ValidationStatusMessage": "string"  
  }  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[RestoreJobs](#)

Tableau d'objets contenant des informations détaillées sur les tâches de restauration des ressources enregistrées.

Type : tableau d'objets [RestoreJobsListMember](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRestoreJobSummaries

Service : AWS Backup

Cette demande obtient un résumé des tâches de restauration créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State,, ResourceType AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état RestourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/restore-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccountId

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

AGGREGATE_ALL agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Ce paramètre définit le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande `GetSupportedResourceTypes` pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

AGGREGATE_ALL agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

AGGREGATE_ALL agrège le nombre de tâches pour tous les états et renvoie la somme.

Valeurs valides : CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED
| AGGREGATE_ALL | ANY

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "NextToken": "string",
  "RestoreJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "Region": "string",
      "ResourceType": "string",
      "StartTime": number,
      "State": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AggregationPeriod](#)

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : String

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[RestoreJobSummaries](#)

Ce retour contient un résumé qui contient la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Type : tableau d'objets [RestoreJobSummary](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)

- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRestoreTestingPlans

Service : AWS Backup

Renvoie une liste de plans de test de la restauration.

Syntaxe de la demande

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "RestoreTestingPlans": [
    {
      "CreationTime": number,
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RestoreTestingPlanArn": "string",
```

```
"RestoreTestingPlanName": "string",  
"ScheduleExpression": "string",  
"ScheduleExpressionTimezone": "string",  
"StartWindowHours": number  
}  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[RestoreTestingPlans](#)

Il s'agit d'une liste renvoyée de plans de test de la restauration.

Type : tableau d'objets [RestoreTestingPlanForList](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListRestoreTestingSelections

Service : AWS Backup

Renvoie une liste de sélections de tests de la restauration. Peut être filtrée par `MaxResults` et `RestoreTestingPlanName`.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?  
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[RestoreTestingPlanName](#)

Renvoie les sélections de tests de la restauration en fonction du nom du plan de tests de la restauration spécifié.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "RestoreTestingSelections": [
    {
      "CreationTime": number,
      "IamRoleArn": "string",
      "ProtectedResourceType": "string",
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[RestoreTestingSelections](#)

Les sélections de tests de la restauration renvoyées associées au plan de test de la restauration.

Type : tableau d'objets [RestoreTestingSelectionForList](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListScanJobs

Service : AWS Backup

Renvoie une liste des tâches de scan existantes pour un compte authentifié au cours des 30 derniers jours.

Syntaxe de la demande

```
GET /scan/jobs?
```

```
ByAccountId=ByAccountId&ByBackupVaultName=ByBackupVaultName&ByCompleteAfter=ByCompleteAfter&ByC
```

```
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByAccountId](#)

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de sauvegarde associées à l'ID de compte spécifié.

S'il est utilisé à partir d'un compte de gestion d' AWS Organizations, le transfert * renvoie toutes les offres d'emploi au sein de l'organisation.

Modèle : `^[0-9]{12}$`

[ByBackupVaultName](#)

Renvoie uniquement les tâches de numérisation qui seront stockées dans le coffre de sauvegarde spécifié. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Modèle : `^[a-zA-Z0-9\-\_\.\]{2,50}$`

[ByCompleteAfter](#)

Renvoie uniquement les tâches de numérisation terminées après une date exprimée au format Unix et en temps universel coordonné (UTC).

[ByCompleteBefore](#)

Renvoie uniquement les tâches de sauvegarde terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

[ByMalwareScanner](#)

Renvoie uniquement les tâches d'analyse pour le scanner de programmes malveillants spécifié. Actuellement, seuls les supports GUARDDUTY.

Valeurs valides : GUARDDUTY

[ByRecoveryPointArn](#)

Renvoie uniquement les tâches d'analyse exécutées sur le point de récupération spécifié.

[ByResourceArn](#)

Renvoie uniquement les tâches de scan qui correspondent à la ressource Amazon Resource Name (ARN) spécifiée.

[ByResourceType](#)

Renvoie les sélections de tests de la restauration en fonction du nom du plan de tests de la restauration spécifié.

- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud
- S3 pour Amazon Simple Storage Service (Amazon S3)

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Valeurs valides : EBS | EC2 | S3

[ByScanResultStatus](#)

Renvoie uniquement les tâches d'analyse pour les résultats d'analyse spécifiés :

- THREATS_FOUND
- NO_THREATS_FOUND

Valeurs valides : NO_THREATS_FOUND | THREATS_FOUND

[ByState](#)

Renvoie uniquement les tâches de numérisation correspondant à l'état de tâche de numérisation spécifié.

Valeurs valides : CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "ScanJobs": [
    {
      "AccountId": "string",
      "BackupVaultArn": "string",
      "BackupVaultName": "string",
      "CompletionDate": number,
      "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
      },
      "CreationDate": number,
      "IamRoleArn": "string",
      "MalwareScanner": "string",
      "RecoveryPointArn": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
```

```
"ScanBaseRecoveryPointArn": "string",
"ScanId": "string",
"ScanJobId": "string",
"ScanMode": "string",
"ScannerRoleArn": "string",
"ScanResult": {
  "ScanResultStatus": "string"
},
"State": "string",
"StatusMessage": "string"
}
]
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[ScanJobs](#)

Tableau de structures contenant des métadonnées relatives à vos tâches de numérisation renvoyées au format JSON.

Type : tableau d'objets [ScanJob](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListScanJobSummaries

Service : AWS Backup

Il s'agit d'une demande de résumé des tâches de scan créées ou exécutées au cours des 30 derniers jours.

Syntaxe de la demande

```
GET /audit/scan-job-summaries?  
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MalwareScanner=MalwareScanner&MaxResults=MaxResults  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccountId

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser cette valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

AGGREGATE_ALL agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY Le nombre de tâches quotidiennes pour le jour précédent.
- SEVEN_DAYS Le nombre de tâches quotidiennes des 7 jours précédents.
- FOURTEEN_DAYS Le nombre de tâches quotidiennes des 14 jours précédents.

Valeurs valides : ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

[MalwareScanner](#)

Renvoie uniquement les tâches d'analyse pour le scanner de programmes malveillants spécifié. Actuellement, le seul MalwareScanner est GUARDDUTY. Mais le terrain soutient également ANY, et AGGREGATE_ALL.

Valeurs valides : GUARDDUTY

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer MaxResults éléments, NextToken vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[ResourceType](#)

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande GetSupportedResourceTypes pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

AGGREGATE_ALL agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

[ScanResultStatus](#)

Renvoie uniquement les tâches d'analyse pour les résultats d'analyse spécifiés.

Valeurs valides : NO_THREATS_FOUND | THREATS_FOUND

[State](#)

Renvoie uniquement les tâches de numérisation correspondant à l'état de tâche de numérisation spécifié.

Valeurs valides : CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AggregationPeriod": "string",
  "NextToken": "string",
  "ScanJobSummaries": [
    {
      "AccountId": "string",
      "Count": number,
      "EndTime": number,
      "MalwareScanner": "string",
      "Region": "string",
      "ResourceType": "string",
      "ScanResultStatus": "string",
      "StartTime": number,
      "State": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAYLe nombre de tâches quotidiennes pour le jour précédent.
- SEVEN_DAYSLe nombre de tâches quotidiennes des 7 jours précédents.

- `FOURTEEN_DAYS` Le nombre de tâches quotidiennes des 14 jours précédents.

Valeurs valides : `'ONE_DAY'` | `'SEVEN_DAYS'` | `'FOURTEEN_DAYS'`

Type : Chaîne

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[ScanJobSummaries](#)

Les informations récapitulatives.

Type : tableau d'objets [ScanJobSummary](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`ServiceUnavailableException`

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListTags

Service : AWS Backup

Renvoie les balises attribuées à la ressource, telles qu'un point de restauration cible, un plan de sauvegarde ou un coffre de sauvegarde.

Cette opération renvoie des résultats en fonction du type de ressource utilisé dans la valeur `resourceArn`. Par exemple, les points de récupération d'Amazon DynamoDB avec paramètres avancés possèdent un ARN (Amazon Resource Name) qui commence par `arn:aws:backup`. Les points de restauration (sauvegardes) de DynamoDB lorsque les paramètres avancés ne sont pas activés possèdent un ARN commençant par `arn:aws:dynamodb`.

Lorsque cette opération est appelée et `resourceArn` que vous incluez des valeurs dont l'ARN est différent de `arn:aws:backup`, elle peut renvoyer l'une des exceptions répertoriées ci-dessous. Pour éviter cette exception, incluez uniquement les valeurs représentant les types de ressources entièrement gérés par AWS Backup. Elles ont un ARN qui commence `arn:aws:backup` et elles sont indiquées dans le tableau [Disponibilité des fonctionnalités par ressource](#).

Syntaxe de la demande

```
GET /tags/resourceArn?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[resourceArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource. Les cibles valides pour `ListTags` sont les points de récupération, les plans de sauvegarde et les coffres-forts de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Tags": {
    "string" : "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[Tags](#)

Informations sur les tags.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListTieringConfigurations

Service : AWS Backup

Renvoie une liste de configurations de hiérarchisation.

Syntaxe de la demande

```
GET /tiering-configurations/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "TieringConfigurations": [
    {
      "BackupVaultName": "string",
      "CreationTime": number,
      "LastUpdatedTime": number,
      "TieringConfigurationArn": "string",
      "TieringConfigurationName": "string"
    }
  ]
}
```

```
}  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : Chaîne

[TieringConfigurations](#)

Un tableau de configurations de hiérarchisation renvoyé par l'`ListTieringConfigurations` appel.

Type : tableau d'objets [TieringConfigurationsListMember](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

`InvalidParameterValueException`

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

`ServiceUnavailableException`

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutBackupVaultAccessPolicy

Service : AWS Backup

Définit une politique basée sur les ressources qui est utilisée pour gérer les autorisations d'accès au coffre-fort de sauvegarde sur la cible. Nécessite un nom de coffre-fort de sauvegarde et un document de stratégie d'accès au format JSON.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
  "Policy": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[Policy](#)

Document de stratégie d'accès au coffre-fort de sauvegarde au format JSON.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutBackupVaultLockConfiguration

Service : AWS Backup

Applique AWS Backup Vault Lock à un coffre-fort de sauvegarde, empêchant ainsi les tentatives de suppression de tout point de récupération stocké ou créé dans un coffre-fort de sauvegarde. Vault Lock empêche également les tentatives de mise à jour de la politique de cycle de vie qui contrôle la période de rétention de tout point de récupération actuellement stocké dans un coffre-fort de sauvegarde. Si cela est spécifié, Vault Lock applique une période de rétention minimale et maximale pour les futures tâches de sauvegarde et de copie ciblant un coffre-fort de sauvegarde.

Note

AWS Backup Vault Lock a été évalué par Cohasset Associates pour une utilisation dans des environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour plus d'informations sur le lien entre AWS Backup Vault Lock et ces réglementations, consultez [l'évaluation de conformité de Cohasset Associates](#).

Pour plus d'informations, consultez la page [AWS Backup Vault Lock](#).

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
  "ChangeableForDays": number,
  "MaxRetentionDays": number,
  "MinRetentionDays": number
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

La configuration AWS Backup Vault Lock qui indique le nom du coffre de sauvegarde qu'il protège.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[ChangeableForDays](#)

La configuration AWS Backup Vault Lock qui indique le nombre de jours avant la date de verrouillage. Par exemple, définir `ChangeableForDays` sur 30 le 1er janvier 2022 à 20 h UTC fixera la date de verrouillage au 31 janvier 2022 à 20 h UTC.

AWS Backup impose une période de réflexion de 72 heures avant que Vault Lock n'entre en vigueur et ne devienne immuable. Vous devez donc définir `ChangeableForDays` sur 3 ou plus.

Avant la date de verrouillage, vous pouvez supprimer le verrouillage du coffre-fort à l'aide de `DeleteBackupVaultLockConfiguration` ou modifier la configuration du verrouillage du coffre-fort en utilisant `PutBackupVaultLockConfiguration`. À compter de la date de verrouillage, le verrouillage du coffre-fort devient immuable et ne peut être ni modifié ni supprimé.

Si ce paramètre n'est pas spécifié, vous pouvez supprimer le verrouillage du coffre-fort à l'aide de `DeleteBackupVaultLockConfiguration` ou modifier la configuration du verrouillage du coffre-fort en utilisant `PutBackupVaultLockConfiguration` à tout moment.

Type : long

Obligatoire : non

[MaxRetentionDays](#)

La configuration AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de restauration. Ce paramètre peut être utile si, par exemple, les politiques de votre organisation vous obligent à détruire certaines données après les avoir conservées pendant quatre ans (1 460 jours).

Si ce paramètre n'est pas inclus, le verrouillage du coffre-fort n'applique pas de période de conservation maximale sur les points de récupération dans le coffre-fort. Si ce paramètre est inclus sans valeur, le verrouillage du coffre-fort n'appliquera pas de période de conservation maximale.

Si ce paramètre est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de conservation égale ou inférieure à la période

de conservation maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. La période de rétention maximale la plus longue que vous puissiez spécifier est de 36 500 jours (environ 100 ans). Les points de récupération déjà enregistrés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

MinRetentionDays

La configuration AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de restauration. Ce paramètre peut être utile si, par exemple, les politiques de votre organisation vous obligent à conserver certaines données pendant au moins sept ans (2 555 jours).

Ce paramètre est obligatoire lors de la création d'un verrou de coffre-fort AWS CloudFormation ; dans le cas contraire, ce paramètre est facultatif. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'appliquera pas de période de conservation minimale.

Si ce paramètre est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de conservation égale ou supérieure à la période de conservation minimale. Si la période de conservation de la tâche est plus courte que cette période de conservation minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. La période de rétention minimale la plus courte que vous puissiez spécifier est d'un jour. Les points de récupération déjà enregistrés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutBackupVaultNotifications

Service : AWS Backup

Active les notifications sur un coffre-fort de sauvegarde pour la rubrique et les événements spécifiés.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
  "BackupVaultEvents": [ "string" ],
  "SNSTopicArn": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupVaultEvents](#)

Tableau d'événements qui indiquent le statut des tâches de sauvegarde des ressources dans le coffre-fort de sauvegarde. Pour obtenir la liste des événements pris en charge, des cas d'utilisation courants et des exemples de code, consultez la section [Options de notification avec AWS Backup](#).

 Note

La liste ci-dessous inclut à la fois les événements pris en charge et les événements obsolètes qui ne sont plus utilisés (à titre de référence). Les événements déconseillés ne renvoient ni statuts ni notifications.

Type : tableau de chaînes

Valeurs valides : BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED |
BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED |
RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL
| RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL |
COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED
| BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED |
S3_RESTORE_OBJECT_FAILED | CONTINUOUS_BACKUP_INTERRUPTED |
RECOVERY_POINT_INDEX_COMPLETED | RECOVERY_POINT_INDEX_DELETED |
RECOVERY_POINT_INDEXING_FAILED

Obligatoire : oui

SNSTopicArn

L'Amazon Resource Name (ARN) qui spécifie la rubrique des événements d'un coffre-fort de secours ; par exemple, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Type : String

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutRestoreValidationResult

Service : AWS Backup

Cette demande vous permet d'envoyer les résultats de validation de votre test de la restauration autonome indépendant. `RestoreJobId` et `ValidationStatus` sont obligatoires. Vous pouvez éventuellement saisir un `ValidationStatusMessage`.

Syntaxe de la demande

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
  "ValidationStatus": "string",
  "ValidationStatusMessage": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[restoreJobId](#)

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[ValidationStatus](#)

État de la validation de votre restauration.

Type : String

Valeurs valides : FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

Obligatoire : oui

ValidationStatusMessage

Il s'agit d'une chaîne de message facultative que vous pouvez saisir pour décrire le statut de validation du test de la restauration.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 204
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

RevokeRestoreAccessBackupVault

Service : AWS Backup

Révoque l'accès à un coffre-fort de sauvegarde avec accès à la restauration, supprimant ainsi la possibilité de restaurer ses points de restauration et supprimant définitivement le coffre-fort.

Syntaxe de la demande

```
DELETE /logically-air-gapped-backup-vaults/backupVaultName/restore-access-backup-vaults/restoreAccessBackupVaultArn?requesterComment=RequesterComment HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Nom du coffre de sauvegarde source associé au coffre de sauvegarde d'accès à la restauration à révoquer.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

[RequesterComment](#)

Un commentaire expliquant la raison de la révocation de l'accès au coffre de sauvegarde de l'accès à la restauration.

[restoreAccessBackupVaultArn](#)

L'ARN du coffre de sauvegarde de l'accès à la restauration à révoquer.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartBackupJob

Service : AWS Backup

Démarre une tâche de sauvegarde à la demande pour la ressource spécifiée.

Syntaxe de la demande

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
  "BackupOptions": {
    "string" : "string"
  },
  "BackupVaultName": "string",
  "CompleteWindowMinutes": number,
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Index": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "LogicallyAirGappedBackupVaultArn": "string",
  "RecoveryPointTags": {
    "string" : "string"
  },
  "ResourceArn": "string",
  "StartWindowMinutes": number
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupOptions

L'option de sauvegarde pour une ressource sélectionnée. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Valeurs valides : définissez sur "WindowsVSS":"enabled" pour activer l'option de sauvegarde WindowsVSS et créer une sauvegarde Windows VSS. Définissez sur "WindowsVSS":"disabled" pour créer une sauvegarde régulière. L'option WindowsVSS n'est pas activée par défaut.

Type : mappage chaîne/chaîne

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompleteWindowMinutes

Valeur en minutes pendant laquelle une sauvegarde démarrée avec succès doit se terminer, faute de quoi AWS Backup annule la tâche. Cette valeur est facultative. Cette valeur commence le compte à rebours à partir du moment auquel la sauvegarde a été planifiée. Cela n'ajoute pas de temps supplémentaire pour `StartWindowMinutes`, ni si la sauvegarde a démarré plus tard que prévu.

Comme `StartWindowMinutes`, ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Type : Long

Obligatoire : non

[IamRoleArn](#)

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

[IdempotencyToken](#)

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartBackupJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

[Index](#)

Incluez ce paramètre pour activer la création d'index si votre tâche de sauvegarde possède un type de ressource qui prend en charge les index de sauvegarde.

Les types de ressources qui prennent en charge les index de sauvegarde sont les suivants :

- EBS pour Amazon Elastic Block Store
- S3 pour Amazon Simple Storage Service (Amazon S3)

L'index peut avoir 1 des 2 valeurs possibles, `ENABLED` soit `DISABLED`.

Pour créer un index de sauvegarde pour un point de `ACTIVE` restauration éligible qui ne possède pas encore d'index de sauvegarde, définissez la valeur sur `ENABLED`.

Pour supprimer un index de sauvegarde, définissez la valeur sur `DISABLED`.

Type : Chaîne

Valeurs valides : `ENABLED` | `DISABLED`

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup fera automatiquement la transition et expirera les sauvegardes en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Ce paramètre a une valeur maximale de 100 ans (36 500 jours).

Type : objet [Lifecycle](#)

Obligatoire : non

LogicallyAirGappedBackupVaultArn

L'ARN d'un coffre-fort à espacement logique. L'ARN doit appartenir au même compte et à la même région. Si elles sont fournies, les ressources entièrement gérées prises en charge sont sauvegardées directement dans un coffre-fort à espacement logique, tandis que les autres ressources prises en charge créent un instantané temporaire (facturable) dans le coffre-fort de sauvegarde, puis le copient dans un coffre-fort à espacement logique. Les ressources non prises en charge ne sont sauvegardées que dans le coffre de sauvegarde spécifié.

Type : chaîne

Obligatoire : non

RecoveryPointTags

Les balises à attribuer aux ressources.

Type : mappage chaîne/chaîne

Obligatoire : non

[ResourceArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : Chaîne

Obligatoire : oui

[StartWindowMinutes](#)

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative et elle est de 8 heures par défaut. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste CREATED jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à RUNNING) ou jusqu'à ce que le statut de la tâche passe à EXPIRED (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : Long

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupJobId": "string",
  "CreationDate": number,
  "IsParent": boolean,
  "RecoveryPointArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupJobId](#)

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : Chaîne

[CreationDate](#)

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[IsParent](#)

Il s'agit d'une valeur booléenne renvoyée indiquant qu'il s'agit d'une tâche de sauvegarde parent (composite).

Type : Boolean

[RecoveryPointArn](#)

Remarque : ce champ n'est renvoyé que pour les ressources Amazon EFS et Advanced DynamoDB.

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartCopyJob

Service : AWS Backup

Démarre une tâche pour créer une copie unique de la ressource spécifiée.

Ne prend pas en charge les sauvegardes continues.

Voir [Réessayer une tâche de copie](#) pour plus d'informations sur la manière dont les nouvelles AWS Backup tentatives de copie peuvent être effectuées.

Syntaxe de la demande

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
  "DestinationBackupVaultArn": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "RecoveryPointArn": "string",
  "SourceBackupVaultName": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[DestinationBackupVaultArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de destination sur lequel effectuer la copie ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

Obligatoire : oui

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour copier le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartCopyJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Lifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Type : objet [Lifecycle](#)

Obligatoire : non

[RecoveryPointArn](#)

ARN identifiant de manière unique un point de récupération à utiliser pour la tâche de copie ; par exemple, arn:aws:backup:us-east-1:123456789012:recovery-point:1 B5E7-9EB0-435A-A80B-108B488B0D45. EB3

Type : Chaîne

Obligatoire : oui

[SourceBackupVaultName](#)

Le nom d'un conteneur source logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CopyJobId": "string",
  "CreationDate": number,
  "IsParent": boolean
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CopyJobId

Identifie de manière unique une tâche de copie.

Type : Chaîne

CreationDate

Date et heure de création d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IsParent

Il s'agit d'une valeur booléenne renvoyée indiquant qu'il s'agit d'une tâche de copie parent (composite).

Type : Boolean

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartReportJob

Service : AWS Backup

Démarre une tâche de rapport à la demande pour le plan de rapport spécifié.

Syntaxe de la demande

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
  "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartReportJobInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ReportJobId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ReportJobId](#)

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. L'ID de tâche de rapport ne peut pas être modifié.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartRestoreJob

Service : AWS Backup

Récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN).

Syntaxe de la demande

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
  "CopySourceTagsToRestoredResource": boolean,
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "Metadata": {
    "string" : "string"
  },
  "RecoveryPointArn": "string",
  "ResourceType": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

CopySourceTagsToRestoredResource

Ce paramètre est facultatif. S'il est égal à `True`, les balises incluses dans la sauvegarde seront copiées sur la ressource restaurée.

Cela ne peut être appliqué qu'aux sauvegardes créées via AWS Backup.

Type : booléen

Obligatoire : non

IamRoleArn

Le nom de ressource Amazon (ARN) du rôle IAM AWS Backup utilisé pour créer la ressource cible ; par exemple `:arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartRestoreJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Metadata

Un ensemble de paires clé-valeur de métadonnées.

Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Par exemple, vous devrez peut-être fournir un nouveau nom de ressource si l'original existe déjà.

Pour plus d'informations sur les métadonnées de chaque ressource, consultez les rubriques suivantes :

- [Métadonnées pour Amazon Aurora](#)
- [Métadonnées pour Amazon DocumentDB](#)
- [Métadonnées pour AWS CloudFormation](#)
- [Métadonnées pour Amazon DynamoDB](#)
- [Métadonnées pour Amazon EBS](#)
- [Métadonnées pour Amazon EC2](#)
- [Métadonnées pour Amazon EFS](#)
- [Métadonnées pour Amazon FSx](#)
- [Métadonnées pour Amazon Neptune](#)
- [Métadonnées pour Amazon RDS](#)
- [Métadonnées pour Amazon Redshift](#)

- [Métadonnées pour AWS Storage Gateway](#)
- [Métadonnées pour Amazon S3](#)
- [Métadonnées pour Amazon Timestream](#)
- [Métadonnées pour les machines virtuelles](#)

Type : mappage chaîne/chaîne

Obligatoire : oui

[RecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : String

Obligatoire : oui

[ResourceType](#)

Démarre une tâche visant à restaurer un point de récupération pour l'une des ressources suivantes :

- Aurora- Amazon Aurora
- DocumentDB- Amazon DocumentDB
- CloudFormation - AWS CloudFormation
- DynamoDB- Amazon DynamoDB
- EBS- Boutique Amazon Elastic Block
- EC2- Amazon Elastic Compute Cloud
- EFS- Amazon Elastic File System
- FSx- Amazon FSx
- Neptune- Amazon Neptune
- RDS- Amazon Relational Database Service
- Redshift- Amazon Redshift
- Storage Gateway - AWS Storage Gateway
- S3- Amazon Simple Storage Service

- Timestream- Amazon Timestream
- VirtualMachine- Machines virtuelles

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "RestoreJobId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[RestoreJobId](#)

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartScanJob

Service : AWS Backup

Lance les tâches de numérisation pour des ressources spécifiques.

Syntaxe de la demande

```
PUT /scan/job HTTP/1.1
Content-type: application/json

{
  "BackupVaultName": "string",
  "IamRoleArn": "string",
  "IdempotencyToken": "string",
  "MalwareScanner": "string",
  "RecoveryPointArn": "string",
  "ScanBaseRecoveryPointArn": "string",
  "ScanMode": "string",
  "ScannerRoleArn": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Type : Chaîne

Obligatoire : oui

[IamRoleArn](#)

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

[IdempotencyToken](#)

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartScanJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

[MalwareScanner](#)

Spécifie le scanner de programmes malveillants utilisé lors de la tâche d'analyse. Actuellement, seuls les supports `GUARDDUTY`.

Type : Chaîne

Valeurs valides : `GUARDDUTY`

Obligatoire : oui

[RecoveryPointArn](#)

Un Amazon Resource Name (ARN) qui identifie de manière unique un point de récupération. Il s'agit de votre point de récupération cible pour une analyse complète. Si vous exécutez une analyse incrémentielle, il s'agira d'un point de récupération créé après la sélection de votre point de récupération de base.

Type : Chaîne

Obligatoire : oui

[ScanBaseRecoveryPointArn](#)

Un ARN qui identifie de manière unique le point de récupération de base à utiliser pour le scan incrémentiel.

Type : chaîne

Obligatoire : non

ScanMode

Spécifie le type de numérisation utilisé pour la tâche de numérisation.

Comprend :

- **FULL_SCAN** Analysera l'intégralité du lignage de données dans la sauvegarde.
- **INCREMENTAL_SCAN** Analysera la différence de données entre le point de récupération cible et l'ARN du point de récupération de base.

Type : Chaîne

Valeurs valides : FULL_SCAN | INCREMENTAL_SCAN

Obligatoire : oui

ScannerRoleArn

Spécifié l'ARN du rôle de scanner IAM.

Type : Chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 201
Content-type: application/json

{
  "CreationDate": number,
  "ScanJobId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

CreationDate

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ScanJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StopBackupJob

Service : AWS Backup

Tente d'annuler une tâche afin de créer une sauvegarde unique d'une ressource.

Cette action n'est pas prise en charge pour les services suivants :

- Amazon Aurora
- Amazon DocumentDB (compatible avec MongoDB)
- Amazon FSx pour Lustre
- Amazon FSx pour NetApp ONTAP
- Amazon FSx pour OpenZFS
- Serveur FSx de fichiers Amazon pour Windows
- Amazon Neptune
- Bases de données SAP HANA sur les instances Amazon EC2
- Amazon RDS

Syntaxe de la demande

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

TagResource

Service : AWS Backup

Assigne un ensemble de paires clé-valeur à une ressource.

Syntaxe de la demande

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[resourceArn](#)

L'ARN qui identifie de manière unique la ressource.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[Tags](#)

Des paires clé-valeur utilisées pour vous aider à organiser vos ressources. Vous pouvez attribuer vos propres métadonnées aux ressources que vous créez. Pour plus de clarté, voici la structure pour attribuer des balises : [{"Key":"string","Value":"string"}].

Type : mappage chaîne/chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UntagResource

Service : AWS Backup

Supprime un ensemble de paires clé-valeur d'un point de récupération, d'un plan de sauvegarde ou d'un coffre-fort de sauvegarde identifié par un Amazon Resource Name (ARN)

Cette API n'est pas prise en charge pour les points de récupération pour les types de ressources tels qu'Aurora et Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune et Amazon RDS.

Syntaxe de la demande

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json
```

```
{
  "TagKeyList": [ "string" ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

resourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource balisée.

ARNs qui n'incluent pas backup sont incompatibles avec le balisage. TagResource et si UntagResource la valeur est invalide ARNs , une erreur se produira. Le contenu ARN acceptable peut inclure `arn:aws:backup:us-east`. Un contenu ARN non valide peut ressembler à `arn:aws:ec2:us-east`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

TagKeyList

Les clés permettant d'identifier les balises clé-valeur à supprimer d'une ressource.

Type : tableau de chaînes

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateBackupPlan

Service : AWS Backup

Met à jour le plan de sauvegarde spécifié. La nouvelle version est identifiée de manière unique par son identifiant.

Syntaxe de la demande

```
POST /backup/plans/backupPlanId HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "BackupPlan": {
    "AdvancedBackupSettings": [
      {
        "BackupOptions": {
          "string": "string"
        },
        "ResourceType": "string"
      }
    ],
    "BackupPlanName": "string",
    "Rules": [
      {
        "CompletionWindowMinutes": number,
        "CopyActions": [
          {
            "DestinationBackupVaultArn": "string",
            "Lifecycle": {
              "DeleteAfterDays": number,
              "DeleteAfterEvent": "string",
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
            }
          }
        ],
        "EnableContinuousBackup": boolean,
        "IndexActions": [
          {
            "ResourceTypes": [ "string" ]
          }
        ],
        "Lifecycle": {
```

```

        "DeleteAfterDays": number,
        "DeleteAfterEvent": "string",
        "MoveToColdStorageAfterDays": number,
        "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointTags": {
        "string" : "string"
    },
    "RuleName": "string",
    "ScanActions": [
        {
            "MalwareScanner": "string",
            "ScanMode": "string"
        }
    ],
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowMinutes": number,
    "TargetBackupVaultName": "string",
    "TargetLogicallyAirGappedBackupVaultArn": "string"
    }
],
"ScanSettings": [
    {
        "MalwareScanner": "string",
        "ResourceTypes": [ "string" ],
        "ScannerRoleArn": "string"
    }
]
}
}

```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupPlanId](#)

ID du plan de sauvegarde.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[BackupPlan](#)

Le corps d'un plan de sauvegarde. Comprend un BackupPlanName et un ou plusieurs ensembles de Rules.

Type : objet [BackupPlanInput](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "AdvancedBackupSettings": [
    {
      "BackupOptions": {
        "string" : "string"
      },
      "ResourceType": "string"
    }
  ],
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "CreationDate": number,
  "ScanSettings": [
    {
      "MalwareScanner": "string",
      "ResourceTypes": [ "string" ],
      "ScannerRoleArn": "string"
    }
  ],
  "VersionId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[AdvancedBackupSettings](#)

Contient une liste d'`BackupOptions` pour chaque type de ressource.

Type : tableau d'objets [AdvancedBackupSetting](#)

[BackupPlanArn](#)

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : Chaîne

[BackupPlanId](#)

Identifie de façon unique un plan de secours.

Type : Chaîne

[CreationDate](#)

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[ScanSettings](#)

Contient votre configuration d'analyse pour le plan de sauvegarde et inclut le scanner de logiciels malveillants, les ressources que vous avez sélectionnées et le rôle d'analyseur.

Type : tableau d'objets [ScanSetting](#)

[VersionId](#)

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateFramework

Service : AWS Backup

Met à jour le framework spécifié.

Syntaxe de la demande

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
  "FrameworkControls": [
    {
      "ControlInputParameters": [
        {
          "ParameterName": "string",
          "ParameterValue": "string"
        }
      ],
      "ControlName": "string",
      "ControlScope": {
        "ComplianceResourceIds": [ "string" ],
        "ComplianceResourceTypes": [ "string" ],
        "Tags": {
          "string" : "string"
        }
      }
    }
  ],
  "FrameworkDescription": "string",
  "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

frameworkName

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[FrameworkControls](#)

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets [FrameworkControl](#)

Obligatoire : non

[FrameworkDescription](#)

Une description facultative du cadre avec 1 024 caractères au maximum.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

[IdempotencyToken](#)

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `UpdateFrameworkInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{  
  "CreationTime": number,  
  "FrameworkArn": "string",  
  "FrameworkName": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, 2020-07-10T15:00:00.000-08:00 représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

[FrameworkArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : String

[FrameworkName](#)

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateGlobalSettings

Service : AWS Backup

Indique si le AWS compte est activé pour la sauvegarde entre comptes. Renvoie une erreur si le compte n'est pas un compte de gestion Organizations. Utilisez l'API DescribeGlobalSettings pour déterminer les paramètres actuels.

Syntaxe de la demande

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
  "GlobalSettings": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[GlobalSettings](#)

Les entrées peuvent inclure :

Une valeur pour isCrossAccountBackupEnabled et une région. Exemple: update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2.

Une valeur pour l'approbation multipartite, intitulée « Mpa » : isMpaEnabled Les valeurs peuvent être vraies ou fausses. Exemple: update-global-settings --global-settings isMpaEnabled=false --region us-west-2.

Une valeur pour la création d'un rôle lié à un service de sauvegarde, stylisée comme isDelegatedAdministratorEnabled Les valeurs peuvent être vraies ou fausses. Exemple: update-global-settings --global-settings isDelegatedAdministratorEnabled=false --region us-west-2.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateRecoveryPointIndexSettings

Service : AWS Backup

Cette opération met à jour les paramètres d'un indice de point de récupération.

Obligatoires : BackupVaultName, RecoveryPointArn, et IAMRole Arn

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/index HTTP/1.1
Content-type: application/json
```

```
{
  "IamRoleArn": "string",
  "Index": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Les caractères acceptés incluent les lettres minuscules, les chiffres et les traits d'union.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[IamRoleArn](#)

Ceci indique l'ARN du rôle IAM utilisé pour cette opération.

Par exemple, `arn:aws:iam::123456789012:role/S3access`

Type : chaîne

Obligatoire : non

[Index](#)

L'index peut avoir 1 des 2 valeurs possibles, `ENABLED` soit `DISABLED`.

Pour créer un index de sauvegarde pour un point de `ACTIVE` restauration éligible qui ne possède pas encore d'index de sauvegarde, définissez la valeur sur `ENABLED`.

Pour supprimer un index de sauvegarde, définissez la valeur sur `DISABLED`.

Type : String

Valeurs valides : `ENABLED` | `DISABLED`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultName": "string",
  "Index": "string",
  "IndexStatus": "string",
  "RecoveryPointArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

[Index](#)

L'index peut avoir 1 des 2 valeurs possibles, `ENABLED` soit `DISABLED`.

La valeur de `ENABLED` signifie qu'un index de sauvegarde pour un point `ACTIVE` de restauration éligible a été créé.

La valeur de `DISABLED` signifie qu'un index de sauvegarde a été supprimé.

Type : String

Valeurs valides : `ENABLED` | `DISABLED`

[IndexStatus](#)

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Un point de récupération dont l'index a le statut de `ACTIVE` peut être inclus dans une recherche.

Type : String

Valeurs valides : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

[RecoveryPointArn](#)

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateRecoveryPointLifecycle

Service : AWS Backup

Définit le cycle de vie de transition d'un point de récupération.

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Important

Si votre cycle de vie utilise actuellement les paramètres `DeleteAfterDays` `MoveToColdStorageAfterDays`, incluez ces paramètres et leurs valeurs lorsque vous appelez cette opération. Le fait de ne pas les inclure peut entraîner la mise à jour de votre plan avec des valeurs nulles.

Cette opération ne prend pas en charge les sauvegardes continues.

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json
```

```
{
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
```



```
}  
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[backupVaultName](#)

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : oui

[recoveryPointArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[Lifecycle](#)

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Type : objet [Lifecycle](#)

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "BackupVaultArn": "string",
  "CalculatedLifecycle": {
    "DeleteAt": number,
    "MoveToColdStorageAt": number
  },
  "Lifecycle": {
    "DeleteAfterDays": number,
    "DeleteAfterEvent": "string",
    "MoveToColdStorageAfterDays": number,
    "OptInToArchiveForSupportedResources": boolean
  },
  "RecoveryPointArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BackupVaultArn](#)

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

[CalculatedLifecycle](#)

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet [CalculatedLifecycle](#)

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet [Lifecycle](#)

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateRegionSettings

Service : AWS Backup

Met à jour les paramètres actuels d'activation du service pour la région.

Utilisez l'API DescribeRegionSettings pour déterminer les types de ressources pris en charge.

Syntaxe de la demande

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
  "ResourceTypeManagementPreference": {
    "string" : boolean
  },
  "ResourceTypeOptInPreference": {
    "string" : boolean
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ResourceTypeManagementPreference

Active ou désactive AWS Backup la gestion complète des sauvegardes pour un type de ressource. [Pour activer AWS Backup la gestion complète de DynamoDB ainsi que les fonctionnalités avancées AWS Backup de sauvegarde DynamoDB, suivez la procédure pour activer la sauvegarde DynamoDB avancée par programmation.](#)

Type : chaîne vers un mappage booléen

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

[ResourceTypeOptInPreference](#)

Met à jour la liste des services ainsi que les préférences d'activation pour la région.

Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués. Si un type de ressource est explicitement attribué à un plan de sauvegarde, tel qu'Amazon S3 EC2, Amazon ou Amazon RDS, il sera inclus dans la sauvegarde même si l'opt-in n'est pas activé pour ce service en particulier. Si un type de ressource et des balises sont spécifiés dans une attribution de ressource, le type de ressource spécifié dans le plan de sauvegarde est prioritaire par rapport à la condition de balise. Les paramètres d'activation du service ne sont pas pris en compte dans ce cas.

Type : chaîne vers un mappage booléen

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateReportPlan

Service : AWS Backup

Met à jour le plan de rapport spécifié.

Syntaxe de la demande

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json
```

```
{
  "IdempotencyToken": "string",
  "ReportDeliveryChannel": {
    "Formats": [ "string" ],
    "S3BucketName": "string",
    "S3KeyPrefix": "string"
  },
  "ReportPlanDescription": "string",
  "ReportSetting": {
    "Accounts": [ "string" ],
    "FrameworkArns": [ "string" ],
    "NumberOfFrameworks": number,
    "OrganizationUnits": [ "string" ],
    "Regions": [ "string" ],
    "ReportTemplate": "string"
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique du plan de rapport. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[IdempotencyToken](#)

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `UpdateReportPlanInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

[ReportDeliveryChannel](#)

Les informations sur l'endroit où envoyer vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet [ReportDeliveryChannel](#)

Obligatoire : non

[ReportPlanDescription](#)

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

[ReportSetting](#)

Modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si le modèle de rapport est `RESOURCE_COMPLIANCE_REPORT` ou `CONTROL_COMPLIANCE_REPORT`, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet [ReportSetting](#)

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "ReportPlanArn": "string",
  "ReportPlanName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Date et heure de création d'un plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[ReportPlanArn](#)

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : String

[ReportPlanName](#)

Le nom unique du plan de rapport.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateRestoreTestingPlan

Service : AWS Backup

Cette demande enverra des modifications au plan de test de la restauration que vous avez spécifié. `RestoreTestingPlanName` ne peut pas être mis à jour après sa création.

`RecoveryPointSelection` peut contenir :

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json
```

```
{
  "RestoreTestingPlan": {
    "RecoveryPointSelection": {
      "Algorithm": "string",
      "ExcludeVaults": [ "string" ],
      "IncludeVaults": [ "string" ],
      "RecoveryPointTypes": [ "string" ],
      "SelectionWindowDays": number
    },
    "ScheduleExpression": "string",
    "ScheduleExpressionTimezone": "string",
    "StartWindowHours": number
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom du plan de test de restauration.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[RestoreTestingPlan](#)

Spécifie le corps d'un plan de test de la restauration.

Type : objet [RestoreTestingPlanForUpdate](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "UpdateTime": number
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Heure à laquelle le plan de test des ressources a été créé.

Type : Timestamp

[RestoreTestingPlanArn](#)

ARN (Amazon Resource Name) unique du plan de test de la restauration.

Type : String

RestoreTestingPlanName

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : String

UpdateTime

Heure à laquelle la mise à jour s'est terminée pour le plan de test de restauration.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

UpdateRestoreTestingSelection

Service : AWS Backup

Met à jour la sélection de test de restauration spécifiée.

La plupart des éléments, à l'exception de `RestoreTestingSelectionName`, peuvent être mis à jour avec cette demande.

Vous pouvez utiliser une ressource ARNs ou des conditions protégées, mais pas les deux.

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json
```

```
{
  "RestoreTestingSelection": {
    "IamRoleArn": "string",
    "ProtectedResourceArns": [ "string" ],
    "ProtectedResourceConditions": {
      "StringEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ],
      "StringNotEquals": [
        {
          "Key": "string",
          "Value": "string"
        }
      ]
    },
    "RestoreMetadataOverrides": {
      "string" : "string"
    },
    "ValidationWindowHours": number
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[RestoreTestingPlanName](#)

Le nom du plan de test de la restauration est requis pour mettre à jour le plan de test indiqué.

Obligatoire : oui

[RestoreTestingSelectionName](#)

Nom de la sélection de test de restauration requise de la sélection de test de restauration que vous souhaitez mettre à jour.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[RestoreTestingSelection](#)

Pour mettre à jour votre sélection de tests de restauration, vous pouvez utiliser des ressources ARNs ou des conditions protégées, mais pas les deux. En d'autres termes, si votre sélection a `ProtectedResourceArns`, la demande de mise à jour avec le paramètre `ProtectedResourceConditions` échouera.

Type : objet [RestoreTestingSelectionForUpdate](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "RestoreTestingPlanArn": "string",
  "RestoreTestingPlanName": "string",
  "RestoreTestingSelectionName": "string",
```

```
"UpdateTime": number
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Heure à laquelle la sélection des ressources testées a été mise à jour avec succès.

Type : Timestamp

[RestoreTestingPlanArn](#)

Chaîne unique qui est le nom du plan de test de la restauration.

Type : String

[RestoreTestingPlanName](#)

Le plan de test de restauration auquel la sélection de test de restauration mise à jour est associée.

Type : String

[RestoreTestingSelectionName](#)

Nom de la sélection de test de restauration renvoyé.

Type : String

[UpdateTime](#)

Heure à laquelle la mise à jour s'est terminée pour la sélection du test de restauration.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateTieringConfiguration

Service : AWS Backup

Cette demande enverra des modifications à la configuration de hiérarchisation que vous avez spécifiée. TieringConfigurationName ne peut pas être mis à jour après sa création.

ResourceSelection peut contenir :

- Resources
- TieringDownSettingsInDays
- ResourceType

Syntaxe de la demande

```
PUT /tiering-configurations/tieringConfigurationName HTTP/1.1
Content-type: application/json

{
  "TieringConfiguration": {
    "BackupVaultName": "string",
    "ResourceSelection": [
      {
        "Resources": [ "string" ],
        "ResourceType": "string",
        "TieringDownSettingsInDays": number
      }
    ]
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

tieringConfigurationName

Nom de la configuration de hiérarchisation à mettre à jour.

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[TieringConfiguration](#)

Spécifie le corps d'une configuration de hiérarchisation.

Type : objet [TieringConfigurationInputForUpdate](#)

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "LastUpdatedTime": number,
  "TieringConfigurationArn": "string",
  "TieringConfigurationName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[CreationTime](#)

Date et heure de création d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[LastUpdatedTime](#)

Date et heure de mise à jour d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `LastUpdatedTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

[TieringConfigurationArn](#)

Un Amazon Resource Name (ARN) qui identifie de manière unique la configuration de hiérarchisation mise à jour.

Type : Chaîne

[TieringConfigurationName](#)

Cette chaîne unique est le nom de la configuration de hiérarchisation.

Type : Chaîne

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AlreadyExistsException

La ressource demandée existe déjà.

Arn

Context

CreatorRequestId

Type

Code d'état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Context

Type

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Context

Type

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Context

Type

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Context

Type

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Context

Type

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Context

Type

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

AWS Backup gateway

Les actions suivantes sont prises en charge par AWS Backup gateway :

- [AssociateGatewayToServer](#)
- [CreateGateway](#)
- [DeleteGateway](#)
- [DeleteHypervisor](#)
- [DisassociateGatewayFromServer](#)

- [GetBandwidthRateLimitSchedule](#)
- [GetGateway](#)
- [GetHypervisor](#)
- [GetHypervisorPropertyMappings](#)
- [GetVirtualMachine](#)
- [ImportHypervisorConfiguration](#)
- [ListGateways](#)
- [ListHypervisors](#)
- [ListTagsForResource](#)
- [ListVirtualMachines](#)
- [PutBandwidthRateLimitSchedule](#)
- [PutHypervisorPropertyMappings](#)
- [PutMaintenanceStartTime](#)
- [StartVirtualMachinesMetadataSync](#)
- [TagResource](#)
- [TestHypervisorConfiguration](#)
- [UntagResource](#)
- [UpdateGatewayInformation](#)
- [UpdateGatewaySoftwareNow](#)
- [UpdateHypervisor](#)

AssociateGatewayToServer

Service : AWS Backup gateway

Associe une passerelle de sauvegarde à votre serveur. Une fois le processus d'association terminé, vous pouvez sauvegarder et restaurer votre compte VMs via la passerelle.

Syntaxe de la requête

```
{
  "GatewayArn": "string",
  "ServerArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle. Utilisez cette `ListGateways` opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

[ServerArn](#)

Amazon Resource Name (ARN) du serveur qui héberge vos machines virtuelles.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[GatewayArn](#)

Amazon Resource Name (ARN) d'une passerelle.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)

- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateGateway

Service : AWS Backup gateway

Crée une passerelle de sauvegarde. Une fois la passerelle créée, vous pouvez l'associer à un serveur à l'aide de l'opération `AssociateGatewayToServer`.

Syntaxe de la requête

```
{
  "ActivationKey": "string",
  "GatewayDisplayName": "string",
  "GatewayType": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[ActivationKey](#)

La clé d'activation de la passerelle créée.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Modèle : `[0-9a-zA-Z\-\ ]+`

Obligatoire : oui

[GatewayDisplayName](#)

Le nom d'affichage de la passerelle créée.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : oui

GatewayType

Type de passerelle créée.

Type : String

Valeurs valides : BACKUP_VM

Obligatoire : oui

Tags

Liste jusqu'à 50 balises à attribuer à la passerelle. Chaque balise est une paire clés-valeurs.

Type : tableau d'objets [Tag](#)

Obligatoire : non

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous créez.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteGateway

Service : AWS Backup gateway

Supprime une passerelle de sauvegarde.

Syntaxe de la requête

```
{  
  "GatewayArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle à supprimer.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez supprimée.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DeleteHypervisor

Service : AWS Backup gateway

Supprime un hyperviseur.

Syntaxe de la requête

```
{  
  "HypervisorArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur à supprimer.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "HypervisorArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur que vous avez supprimé.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

ErrorCode

Une description des raisons pour lesquelles vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne qui s'est produite.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

DisassociateGatewayFromServer

Service : AWS Backup gateway

Dissocie une passerelle de sauvegarde du serveur spécifié. Une fois le processus de dissociation terminé, la passerelle ne peut plus accéder aux machines virtuelles du serveur.

Syntaxe de la requête

```
{  
  "GatewayArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle à dissocier.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez dissociée.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetBandwidthRateLimitSchedule

Service : AWS Backup gateway

Récupère la planification de limite de débit de la bande passante pour une passerelle spécifiée. Par défaut, les passerelles n'ont pas de planification de limite de débit de la bande passante, ce qui signifie qu'aucune limitation de débit de bande passante n'est en vigueur. Utilisez ceci pour obtenir la planification de limite de débit de la bande passante d'une passerelle.

Syntaxe de la requête

```
{
  "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette [ListGateways](#) opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9+){3}\/[a-zA-Z0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "BandwidthRateLimitIntervals": [
    {
      "AverageUploadRateLimitInBitsPerSec": number,
```



```

    "DaysOfWeek": [ number ],
    "EndHourOfDay": number,
    "EndMinuteOfHour": number,
    "StartHourOfDay": number,
    "StartMinuteOfHour": number
  }
],
  "GatewayArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[BandwidthRateLimitIntervals](#)

Un tableau contenant les intervalles de planification de limite de débit de la bande passante pour une passerelle. Lorsqu'aucun intervalle de limite de débit de bande passante n'a été planifié, le tableau est vide.

Type : tableau d'objets [BandwidthRateLimitInterval](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 20 éléments.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle. Utilisez cette [ListGateways](#) opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetGateway

Service : AWS Backup gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la passerelle.

Syntaxe de la requête

```
{
  "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "Gateway": {
    "GatewayArn": "string",
    "GatewayDisplayName": "string",
    "GatewayType": "string",
    "HypervisorId": "string",
    "LastSeenTime": number,
    "MaintenanceStartTime": {
      "DayOfMonth": number,
```

```
    "DayOfWeek": number,
    "HourOfDay": number,
    "MinuteOfHour": number
  },
  "NextUpdateAvailabilityTime": number,
  "VpcEndpoint": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la passerelle.

Type : objet [GatewayDetails](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetHypervisor

Service : AWS Backup gateway

Cette action demande des informations sur l'hyperviseur spécifié auquel la passerelle va se connecter. Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Syntaxe de la requête

```
{  
  "HypervisorArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{3}`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Hypervisor": {  
    "Host": "string",  
    "HypervisorArn": "string",  
    "KmsKeyArn": "string",  
    "LastSuccessfulMetadataSyncTime": number,  
  }
```

```
"LatestMetadataSyncStatus": "string",  
"LatestMetadataSyncStatusMessage": "string",  
"LogGroupArn": "string",  
"Name": "string",  
"State": "string"  
}  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Hypervisor](#)

Détails sur l'hyperviseur demandé.

Type : objet [HypervisorDetails](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetHypervisorPropertyMappings

Service : AWS Backup gateway

Cette action récupère les mappages de propriétés pour l'hyperviseur spécifié. Un mappage de propriétés d'hyperviseur affiche la relation entre les propriétés d'entité disponibles dans l'hyperviseur et les propriétés disponibles dans AWS.

Syntaxe de la requête

```
{
  "HypervisorArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "HypervisorArn": "string",
  "IamRoleArn": "string",
  "VmwareToAwsTagMappings": [
    {
      "AwsTagKey": "string",
```

```
    "AwsTagValue": "string",  
    "VmwareCategory": "string",  
    "VmwareTagName": "string"  
  }  
]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

[IamRoleArn](#)

L'Amazon Resource Name (ARN) du rôle IAM.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:(aws|aws-cn|aws-us-gov):iam:([0-9]+):role/(\S+)`

[VmwareToAwsTagMappings](#)

Il s'agit d'un affichage des mappages entre les VMware balises et les AWS balises.

Type : tableau d'objets [VmwareToAwsTagMapping](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetVirtualMachine

Service : AWS Backup gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la machine virtuelle.

Syntaxe de la requête

```
{  
  "ResourceArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "VirtualMachine": {  
    "HostName": "string",  
    "HypervisorId": "string",  
    "LastBackupDate": number,  
    "Name": "string",  
    "Path": "string",  
    "ResourceArn": "string",  
    "VmwareTags": [  

```

```
{
  {
    "VmwareCategory": "string",
    "VmwareTagDescription": "string",
    "VmwareTagName": "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

VirtualMachine

Cet objet contient les attributs de base de la VirtualMachine contenus dans la sortie de GetVirtualMachine

Type : objet [VirtualMachineDetails](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ImportHypervisorConfiguration

Service : AWS Backup gateway

Se connecte à un hyperviseur en important sa configuration.

Syntaxe de la requête

```
{
  "Host": "string",
  "KmsKeyArn": "string",
  "Name": "string",
  "Password": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : .+

Obligatoire : oui

KmsKeyArn

Le AWS Key Management Service pour l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)`

Obligatoire : non

Name

Le nom de l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[a-zA-Z0-9-]*`

Obligatoire : oui

Password

Le mot de passe pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[ -~]+`

Obligatoire : non

Tags

Les balises de la configuration de l'hyperviseur à importer.

Type : tableau d'objets [Tag](#)

Obligatoire : non

Username

Le nom d'utilisateur pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [-\\.0-\\[\\]-~]*[!-\\.0-\\[\\]-~][-\\.0-\\[\\]-~]*

Obligatoire : non

Syntaxe de la réponse

```
{  
  "HypervisorArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur que vous avez dissocié.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

ErrorCode

Une description des raisons pour lesquelles vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne qui s'est produite.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListGateways

Service : AWS Backup gateway

Répertorie les passerelles de sauvegarde détenues par un Compte AWS dans un Région AWS. La liste renvoyée est classée par Amazon Resource Name (ARN) de passerelle.

Syntaxe de la requête

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[MaxResults](#)

Nombre maximum de passerelles à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer MaxResults ressources, NextToken vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : .+

Obligatoire : non

Syntaxe de la réponse

```
{
  "Gateways": [
    {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Gateways](#)

Une liste de vos passerelles.

Type : tableau d'objets [Gateway](#)

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : . +

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListHypervisors

Service : AWS Backup gateway

Répertorie vos hyperviseurs.

Syntaxe de la requête

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[MaxResults](#)

Nombre maximal d'hyperviseurs à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : .+

Obligatoire : non

Syntaxe de la réponse

```
{
  "Hypervisors": [
    {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "Name": "string",
      "State": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[Hypervisors](#)

Une liste de vos Hypervisor objets, classés par leur nom de ressource Amazon (ARNs).

Type : tableau d'objets [Hypervisor](#)

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : . +

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne qui s'est produite.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)

- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListTagsForResource

Service : AWS Backup gateway

Répertorie les balises appliquées à la ressource identifiée par son Amazon Resource Name (ARN).

Syntaxe de la requête

```
{
  "ResourceArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

ResourceArn

Amazon Resource Name (ARN) des balises de la ressource à répertorier.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ResourceArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ResourceArn](#)

Amazon Resource Name (ARN) des balises de la ressource que vous avez répertoriée.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

[Tags](#)

Liste des balises de la ressource.

Type : tableau d'objets [Tag](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListVirtualMachines

Service : AWS Backup gateway

Répertorie vos machines virtuelles.

Syntaxe de la requête

```
{  
  "HypervisorArn": "string",  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur connecté à votre machine virtuelle.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : non

[MaxResults](#)

Le nombre maximal de machines virtuelles à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : .+

Obligatoire : non

Syntaxe de la réponse

```
{
  "NextToken": "string",
  "VirtualMachines": [
    {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : . +

VirtualMachines

Une liste de vos VirtualMachine objets, classés par leur nom de ressource Amazon (ARNs).

Type : tableau d'objets [VirtualMachine](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutBandwidthRateLimitSchedule

Service : AWS Backup gateway

Cette action définit la planification de limite de débit de la bande passante pour une passerelle spécifiée. Par défaut, les passerelles n'ont pas de planification de limite de débit de la bande passante, ce qui signifie qu'aucune limitation de débit de bande passante n'est en vigueur. Utilisez-le pour lancer la planification de limite de débit de la bande passante d'une passerelle.

Syntaxe de la requête

```
{
  "BandwidthRateLimitIntervals": [
    {
      "AverageUploadRateLimitInBitsPerSec": number,
      "DaysOfWeek": [ number ],
      "EndHourOfDay": number,
      "EndMinuteOfHour": number,
      "StartHourOfDay": number,
      "StartMinuteOfHour": number
    }
  ],
  "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[BandwidthRateLimitIntervals](#)

Un tableau contenant les intervalles de planification de limite de débit de la bande passante pour une passerelle. Lorsqu'aucun intervalle de limite de débit de bande passante n'a été planifié, le tableau est vide.

Type : tableau d'objets [BandwidthRateLimitInterval](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 20 éléments.

Obligatoire : oui

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette [ListGateways](#) opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette [ListGateways](#) opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutHypervisorPropertyMappings

Service : AWS Backup gateway

Cette action définit les mappages de propriétés pour l'hyperviseur spécifié. Un mappage de propriétés d'hyperviseur affiche la relation entre les propriétés d'entité disponibles dans l'hyperviseur et les propriétés disponibles dans AWS.

Syntaxe de la requête

```
{
  "HypervisorArn": "string",
  "IamRoleArn": "string",
  "VmwareToAwsTagMappings": [
    {
      "AwsTagKey": "string",
      "AwsTagValue": "string",
      "VmwareCategory": "string",
      "VmwareTagName": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

[IamRoleArn](#)

L'Amazon Resource Name (ARN) du rôle IAM.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)`

Obligatoire : oui

[VmwareToAwsTagMappings](#)

Cette action demande le mappage des VMware balises aux AWS balises.

Type : tableau d'objets [VmwareToAwsTagMapping](#)

Obligatoire : oui

Syntaxe de la réponse

```
{
  "HypervisorArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3}\/[a-zA-Z-0-9]+)`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

ErrorCode

Une description des raisons pour lesquelles vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

PutMaintenanceStartTime

Service : AWS Backup gateway

Définissez l'heure de début de la maintenance pour une passerelle.

Syntaxe de la requête

```
{
  "DayOfMonth": number,
  "DayOfWeek": number,
  "GatewayArn": "string",
  "HourOfDay": number,
  "MinuteOfHour": number
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[DayOfMonth](#)

Le jour du mois auquel commencer la maintenance d'une passerelle.

La plage des valeurs valides s'étend de Sunday à Saturday.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 31.

Obligatoire : non

[DayOfWeek](#)

Le jour de la semaine auquel commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : non

GatewayArn

Amazon Resource Name (ARN) de la passerelle, utilisé pour spécifier l'heure de début de la maintenance.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatoire : oui

HourOfDay

L'heure de la journée à laquelle commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

MinuteOfHour

La minute de l'heure à laquelle commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) d'une passerelle pour laquelle vous définissez l'heure de début de la maintenance.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartVirtualMachinesMetadataSync

Service : AWS Backup gateway

Cette action envoie une demande de synchronisation des métadonnées entre les machines virtuelles spécifiées.

Syntaxe de la requête

```
{  
  "HypervisorArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "HypervisorArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

ErrorCode

Une description des raisons pour lesquelles vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

TagResource

Service : AWS Backup gateway

Balise la ressource.

Syntaxe de la requête

```
{
  "ResourceARN": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[ResourceARN](#)

Amazon Resource Name (ARN) de la ressource à baliser.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatoire : oui

[Tags](#)

Liste des balises à attribuer à la ressource.

Type : tableau d'objets [Tag](#)

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ResourceARN": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ResourceARN](#)

Amazon Resource Name (ARN) de la ressource que vous avez balisée.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9+]){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)

- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

TestHypervisorConfiguration

Service : AWS Backup gateway

Teste la configuration de votre hyperviseur pour vérifier que la passerelle de sauvegarde peut se connecter à l'hyperviseur et à ses ressources.

Syntaxe de la requête

```
{
  "GatewayArn": "string",
  "Host": "string",
  "Password": "string",
  "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle de l'hyperviseur à tester.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

[Host](#)

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : .+

Obligatoire : oui

Password

Le mot de passe pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [-~]+

Obligatoire : non

Username

Le nom d'utilisateur pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [-\.0-\[\]-~]*[!-\.0-\[\]-~] [-\.0-\[\]-~]*

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UntagResource

Service : AWS Backup gateway

Supprime des balises de la ressource.

Syntaxe de la requête

```
{
  "ResourceARN": "string",
  "TagKeys": [ "string" ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[ResourceARN](#)

Amazon Resource Name (ARN) de la ressource pour laquelle supprimer des balises.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

[TagKeys](#)

La liste des clés de balise spécifiant les balises à supprimer.

Type : tableau de chaînes

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `([\p{L}\p{Z}\p{N}_.: /+=\ -@]*)`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ResourceARN": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceARN

Amazon Resource Name (ARN) de la ressource pour laquelle vous avez supprimé des balises.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateGatewayInformation

Service : AWS Backup gateway

Met à jour le nom d'une passerelle. Spécifiez la passerelle à mettre à jour en utilisant l'Amazon Resource Name (ARN) de la passerelle dans votre demande.

Syntaxe de la requête

```
{  
  "GatewayArn": "string",  
  "GatewayDisplayName": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle à mettre à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9+){3}\/[a-zA-Z0-9]+`

Obligatoire : oui

[GatewayDisplayName](#)

Le nom d'affichage mis à jour de la passerelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[a-zA-Z0-9-]*`

Obligatoire : non

Syntaxe de la réponse

```
{  
  "GatewayArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle que vous avez mis à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{3}`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)

- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateGatewaySoftwareNow

Service : AWS Backup gateway

Met à jour le logiciel d'une machine virtuelle (VM) de passerelle. La demande déclenche immédiatement la mise à jour logicielle.

Note

Lorsque vous effectuez cette demande, vous obtenez immédiatement une réponse 200 OK positive. La mise à jour peut toutefois prendre un certain temps.

Syntaxe de la requête

```
{  
  "GatewayArn": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle à mettre à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : oui

Syntaxe de la réponse

```
{
```

```
"GatewayArn": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[GatewayArn](#)

Amazon Resource Name (ARN) de la passerelle que vous avez mis à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne survenue.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource introuvable.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UpdateHypervisor

Service : AWS Backup gateway

Met à jour les métadonnées d'un hyperviseur, notamment son hôte, son nom d'utilisateur et son mot de passe. Spécifiez l'hyperviseur à mettre à jour en utilisant l'Amazon Resource Name (ARN) de l'hyperviseur dans votre demande.

Syntaxe de la requête

```
{
  "Host": "string",
  "HypervisorArn": "string",
  "LogGroupArn": "string",
  "Name": "string",
  "Password": "string",
  "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

Cette demande accepte les données suivantes au format JSON.

[Host](#)

L'hôte mis à jour de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : . +

Obligatoire : non

[HypervisorArn](#)

Amazon Resource Name (ARN) de l'hyperviseur à mettre à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9+]{3}\/[a-zA-Z0-9]+)`

Obligatoire : oui

LogGroupArn

Amazon Resource Name (ARN) du groupe de passerelles dans le journal demandé.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : `$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_-\./\+:\*]`

Obligatoire : non

Name

Le nom mis à jour pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[a-zA-Z0-9-]*`

Obligatoire : non

Password

Le mot de passe mis à jour pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[-~]+`

Obligatoire : non

Username

Le nom d'utilisateur mis à jour pour l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [-\.0-\[\]-~]*[!-\\.0-\[\]-~][-\.0-\[\]-~]*

Obligatoire : non

Syntaxe de la réponse

```
{  
  "HypervisorArn": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur que vous avez mis à jour.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9+){3}\/[a-zA-Z-0-9+)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

ErrorCode

Une description des raisons pour lesquelles vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

ErrorCode

Description de la raison pour laquelle l'opération n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerErrorException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

ErrorCode

Description de l'erreur interne qui s'est produite.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

ErrorCode

Description de la ressource qui n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

ErrorCode

Erreur : le TPS a été limité afin de se protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

ErrorCode

Description de l'origine de l'erreur de validation.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

AWS Backup

Les actions suivantes sont prises en charge par AWS Backup :

- [GetSearchJob](#)
- [GetSearchResultExportJob](#)
- [ListSearchJobBackups](#)
- [ListSearchJobResults](#)
- [ListSearchJobs](#)
- [ListSearchResultExportJobs](#)
- [ListTagsForResource](#)
- [StartSearchJob](#)

- [StartSearchResultExportJob](#)
- [StopSearchJob](#)
- [TagResource](#)
- [UntagResource](#)

GetSearchJob

Service : AWS Backup

Cette opération permet de récupérer les métadonnées d'une tâche de recherche, y compris sa progression.

Syntaxe de la demande

```
GET /search-jobs/SearchJobIdentifier HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

SearchJobIdentifier

Chaîne unique obligatoire qui spécifie la tâche de recherche.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "CurrentSearchProgress": {
    "ItemsMatchedCount": number,
    "ItemsScannedCount": number,
    "RecoveryPointsScannedCount": number
  },
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
```

```

        "Operator": "string",
        "Value": number
    }
],
"FilePaths": [
    {
        "Operator": "string",
        "Value": "string"
    }
],
"LastModificationTimes": [
    {
        "Operator": "string",
        "Value": number
    }
],
"Sizes": [
    {
        "Operator": "string",
        "Value": number
    }
]
}
],
"S3ItemFilters": [
    {
        "CreationTimes": [
            {
                "Operator": "string",
                "Value": number
            }
        ],
        "ETags": [
            {
                "Operator": "string",
                "Value": "string"
            }
        ],
        "ObjectKeys": [
            {
                "Operator": "string",
                "Value": "string"
            }
        ]
    }
],

```

```

    "Sizes": [
      {
        "Operator": "string",
        "Value": number
      }
    ],
    "VersionIds": [
      {
        "Operator": "string",
        "Value": "string"
      }
    ]
  }
],
"Name": "string",
"SearchJobArn": "string",
"SearchJobIdentifier": "string",
"SearchScope": {
  "BackupResourceArns": [ "string" ],
  "BackupResourceCreationTime": {
    "CreatedAfter": number,
    "CreatedBefore": number
  },
  "BackupResourceTags": {
    "string" : "string"
  },
  "BackupResourceTypes": [ "string" ],
  "SourceResourceArns": [ "string" ]
},
"SearchScopeSummary": {
  "TotalItemsToScanCount": number,
  "TotalRecoveryPointsToScanCount": number
},
"Status": "string",
"StatusMessage": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CompletionTime

Date et heure de fin d'une tâche de recherche, au format Unix et en temps universel coordonné (UTC). La valeur de `CompletionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreationTime

Date et heure de création d'une tâche de recherche, au format Unix et en temps universel coordonné (UTC). La valeur de `CompletionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CurrentSearchProgress

Renvoie des nombres représentant `BackupsScannedCount` `ItemsScanned`, et `ItemsMatched`.

Type : objet [CurrentSearchProgress](#)

EncryptionKeyArn

La clé de chiffrement pour la tâche de recherche spécifiée.

Exemple : `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : String

ItemFilters

Les filtres d'éléments représentent toutes les propriétés des éléments d'entrée spécifiées lors de la création de la recherche.

Type : objet [ItemFilters](#)

Name

Nom renvoyé de la tâche de recherche spécifiée.

Type : String

SearchJobArn

Chaîne unique qui identifie le nom de ressource Amazon (ARN) de la tâche de recherche spécifiée.

Type : String

[SearchJobIdentifier](#)

Chaîne unique qui identifie la tâche de recherche spécifiée.

Type : String

[SearchScope](#)

L'étendue de la recherche comprend toutes les propriétés de sauvegarde saisies dans une recherche.

Type : objet [SearchScope](#)

[SearchScopeSummary](#)

Résumé renvoyé de l'étendue de la tâche de recherche spécifiée, y compris :

- TotalBackupsToScanCount, le nombre de points de récupération renvoyés par la recherche.
- TotalItemsToScanCount, le nombre d'éléments renvoyés par la recherche.

Type : objet [SearchScopeSummary](#)

[Status](#)

État actuel de la tâche de recherche spécifiée.

Une tâche de recherche peut avoir l'un des statuts suivants : RUNNING ; COMPLETED ; STOPPED ; FAILED TIMED_OUT ; ou EXPIRED.

Type : String

Valeurs valides : RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[StatusMessage](#)

Un message d'état sera renvoyé pour une tâche de recherche avec un statut de ERRORRED ou pour un statut de COMPLETED tâches présentant des problèmes.

Par exemple, un message peut indiquer qu'une recherche contient des points de récupération qui ne peuvent pas être analysés en raison d'un problème d'autorisation.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)

- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

GetSearchResultExportJob

Service : AWS Backup

Cette opération permet de récupérer les métadonnées d'une tâche d'exportation.

Une tâche d'exportation est une opération qui transmet les résultats d'une tâche de recherche à un compartiment S3 spécifié dans un fichier .csv.

Une tâche d'exportation vous permet de conserver les résultats d'une recherche au-delà des 7 jours prévus pour la tâche de recherche.

Syntaxe de la demande

```
GET /export-search-jobs/ExportJobIdentifier HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ExportJobIdentifier

Il s'agit de la chaîne unique qui identifie une tâche d'exportation spécifique.

Nécessaire pour cette opération.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CompletionTime": number,
  "CreationTime": number,
  "ExportJobArn": "string",
  "ExportJobIdentifier": "string",
  "ExportSpecification": { ... },
```

```
"SearchJobArn": "string",  
"Status": "string",  
"StatusMessage": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CompletionTime

Date et heure de fin d'une tâche d'exportation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreationTime

Date et heure de création d'une tâche d'exportation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ExportJobArn

Nom de ressource Amazon (ARN) unique qui identifie de manière unique la tâche d'exportation.

Type : String

ExportJobIdentifier

Il s'agit de la chaîne unique qui identifie la tâche d'exportation spécifiée.

Type : String

ExportSpecification

La spécification d'exportation comprend le compartiment S3 de destination vers lequel les résultats de recherche ont été exportés, ainsi que le préfixe de destination.

Type : objet [ExportSpecification](#)

Remarque : Cet objet est une union. Un seul membre de cet objet peut être spécifié ou renvoyé.

[SearchJobArn](#)

Chaîne unique qui identifie le nom de ressource Amazon (ARN) de la tâche de recherche spécifiée.

Type : String

[Status](#)

Il s'agit de l'état actuel de la tâche d'exportation.

Type : String

Valeurs valides : RUNNING | FAILED | COMPLETED

[StatusMessage](#)

Un message d'état est une chaîne renvoyée pour une tâche de recherche avec un statut égal à FAILED, ainsi que les étapes à suivre pour y remédier et recommencer l'opération.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerErrorException

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

`retryAfterSeconds`

Réessayez l'appel après quelques secondes.

Code d'état HTTP : 500

`ResourceNotFoundException`

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

`message`

La requête fait référence à une ressource qui n'existe pas.

`resourceId`

Identifiant hypothétique de la ressource affectée.

`resourceType`

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

`ThrottlingException`

La demande a été refusée suite à une limitation des demandes.

`message`

La demande a échoué en raison d'une limitation des demandes.

`quotaCode`

Il s'agit du code propre au service d'origine avec le quota.

`retryAfterSeconds`

Réessayez l'appel après quelques secondes.

`serviceCode`

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListSearchJobBackups

Service : AWS Backup

Cette opération renvoie une liste de toutes les sauvegardes (points de restauration) dans un format paginé qui ont été incluses dans la tâche de recherche.

Si aucune sauvegarde attendue n'apparaît dans les résultats d'une recherche, vous pouvez effectuer cette opération pour afficher chaque sauvegarde incluse dans la recherche. Toutes les sauvegardes qui n'ont pas été incluses parce qu'elles ont un FAILED statut dû à un problème d'autorisation seront affichées, accompagnées d'un message d'état.

Seuls les points de restauration dotés d'un index de sauvegarde dont le statut est égal à ACTIVE seront inclus dans les résultats de recherche. Si l'index possède un autre statut, son statut sera affiché avec un message d'état.

Syntaxe de la demande

```
GET /search-jobs/SearchJobIdentifier/backups?maxResults=MaxResults&nextToken=NextToken  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant une liste partielle des sauvegardes renvoyées incluses dans une tâche de recherche.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[SearchJobIdentifier](#)

Chaîne unique qui spécifie la tâche de recherche.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Results": [
    {
      "BackupCreationTime": number,
      "BackupResourceArn": "string",
      "IndexCreationTime": number,
      "ResourceType": "string",
      "SourceResourceArn": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant une liste partielle des sauvegardes renvoyées incluses dans une tâche de recherche.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Results

Les points de récupération ont renvoyé les résultats d'une tâche de recherche

Type : tableau d'objets [SearchJobBackupsResult](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListSearchJobResults

Service : AWS Backup

Cette opération renvoie la liste d'une tâche de recherche spécifiée.

Syntaxe de la demande

```
GET /search-jobs/SearchJobIdentifier/search-results?  
maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant une liste partielle des résultats de recherche renvoyés.

Par exemple, si une demande est faite pour renvoyer un `MaxResults` nombre de résultats de recherche, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[SearchJobIdentifier](#)

Chaîne unique qui spécifie la tâche de recherche.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "Results": [
    { ... }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant une liste partielle des résultats de recherche d'emploi.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[Results](#)

Les résultats sont soit `EBSResultItem`, soit `S3ResultItem`.

Type : tableau d'objets [ResultItem](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.
message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.
message

Erreur inattendue lors du traitement de la demande.
retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.
resourceId

Identifiant hypothétique de la ressource affectée.
resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.
message

La demande a échoué en raison d'une limitation des demandes.
quotaCode

Il s'agit du code propre au service d'origine avec le quota.
retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListSearchJobs

Service : AWS Backup

Cette opération renvoie une liste des tâches de recherche associées à un compte.

Syntaxe de la demande

```
GET /search-jobs?MaxResults=MaxResults&NextToken=NextToken&Status=ByStatus HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[ByStatus](#)

Incluez ce paramètre pour filtrer la liste en fonction du statut de la tâche de recherche.

Valeurs valides : RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant une liste partielle des tâches de recherche renvoyées.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200  
Content-type: application/json
```

```
{
  "NextToken": "string",
  "SearchJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "Name": "string",
      "SearchJobArn": "string",
      "SearchJobIdentifier": "string",
      "SearchScopeSummary": {
        "TotalItemsToScanCount": number,
        "TotalRecoveryPointsToScanCount": number
      },
      "Status": "string",
      "StatusMessage": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[NextToken](#)

L'élément suivant une liste partielle des sauvegardes renvoyées incluses dans une tâche de recherche.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

[SearchJobs](#)

Les tâches de recherche figurant dans la liste, avec les détails des tâches de recherche renvoyées.

Type : tableau d'objets [SearchJobSummary](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande a échoué en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListSearchResultExportJobs

Service : AWS Backup

Cette opération exporte les résultats de recherche d'une tâche de recherche vers un compartiment S3 de destination spécifié.

Syntaxe de la demande

```
GET /export-search-jobs?  
MaxResults=MaxResults&NextToken=NextToken&SearchJobIdentifier=SearchJobIdentifier&Status=Status  
HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

[MaxResults](#)

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

[NextToken](#)

L'élément suivant une liste partielle des sauvegardes renvoyées incluses dans une tâche de recherche.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

[SearchJobIdentifier](#)

Chaîne unique qui spécifie la tâche de recherche.

[Status](#)

Les tâches de recherche à inclure dans la tâche d'exportation peuvent être filtrées en incluant ce paramètre.

Valeurs valides : `RUNNING` | `FAILED` | `COMPLETED`

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "ExportJobs": [
    {
      "CompletionTime": number,
      "CreationTime": number,
      "ExportJobArn": "string",
      "ExportJobIdentifier": "string",
      "SearchJobArn": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ExportJobs](#)

L'opération renvoie les tâches d'exportation incluses.

Type : tableau d'objets [ExportJobSummary](#)

[NextToken](#)

L'élément suivant une liste partielle des sauvegardes renvoyées incluses dans une tâche de recherche.

Par exemple, si une demande est faite pour renvoyer le `MaxResults` nombre de sauvegardes, cela vous `NextToken` permet de renvoyer plus d'éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerErrorException

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ServiceQuotaExceededException

La demande a été refusée en raison du dépassement des limites de quotas autorisées.
message

Cette demande n'a pas abouti en raison d'un quota de service dépassant les limites.

quotaCode

Il s'agit du code spécifique au type de quota.

resourceId

Identifiant de la ressource.

resourceType

Type de ressource.

serviceCode

Il s'agit du code propre au service d'origine avec le quota.

Code d'état HTTP : 402

ThrottlingException

La demande a été refusée suite à une limitation des demandes.
message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ListTagsForResource

Service : AWS Backup

Cette opération renvoie les balises d'un type de ressource.

Syntaxe de la demande

```
GET /tags/ResourceArn HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique la ressource. >

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Tags

Liste des balises renvoyées par l'opération.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel après quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande a échoué en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel après quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)

- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartSearchJob

Service : AWS Backup

Cette opération crée une tâche de recherche qui renvoie les points de récupération filtrés par SearchScope et les éléments filtrés par ItemFilters.

Vous pouvez éventuellement inclure ClientToken EncryptionKeyArn, Nom, and/or Tags.

Syntaxe de la demande

```
PUT /search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "EncryptionKeyArn": "string",
  "ItemFilters": {
    "EBSItemFilters": [
      {
        "CreationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "FilePaths": [
          {
            "Operator": "string",
            "Value": "string"
          }
        ],
        "LastModificationTimes": [
          {
            "Operator": "string",
            "Value": number
          }
        ],
        "Sizes": [
          {
            "Operator": "string",
            "Value": number
          }
        ]
      }
    ]
  }
}
```



```

    }
  ],
  "S3ItemFilters": [
    {
      "CreationTimes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "ETags": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "ObjectKeys": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ],
      "Sizes": [
        {
          "Operator": "string",
          "Value": number
        }
      ],
      "VersionIds": [
        {
          "Operator": "string",
          "Value": "string"
        }
      ]
    }
  ]
},
"Name": "string",
"SearchScope": {
  "BackupResourceArns": [ "string" ],
  "BackupResourceCreationTime": {
    "CreatedAfter": number,
    "CreatedBefore": number
  }
},

```

```
"BackupResourceTags": {
  "string" : "string"
},
"BackupResourceTypes": [ "string" ],
"SourceResourceArns": [ "string" ]
},
"Tags": {
  "string" : "string"
}
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

[ClientToken](#)

Incluez ce paramètre pour autoriser plusieurs appels identiques pour l'idempuissance.

Un jeton client est valide pendant 8 heures après la fin de la première demande l'utilisant. Passé ce délai, toute demande comportant le même jeton est traitée comme une nouvelle demande.

Type : chaîne

Obligatoire : non

[EncryptionKeyArn](#)

La clé de chiffrement pour la tâche de recherche spécifiée.

Type : chaîne

Obligatoire : non

[ItemFilters](#)

Les filtres d'éléments représentent toutes les propriétés des éléments d'entrée spécifiées lors de la création de la recherche.

Contient soit des EBSItem filtres, soit du S3 ItemFilters

Type : objet [ItemFilters](#)

Obligatoire : non

Name

Incluez des caractères alphanumériques pour créer un nom pour cette tâche de recherche.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 500.

Obligatoire : non

SearchScope

Cet objet peut contenir BackupResourceTypes,, BackupResourceArns BackupResourceCreationTime BackupResourceTags, et SourceResourceArns pour filtrer les points de récupération renvoyés par la tâche de recherche.

Type : objet [SearchScope](#)

Obligatoire : oui

Tags

Liste des balises renvoyées par l'opération.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
  "CreationTime": number,
  "SearchJobArn": "string",
  "SearchJobIdentifier": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'une tâche, au format Unix et en temps universel coordonné (UTC). La valeur de `CompletionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

SearchJobArn

Chaîne unique qui identifie le nom de ressource Amazon (ARN) de la tâche de recherche spécifiée.

Type : String

SearchJobIdentifier

Chaîne unique qui spécifie la tâche de recherche.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

ConflictException

Cette exception se produit lorsqu'un conflit avec une opération précédente réussie est détecté. Cela se produit généralement lorsque l'opération précédente n'a pas eu le temps de se propager à l'hôte qui répond à la demande en cours.

Une nouvelle tentative (avec une logique d'interruption appropriée) est la réponse recommandée à cette exception.

message

La mise à jour ou la suppression d'une ressource peut entraîner un état incohérent.

resourceId

Identifiant de la ressource affectée.

resourceType

Type de ressource affectée.

Code d'état HTTP : 409

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel après quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ServiceQuotaExceededException

La demande a été refusée en raison du dépassement des limites de quotas autorisées.

message

Cette demande n'a pas abouti en raison d'un quota de service dépassant les limites.

quotaCode

Il s'agit du code spécifique au type de quota.

resourceId

Identifiant de la ressource.

resourceType

Type de ressource.

serviceCode

Il s'agit du code propre au service d'origine avec le quota.

Code d'état HTTP : 402

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande a échoué en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel après quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StartSearchResultExportJob

Service : AWS Backup

Cette opération lance une tâche pour exporter les résultats de la tâche de recherche vers un compartiment S3 désigné.

Syntaxe de la demande

```
PUT /export-search-jobs HTTP/1.1
Content-type: application/json

{
  "ClientToken": "string",
  "ExportSpecification": { ... },
  "RoleArn": "string",
  "SearchJobIdentifier": "string",
  "Tags": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ClientToken

Incluez ce paramètre pour autoriser plusieurs appels identiques à des fins d'idempotence.

Un jeton client est valide pendant 8 heures après la fin de la première demande l'utilisant. Passé ce délai, toute demande comportant le même jeton est traitée comme une nouvelle demande.

Type : chaîne

Obligatoire : non

ExportSpecification

Cette spécification contient une chaîne obligatoire du compartiment de destination ; vous pouvez éventuellement inclure le préfixe de destination.

Type : objet [ExportSpecification](#)

Remarque : Cet objet est une union. Un seul membre de cet objet peut être spécifié ou renvoyé.

Obligatoire : oui

[RoleArn](#)

Ce paramètre spécifie le rôle ARN utilisé pour démarrer les tâches d'exportation des résultats de recherche.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:(?:aws|aws-cn|aws-us-gov):iam::[a-z0-9-]+:role/(.+)`

Obligatoire : non

[SearchJobIdentifier](#)

Chaîne unique qui spécifie la tâche de recherche.

Type : String

Obligatoire : oui

[Tags](#)

Balises facultatives à inclure. Une balise est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : /.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
```

```
"ExportJobArn": "string",  
"ExportJobIdentifier": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

[ExportJobArn](#)

Il s'agit de l'ARN (Amazon Resource Name) unique qui appartient à la nouvelle tâche d'exportation.

Type : String

[ExportJobIdentifier](#)

Il s'agit de l'identifiant unique qui spécifie la nouvelle tâche d'exportation.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

ConflictException

Cette exception se produit lorsqu'un conflit avec une opération précédente réussie est détecté.

Cela se produit généralement lorsque l'opération précédente n'a pas eu le temps de se propager à l'hôte qui répond à la demande en cours.

Une nouvelle tentative (avec une logique d'interruption appropriée) est la réponse recommandée à cette exception.

message

La mise à jour ou la suppression d'une ressource peut entraîner un état incohérent.

resourceId

Identifiant de la ressource affectée.

resourceType

Type de ressource affectée.

Code d'état HTTP : 409

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ServiceQuotaExceededException

La demande a été refusée en raison du dépassement des limites de quotas autorisées.

message

Cette demande n'a pas abouti en raison d'un quota de service dépassant les limites.

quotaCode

Il s'agit du code spécifique au type de quota.

resourceId

Identifiant de la ressource.

resourceType

Type de ressource.

serviceCode

Il s'agit du code propre au service d'origine avec le quota.

Code d'état HTTP : 402

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

StopSearchJob

Service : AWS Backup

Cette opération met fin à une tâche de recherche.

Seule une tâche de recherche dont le statut est égal à RUNNING peut être arrêtée.

Syntaxe de la demande

```
PUT /search-jobs/SearchJobIdentifier/actions/cancel HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

SearchJobIdentifier

Chaîne unique qui spécifie la tâche de recherche.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

ConflictException

Cette exception se produit lorsqu'un conflit avec une opération précédente réussie est détecté. Cela se produit généralement lorsque l'opération précédente n'a pas eu le temps de se propager à l'hôte qui répond à la demande en cours.

Une nouvelle tentative (avec une logique d'interruption appropriée) est la réponse recommandée à cette exception.

message

La mise à jour ou la suppression d'une ressource peut entraîner un état incohérent.

resourceId

Identifiant de la ressource affectée.

resourceType

Type de ressource affectée.

Code d'état HTTP : 409

InternalServerErrorException

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

TagResource

Service : AWS Backup

Cette opération place des balises sur la ressource que vous indiquez.

Syntaxe de la demande

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json

{
  "Tags": {
    "string" : "string"
  }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique la ressource.

Il s'agit de la ressource qui aura les balises indiquées.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Tags

Balises obligatoires à inclure. Une balise est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : /.

Type : mappage chaîne/chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerErrorException

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)

- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

UntagResource

Service : AWS Backup

Cette opération supprime les balises de la ressource spécifiée.

Syntaxe de la demande

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique la ressource pour laquelle vous souhaitez supprimer des balises.

Obligatoire : oui

TagKeys

Ce paramètre obligatoire contient les clés de balise que vous souhaitez supprimer de la source.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

message

L'utilisateur ne dispose pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 403

InternalServerError

Une erreur interne du serveur s'est produite. Réessayez votre demande.

message

Erreur inattendue lors du traitement de la demande.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

Code d'état HTTP : 500

ResourceNotFoundException

La ressource n'a pas été trouvée pour cette demande.

Vérifiez que les informations sur la ressource, telles que l'ARN ou le type, sont correctes et existent, puis réessayez la demande.

message

La requête fait référence à une ressource qui n'existe pas.

resourceId

Identifiant hypothétique de la ressource affectée.

resourceType

Type hypothétique de la ressource affectée.

Code d'état HTTP : 404

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

message

La demande n'a pas abouti en raison d'une limitation des demandes.

quotaCode

Il s'agit du code propre au service d'origine avec le quota.

retryAfterSeconds

Réessayez l'appel au bout de quelques secondes.

serviceCode

Il s'agit du code propre au service d'origine.

Code d'état HTTP : 429

ValidationException

L'entrée ne satisfait pas les contraintes spécifiées par un service.

message

L'entrée ne répond pas aux contraintes spécifiées par un service Amazon.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS Interface de ligne de commande V2](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)
- [AWS SDK pour Go v2](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour V3 JavaScript](#)
- [AWS SDK pour Kotlin](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)

- [AWS SDK pour Ruby V3](#)

Types de données

Les types de données suivants sont pris en charge par AWS Backup :

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)
- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)
- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)
- [Framework](#)
- [FrameworkControl](#)

- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)
- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)
- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)
- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)

- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)
- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)
- [TieringConfigurationsListMember](#)

Les types de données suivants sont pris en charge par AWS Backup gateway :

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)
- [VmwareToAwsTagMapping](#)

Les types de données suivants sont pris en charge par AWS Backup :

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)
- [SearchScopeSummary](#)
- [StringCondition](#)
- [TimeCondition](#)

AWS Backup

Les types de données suivants sont pris en charge par AWS Backup :

- [AdvancedBackupSetting](#)
- [AggregatedScanResult](#)
- [BackupJob](#)
- [BackupJobSummary](#)
- [BackupPlan](#)
- [BackupPlanInput](#)
- [BackupPlansListMember](#)
- [BackupPlanTemplatesListMember](#)
- [BackupRule](#)

- [BackupRuleInput](#)
- [BackupSelection](#)
- [BackupSelectionsListMember](#)
- [BackupVaultListMember](#)
- [CalculatedLifecycle](#)
- [Condition](#)
- [ConditionParameter](#)
- [Conditions](#)
- [ControlInputParameter](#)
- [ControlScope](#)
- [CopyAction](#)
- [CopyJob](#)
- [CopyJobSummary](#)
- [DateRange](#)
- [Framework](#)
- [FrameworkControl](#)
- [IndexAction](#)
- [IndexedRecoveryPoint](#)
- [KeyValue](#)
- [LatestMpaApprovalTeamUpdate](#)
- [LatestRevokeRequest](#)
- [LegalHold](#)
- [Lifecycle](#)
- [ProtectedResource](#)
- [ProtectedResourceConditions](#)
- [RecoveryPointByBackupVault](#)
- [RecoveryPointByResource](#)
- [RecoveryPointCreator](#)
- [RecoveryPointMember](#)
- [RecoveryPointSelection](#)

- [ReportDeliveryChannel](#)
- [ReportDestination](#)
- [ReportJob](#)
- [ReportPlan](#)
- [ReportSetting](#)
- [ResourceSelection](#)
- [RestoreAccessBackupVaultListMember](#)
- [RestoreJobCreator](#)
- [RestoreJobsListMember](#)
- [RestoreJobSummary](#)
- [RestoreTestingPlanForCreate](#)
- [RestoreTestingPlanForGet](#)
- [RestoreTestingPlanForList](#)
- [RestoreTestingPlanForUpdate](#)
- [RestoreTestingRecoveryPointSelection](#)
- [RestoreTestingSelectionForCreate](#)
- [RestoreTestingSelectionForGet](#)
- [RestoreTestingSelectionForList](#)
- [RestoreTestingSelectionForUpdate](#)
- [ScanAction](#)
- [ScanJob](#)
- [ScanJobCreator](#)
- [ScanJobSummary](#)
- [ScanResult](#)
- [ScanResultInfo](#)
- [ScanSetting](#)
- [ScheduledPlanExecutionMember](#)
- [TieringConfiguration](#)
- [TieringConfigurationInputForCreate](#)
- [TieringConfigurationInputForUpdate](#)

- [TieringConfigurationsListMember](#)

AdvancedBackupSetting

Service : AWS Backup

Les options de sauvegarde pour chaque type de ressource.

Table des matières

BackupOptions

Spécifie l'option de sauvegarde pour une ressource sélectionnée. Cette option est disponible pour les tâches de sauvegarde Windows VSS et les sauvegardes S3.

Valeurs valides :

Définissez sur "WindowsVSS": "enabled" pour activer l'option de sauvegarde WindowsVSS et créer une sauvegarde Windows VSS.

Définissez sur "WindowsVSS": "disabled" pour créer une sauvegarde régulière. L'option WindowsVSS n'est pas activée par défaut.

Pour les sauvegardes S3, définissez ce "S3BackupACLs": "disabled" paramètre sur pour ACLs exclure de la sauvegarde ou "S3BackupObjectTags": "disabled" pour exclure les balises d'objet de la sauvegarde. Par défaut, les balises à la fois ACLs et les balises d'objet sont incluses dans les sauvegardes S3.

Si vous spécifiez une option non valide, vous obtenez une exception `InvalidParameterValueException`.

Pour plus d'informations sur les sauvegardes Windows VSS, consultez [Création d'une sauvegarde Windows avec VSS](#).

Type : mappage chaîne/chaîne

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

ResourceType

Spécifie un objet contenant le type de ressource et les options de sauvegarde. Le seul type de ressource pris en charge est celui EC2 des instances Amazon dotées du service Windows

Volume Shadow Copy (VSS). Pour un CloudFormation exemple, consultez l'[exemple de CloudFormation modèle pour activer Windows VSS](#) dans le Guide de l' AWS Backup utilisateur.

Valeurs valides : EC2.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

AggregatedScanResult

Service : AWS Backup

Contient les résultats d'analyse agrégés issus de plusieurs opérations d'analyse, fournissant un résumé de l'état et des résultats de l'analyse.

Table des matières

FailedScan

Valeur booléenne indiquant si l'un des scans agrégés a échoué.

Type : booléen

Obligatoire : non

Findings

Un ensemble de résultats découverts dans tous les scans agrégés.

Type : tableau de chaînes

Valeurs valides : MALWARE

Obligatoire : non

LastComputed

Horodatage du dernier calcul du résultat du scan agrégé, au format Unix et en temps universel coordonné (UTC).

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de sauvegarde.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de sauvegarde.

Type : String

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : chaîne

Obligatoire : non

BackupOptions

Spécifie l'option de sauvegarde pour une ressource sélectionnée. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Valeurs valides : définissez sur `"WindowsVSS": "enabled"` pour activer l'option de sauvegarde WindowsVSS et créer une sauvegarde Windows VSS. Définissez sur `"WindowsVSS": "disabled"` pour créer une sauvegarde régulière. Si vous spécifiez une option non valide, vous obtenez une exception `InvalidParameterValueException`.

Type : mappage chaîne/chaîne

Modèle de clé : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

BackupSizeInBytes

Taille, en octets, d'une sauvegarde (point de restauration).

Cette valeur peut s'afficher différemment selon le type de ressource, car AWS Backup elle extrait des informations de données provenant d'autres AWS services. Par exemple, la valeur renvoyée peut afficher une valeur de 0, qui peut être différente de la valeur prévue.

Le comportement attendu pour les valeurs par type de ressource est décrit comme suit :

- Amazon Aurora, Amazon DocumentDB et Amazon Neptune n'ont pas cette valeur renseignée à partir de l'opération `GetBackupJobStatus`
- Pour Amazon DynamoDB doté de fonctionnalités avancées, cette valeur fait référence à la taille du point de restauration (sauvegarde).
- Amazon EC2 et Amazon EBS indiquent la taille du volume (stockage provisionné) renvoyé dans le cadre de cette valeur. Amazon EBS ne renvoie pas d'informations sur la taille de sauvegarde ; la taille de l'instantané aura la même valeur que la ressource d'origine qui a été sauvegardée.
- Pour Amazon EFS, cette valeur fait référence aux octets delta transférés lors d'une sauvegarde.
- Amazon FSx ne renseigne pas cette valeur à partir de l'opération `GetBackupJobStatus` pour les systèmes de FSx fichiers.
- Une instance Amazon RDS s'affichera sous la forme 0.
- Pour les machines virtuelles en cours d'exécution VMware, cette valeur est transmise AWS Backup via un flux de travail asynchrone, ce qui peut signifier que la valeur affichée peut sous-représenter la taille réelle de la sauvegarde.

Type : long

Obligatoire : non

BackupType

Représente le type de sauvegarde pour une tâche de sauvegarde.

Type : chaîne

Obligatoire : non

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

BytesTransferred

Taille en octets transférée vers un coffre-fort de sauvegarde au moment où le statut de la tâche a été demandé.

Type : long

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de sauvegarde, dont `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour la créer.

Type : objet [RecoveryPointCreator](#)

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

EncryptionKeyArn

Le nom de ressource Amazon (ARN) de la clé KMS utilisée pour chiffrer la sauvegarde. Il peut s'agir d'une clé gérée par le client ou d'une clé AWS gérée, selon la configuration du coffre-fort.

Type : chaîne

Obligatoire : non

ExpectedCompletionDate

Date et heure de fin attendues d'une tâche de sauvegarde des ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `ExpectedCompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible. Les rôles IAM autres que le rôle par défaut doivent inclure `AWSBackup` ou `AwsBackup` dans le nom du rôle. Par exemple, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Les noms de rôles dépourvus de ces chaînes ne sont pas autorisés à effectuer des tâches de sauvegarde.

Type : chaîne

Obligatoire : non

InitiationDate

Date à laquelle la tâche de sauvegarde a été lancée.

Type : Timestamp

Obligatoire : non

IsEncrypted

Valeur booléenne indiquant si la sauvegarde est cryptée. Toutes les sauvegardes AWS Backup sont cryptées, mais ce champ indique l'état du chiffrement pour des raisons de transparence.

Type : booléen

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'une tâche de sauvegarde parent (composite).

Type : booléen

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure AccessDenied, SUCCESS, AGGREGATE_ALL et INVALIDPARAMETERS. Voir [Surveillance](#) pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

ParentJobId

Cela identifie de manière unique une demande vers AWS Backup pour sauvegarder une ressource. Le retour sera l'ID de tâche parent (composite).

Type : chaîne

Obligatoire : non

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

RecoveryPointLifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Type : objet [Lifecycle](#)

Obligatoire : non

ResourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

StartBy

Spécifie l'heure au format Unix et au format UTC (Coordinated Universal Time) quand une tâche de sauvegarde doit être démarrée avant d'être annulée. La valeur est calculée en ajoutant la fenêtre de démarrage à l'heure planifiée. Ainsi, si l'heure prévue était 18 h 00 et que la fenêtre de début était de 2 heures, l'heure `StartBy` serait 20 h 00 à la date spécifiée. La valeur de `StartBy` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

L'état actuel d'une tâche de sauvegarde.

Type : String

Valeurs valides : CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de sauvegarde d'une ressource.

Type : chaîne

Obligatoire : non

VaultLockState

État de verrouillage du coffre-fort de sauvegarde. Pour les coffres-forts à espacement logique, cela indique si le coffre-fort est verrouillé en mode de conformité. Les valeurs valides sont LOCKED et UNLOCKED.

Type : chaîne

Obligatoire : non

VaultType

Type de coffre-fort de sauvegarde dans lequel le point de restauration est stocké. Les valeurs valides concernent BACKUP_VAULT les coffres-forts de sauvegarde standard et les coffres-forts LOGICALLY_AIR_GAPPED_BACKUP_VAULT à espacement logique.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupJobSummary

Service : AWS Backup

Il s'agit d'un résumé des tâches créées ou en cours d'exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État RestourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L'ID de compte qui possède les tâches figurant dans le résumé.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l'heure au format numérique de l'heure de fin d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes incluent AccessDenied, Success et InvalidParameters. Voir [Surveillance](#) pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

Region

Les AWS régions dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande GetSupportedResourceTypes renvoie des chaînes pour les types de ressources pris en charge.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : String

Valeurs valides : CREATED | PENDING | RUNNING | ABORTING | ABORTED |
COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupPlan

Service : AWS Backup

Contient un nom d'affichage de plan de sauvegarde facultatif et un tableau d'objets `BackupRule`, chaque objet spécifiant une règle de sauvegarde. Dans un plan de sauvegarde, chaque règle est une tâche planifiée distincte et peut sauvegarder une sélection différente de ressources AWS .

Table des matières

BackupPlanName

Nom complet d'un plan de sauvegarde. Ne doit contenir que des caractères alphanumériques ou « - _ ». caractères spéciaux.

S'il est défini dans la console, il peut contenir de 1 à 50 caractères ; s'il est défini via une CLI ou une API, il peut contenir de 1 à 200 caractères.

Type : Chaîne

Obligatoire : oui

Rules

Tableau d'objets `BackupRule`, dont chacun spécifie une tâche planifiée qui est utilisée pour sauvegarder une sélection de ressources.

Type : tableau d'objets [BackupRule](#)

Obligatoire : oui

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour chaque type de ressource.

Type : tableau d'objets [AdvancedBackupSetting](#)

Obligatoire : non

ScanSettings

Contient votre configuration d'analyse pour le plan de sauvegarde et inclut le scanner de logiciels malveillants, les ressources que vous avez sélectionnées et le rôle d'analyseur.

Type : tableau d'objets [ScanSetting](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupPlanInput

Service : AWS Backup

Contient un nom d'affichage de plan de sauvegarde facultatif et un tableau d'objets `BackupRule`, chaque objet spécifiant une règle de sauvegarde. Dans un plan de sauvegarde, chaque règle est une tâche planifiée distincte.

Table des matières

BackupPlanName

Nom complet d'un plan de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « - _ . » caractères.

Type : Chaîne

Obligatoire : oui

Rules

Tableau d'objets `BackupRule`, dont chacun spécifie une tâche planifiée qui est utilisée pour sauvegarder une sélection de ressources.

Type : tableau d'objets [BackupRuleInput](#)

Obligatoire : oui

AdvancedBackupSettings

Spécifie une liste d'`BackupOptions` pour chaque type de ressource. Ces paramètres sont uniquement disponibles pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Type : tableau d'objets [AdvancedBackupSetting](#)

Obligatoire : non

ScanSettings

Contient votre configuration d'analyse pour la règle de sauvegarde et inclut le scanner de malwares et le mode d'analyse complet ou incrémentiel.

Type : tableau d'objets [ScanSetting](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupPlansListMember

Service : AWS Backup

Contient des métadonnées relatives à un plan de sauvegarde.

Table des matières

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour un type de ressource.

Type : tableau d'objets [AdvancedBackupSetting](#)

Obligatoire : non

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

Obligatoire : non

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

BackupPlanName

Nom complet d'un plan de sauvegarde enregistré.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'un plan de sauvegarde de ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

DeletionDate

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastExecutionDate

La dernière fois que ce plan de sauvegarde a été exécuté. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. La version IDs ne peut pas être modifiée.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupPlanTemplatesListMember

Service : AWS Backup

Objet spécifiant les métadonnées associées à un modèle de plan de sauvegarde.

Table des matières

BackupPlanTemplateId

Identifie de manière unique un modèle de plan de sauvegarde enregistré.

Type : chaîne

Obligatoire : non

BackupPlanTemplateName

Nom d'affichage facultatif d'un modèle de plan de sauvegarde.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupRule

Service : AWS Backup

Spécifie une tâche planifiée utilisée pour sauvegarder une sélection de ressources.

Table des matières

RuleName

Nom d'affichage d'une règle de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

Obligatoire : oui

TargetBackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompletionWindowMinutes

Une valeur en minutes après le démarrage réussi d'une tâche de sauvegarde et avant qu'elle doive être terminée ou qu'elle soit annulée par AWS Backup. Cette valeur est facultative.

Type : Long

Obligatoire : non

CopyActions

Tableau d'objets `CopyAction`, qui contient les détails de l'opération de copie.

Type : tableau d'objets [CopyAction](#)

Obligatoire : non

EnableContinuousBackup

Spécifie s'il AWS Backup crée des sauvegardes continues. De véritables raisons AWS Backup de créer des sauvegardes continues capables de point-in-time restauration (PITR). Faux (ou non spécifié) entraîne AWS Backup la création de sauvegardes instantanées.

Type : booléen

Obligatoire : non

IndexActions

IndexActions est un tableau que vous utilisez pour spécifier la manière dont les données de sauvegarde doivent être indexées.

Chacune BackupRule peut avoir 0 ou 1 IndexAction, car chaque sauvegarde peut être associée à un index au maximum.

Dans le tableau se trouve ResourceType. Un seul sera accepté pour chacun BackupRule.

Type : tableau d'objets [IndexAction](#)

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet [Lifecycle](#)

Obligatoire : non

RecoveryPointTags

Les balises attribuées aux ressources associées à cette règle lors de la restauration à partir d'une sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

RuleId

Identifie de manière unique une règle utilisée pour planifier la sauvegarde d'une sélection de ressources.

Type : chaîne

Obligatoire : non

ScanActions

Contient votre configuration d'analyse pour la règle de sauvegarde et inclut le scanner de malwares et le mode d'analyse complet ou incrémentiel.

Type : tableau d'objets [ScanAction](#)

Obligatoire : non

ScheduleExpression

Expression cron en UTC indiquant à quel moment une tâche de sauvegarde est AWS Backup initiée. Lorsqu'aucune expression CRON n'est fournie, AWS Backup utilise l'expression `cron(0 5 ? * * *)` par défaut.

Pour plus d'informations sur les expressions AWS cron, consultez la section [Schedule Expressions for Rules](#) dans le guide de l'utilisateur Amazon CloudWatch Events.

Deux exemples d'expressions AWS cron sont `15 * ? * * *` (effectuer une sauvegarde toutes les heures 15 minutes après l'heure) et `0 12 * * ? *` (effectuer une sauvegarde tous les jours à midi UTC).

Pour consulter un tableau d'exemples, cliquez sur le lien précédent et faites défiler la page vers le bas.

Type : chaîne

Obligatoire : non

`ScheduleExpressionTimezone`

Fuseau horaire dans lequel l'expression de planification est définie. Par défaut, `ScheduleExpressions` ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

`StartWindowMinutes`

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste `CREATED` jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à `RUNNING`) ou jusqu'à ce que le statut de la tâche passe à `EXPIRED` (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : Long

Obligatoire : non

`TargetLogicallyAirGappedBackupVaultArn`

L'ARN d'un coffre-fort à espacement logique. L'ARN doit appartenir au même compte et à la même région. Si elles sont fournies, les ressources entièrement gérées prises en charge sont sauvegardées directement dans un coffre-fort à espacement logique, tandis que les autres ressources prises en charge créent un instantané temporaire (facturable) dans le coffre-fort de sauvegarde, puis le copient dans un coffre-fort à espacement logique. Les ressources non prises en charge ne sont sauvegardées que dans le coffre de sauvegarde spécifié.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupRuleInput

Service : AWS Backup

Spécifie une tâche planifiée utilisée pour sauvegarder une sélection de ressources.

Table des matières

RuleName

Nom d'affichage d'une règle de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

Obligatoire : oui

TargetBackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompletionWindowMinutes

Une valeur en minutes après le démarrage réussi d'une tâche de sauvegarde et avant qu'elle doive être terminée ou qu'elle soit annulée par AWS Backup. Cette valeur est facultative.

Type : Long

Obligatoire : non

CopyActions

Tableau d'objets `CopyAction`, qui contient les détails de l'opération de copie.

Type : tableau d'objets [CopyAction](#)

Obligatoire : non

EnableContinuousBackup

Spécifie s'il AWS Backup crée des sauvegardes continues. De véritables raisons AWS Backup de créer des sauvegardes continues capables de point-in-time restauration (PITR). Faux (ou non spécifié) entraîne AWS Backup la création de sauvegardes instantanées.

Type : booléen

Obligatoire : non

IndexActions

Il peut y en avoir jusqu'à un IndexAction dans chacune BackupRule, car chaque sauvegarde peut être associée à 0 ou 1 index de sauvegarde.

Dans le tableau se trouve ResourceTypes. Un seul type de ressource sera accepté pour chacun BackupRule. Valeurs valides :

- EBS pour Amazon Elastic Block Store
- S3pour Amazon Simple Storage Service (Amazon S3)

Type : tableau d'objets [IndexAction](#)

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup fera automatiquement la transition et expirera les sauvegardes en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition vers le froid après plusieurs jours » ne peut pas être modifié une fois qu'une sauvegarde a été transférée vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Ce paramètre a une valeur maximale de 100 ans (36 500 jours).

Type : objet [Lifecycle](#)

Obligatoire : non

RecoveryPointTags

Les balises à attribuer aux ressources.

Type : mappage chaîne/chaîne

Obligatoire : non

ScanActions

Contient votre configuration d'analyse pour la règle de sauvegarde et inclut le scanner de malwares et le mode d'analyse complet ou incrémentiel.

Type : tableau d'objets [ScanAction](#)

Obligatoire : non

ScheduleExpression

Expression CRON en UTC indiquant à quel moment une tâche de sauvegarde est AWS Backup initiée. Lorsqu'aucune expression CRON n'est fournie, AWS Backup utilise l'expression `cron(0 5 ? * * *)` par défaut.

Type : chaîne

Obligatoire : non

ScheduleExpressionTimezone

Fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowMinutes

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste CREATED jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à RUNNING) ou jusqu'à ce que le statut de la tâche passe à EXPIRED (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : Long

Obligatoire : non

TargetLogicallyAirGappedBackupVaultArn

L'ARN d'un coffre-fort à espacement logique. L'ARN doit appartenir au même compte et à la même région. Si elles sont fournies, les ressources entièrement gérées prises en charge sont sauvegardées directement dans un coffre-fort à espacement logique, tandis que les autres ressources prises en charge créent un instantané temporaire (facturable) dans le coffre-fort de sauvegarde, puis le copient dans un coffre-fort à espacement logique. Les ressources non prises en charge ne sont sauvegardées que dans le coffre de sauvegarde spécifié.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupSelection

Service : AWS Backup

Utilisez pour spécifier un ensemble de ressources à un plan de sauvegarde.

Nous vous recommandons de spécifier les conditions, les balises ou les ressources à inclure ou à exclure. Dans le cas contraire, Backup tente de sélectionner toutes les ressources de stockage prises en charge et acceptées, ce qui peut avoir des conséquences financières imprévues.

Pour plus d'informations, consultez la section [Affectation de ressources par programmation](#).

Table des matières

IamRoleArn

L'ARN du rôle IAM AWS Backup utilisé pour s'authentifier lors de la sauvegarde de la ressource cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`

Type : String

Obligatoire : oui

SelectionName

Nom complet d'un document de sélection de ressource. Doit contenir de 1 à 50 caractères alphanumériques ou « `-_.` » caractères.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : oui

Conditions

Les conditions que vous définissez pour affecter des ressources à vos plans de sauvegarde à l'aide de balises. Par exemple, `"StringEquals": { "ConditionKey": "aws:ResourceTag/backup", "ConditionValue": "daily" }`.

Conditionssoutient `StringEqualsStringLike,StringNotEquals`, et `StringNotLike`. Les opérateurs de condition sont sensibles à la casse.

Si vous spécifiez plusieurs conditions, les ressources doivent répondre à toutes les conditions (logique ET).

Type : objet [Conditions](#)

Obligatoire : non

ListOfTags

Nous vous recommandons d'utiliser le `Conditions` paramètre au lieu de celui-ci.

Les conditions que vous définissez pour affecter des ressources à vos plans de sauvegarde à l'aide de balises. Par exemple, `"StringEquals": { "ConditionKey": "backup", "ConditionValue": "daily"}`.

`ListOfTagssupports` uniquement `StringEquals`. Les opérateurs de condition sont sensibles à la casse.

Si vous spécifiez plusieurs conditions, les ressources doivent correspondre à n'importe laquelle des conditions (logique OR).

Type : tableau d'objets [Condition](#)

Obligatoire : non

NotResources

Les Amazon Resource Names (ARNs) des ressources à exclure d'un plan de sauvegarde. Le nombre maximum de ARNs est de 500 sans caractères génériques ou de 30 ARNs avec des caractères génériques.

Si vous devez exclure de nombreuses ressources d'un plan de sauvegarde, envisagez une stratégie de sélection de ressources différente, comme l'attribution d'un seul ou de quelques types de ressource, ou l'affinement de votre sélection de ressources à l'aide de balises.

Type : tableau de chaînes

Obligatoire : non

Resources

Les Amazon Resource Names (ARNs) des ressources à attribuer à un plan de sauvegarde. Le nombre maximum de ARNs est de 500 sans caractères génériques ou de 30 ARNs avec des caractères génériques.

Si vous devez attribuer de nombreuses ressources à un plan de sauvegarde, envisagez une stratégie de sélection de ressources différente, comme l'attribution de toutes les ressources d'un type de ressource, ou l'affinement de votre sélection de ressources à l'aide de balises.

Si vous en spécifiez plusieurs ARNs, les ressources doivent correspondre à l'une des ARNs valeurs (logique OR).

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupSelectionsListMember

Service : AWS Backup

Contient des métadonnées relatives à un objet BackupSelection.

Table des matières

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de CreationDate est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

IamRoleArn

Spécifie l'Amazon Resource Name (ARN) du rôle IAM pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

SelectionId

Identifie de façon unique une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : chaîne

Obligatoire : non

SelectionName

Nom complet d'un document de sélection de ressource.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

BackupVaultListMember

Service : AWS Backup

Contient des métadonnées relatives à un coffre-fort de sauvegarde.

Table des matières

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

CreationDate

Date et heure de création d'une sauvegarde de ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

EncryptionKeyArn

Une clé de chiffrement côté serveur que vous pouvez spécifier pour chiffrer vos sauvegardes à partir de services prenant en charge la AWS Backup gestion complète, par exemple, `arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Si vous spécifiez une clé, vous devez indiquer son ARN et non son alias. Si vous ne spécifiez aucune clé, AWS Backup crée une clé KMS pour vous par défaut.

Pour savoir quels AWS Backup services prennent en charge AWS Backup la gestion complète et comment AWS Backup gère le chiffrement des sauvegardes provenant de services qui ne le sont pas encore AWS Backup, voir [Chiffrement des sauvegardes dans AWS Backup](#)

Type : chaîne

Obligatoire : non

EncryptionKeyType

Type de clé de chiffrement utilisée pour le coffre de sauvegarde. Les valeurs valides sont `CUSTOMER_MANAGED_KMS_KEY` pour les clés gérées par le client ou `_OWNED_KMS_KEY` pour les clés détenues par le client. AWS AWS

Type : Chaîne

Valeurs valides : `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatoire : non

LockDate

Date et heure auxquelles la configuration de AWS Backup Vault Lock devient immuable, ce qui signifie qu'elle ne peut être ni modifiée ni supprimée.

Si vous avez appliqué Vault Lock à votre coffre-fort sans spécifier de date de verrouillage, vous pouvez modifier les paramètres de Vault Lock ou supprimer complètement Vault Lock du coffre-fort à tout moment.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Locked

Valeur booléenne qui indique si AWS Backup Vault Lock s'applique au coffre-fort de sauvegarde sélectionné. Si `true`, Vault Lock empêche les opérations de suppression et de mise à jour sur les points de récupération du coffre-fort sélectionné.

Type : booléen

Obligatoire : non

MaxRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, Vault Lock n'applique pas de période de rétention maximale sur les points de récupération dans le coffre-fort (permettant un stockage indéfini).

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou inférieure à la période de rétention maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : Long

Obligatoire : non

MinRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'applique pas de période de rétention minimale.

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou supérieure à la période de rétention

minimale. Si la période de rétention de la tâche est plus courte que cette période de rétention minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : Long

Obligatoire : non

NumberOfRecoveryPoints

Nombre de points de récupération stockés dans un coffre-fort de sauvegarde.

Type : Long

Obligatoire : non

VaultState

État actuel du coffre.

Type : Chaîne

Valeurs valides : CREATING | AVAILABLE | FAILED

Obligatoire : non

VaultType

Type de coffre-fort dans lequel le point de récupération décrit est stocké.

Type : Chaîne

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CalculatedLifecycle

Service : AWS Backup

Contient des horodatages `DeleteAt` et `MoveToColdStorageAt`, qui sont utilisés pour spécifier le cycle de vie d'un point de récupération.

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Table des matières

DeleteAt

Un horodatage qui indique quand supprimer un point de récupération.

Type : Timestamp

Obligatoire : non

MoveToColdStorageAt

Horodatage qui indique à quel moment il faut passer d'un point de récupération à un stockage à froid.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Condition

Service : AWS Backup

Contient un tableau de triplets composé d'un type de condition (par exemple, `StringEquals`), d'une clé et d'une valeur. Utilisé pour filtrer les ressources à l'aide de leurs balises et les attribuer à un plan de sauvegarde. Sensible à la casse.

Table des matières

ConditionKey

Clé dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Department` est la clé.

Type : String

Obligatoire : oui

ConditionType

Opération appliquée à une paire clé-valeur utilisée pour attribuer des ressources à votre plan de sauvegarde. Condition prenant en charge uniquement `StringEquals`. Pour des options d'attribution plus flexibles, notamment `StringLike` et la possibilité d'exclure des ressources de votre plan de sauvegarde, utilisez `Conditions` (avec un « s » à la fin) pour votre [BackupSelection](#).

Type : String

Valeurs valides : `STRINGEQUALS`

Obligatoire : oui

ConditionValue

Valeur dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Accounting` est la valeur.

Type : String

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ConditionParameter

Service : AWS Backup

Inclut des informations sur les balises que vous définissez pour attribuer des ressources balisées à un plan de sauvegarde.

Incluez le préfixe `aws:ResourceTag` dans vos balises. Par exemple, `"aws:ResourceTag/TagKey1": "Value1"`.

Table des matières

ConditionKey

Clé dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Department` est la clé.

Type : chaîne

Obligatoire : non

ConditionValue

Valeur dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Accounting` est la valeur.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Conditions

Service : AWS Backup

Contient des informations sur les ressources à inclure ou à exclure d'un plan de sauvegarde à l'aide de leurs balises. Les conditions sont sensibles à la casse.

Table des matières

StringEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées avec la même valeur. Également appelé « correspondance exacte ».

Type : tableau d'objets [ConditionParameter](#)

Obligatoire : non

StringLike

Filtre les valeurs de vos ressources balisées pour faire correspondre les valeurs des balises à l'aide d'un caractère générique (*) n'importe où dans la chaîne. Par exemple, « prod* » ou « *rod* » correspond à la valeur de balise « production ».

Type : tableau d'objets [ConditionParameter](#)

Obligatoire : non

StringNotEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées qui n'ont pas la même valeur. Également appelé « correspondance négative ».

Type : tableau d'objets [ConditionParameter](#)

Obligatoire : non

StringNotLike

Filtre les valeurs de vos ressources balisées pour détecter les valeurs de balise non correspondantes à l'aide d'un caractère générique (*) n'importe où dans la chaîne.

Type : tableau d'objets [ConditionParameter](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ControlInputParameter

Service : AWS Backup

Les paramètres d'un contrôle. Un contrôle peut comporter aucun, un ou plusieurs paramètres. Un exemple de contrôle avec deux paramètres : « la fréquence du plan de sauvegarde est d'au moins `daily` et la période de conservation est d'au moins `1 year` ». Le premier paramètre est `daily`. Le second paramètre est `1 year`.

Table des matières

ParameterName

Le nom d'un paramètre, par exemple `BackupPlanFrequency`.

Type : chaîne

Obligatoire : non

ParameterValue

La valeur d'un paramètre, par exemple `hourly`.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ControlScope

Service : AWS Backup

Un cadre est constitué d'un ou plusieurs contrôles. Chaque contrôle possède sa propre portée de contrôle. La portée de contrôle peut s'appliquer à un ou plusieurs types de ressource, à une combinaison de clé et de valeur de balise ou à une combinaison de type de ressource et d'ID de ressource. Si aucune portée n'est spécifiée, les évaluations de la règle sont déclenchées lorsque n'importe quelle ressource de votre groupe d'enregistrement change dans la configuration.

Note

Pour définir une portée de contrôle qui inclut l'ensemble d'une ressource donnée, laissez `ControlScope` vide ou ne le transmettez pas lors de l'appel de `CreateFramework`.

Table des matières

ComplianceResourceIds

L'ID de la seule AWS ressource que vous souhaitez que votre étendue de contrôle contienne.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 100 éléments.

Obligatoire : non

ComplianceResourceTypes

Indique si la portée de contrôle inclut un ou plusieurs types de ressources, tels que EFS ou RDS.

Type : tableau de chaînes

Obligatoire : non

Tags

La paire clé-valeur de balise appliquée aux AWS ressources pour lesquelles vous souhaitez déclencher l'évaluation d'une règle. Une seule paire clé-valeur peut être fournie. La valeur de la balise est facultative, mais elle ne peut pas être une chaîne vide si vous créez ou modifiez un framework depuis la console (bien que la valeur puisse être une chaîne vide lorsqu'elle est incluse dans un CloudFormation modèle).

La structure pour attribuer une étiquette est la suivante :
[{"Key":"string","Value":"string"}].

Type : mappage chaîne/chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CopyAction

Service : AWS Backup

Les détails de l'opération de copie.

Table des matières

DestinationBackupVaultArn

Un nom de ressource Amazon (ARN) qui identifie de manière unique le coffre-fort de sauvegarde de destination pour la sauvegarde copiée. Par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : String

Obligatoire : oui

Lifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Type : objet [Lifecycle](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CopyJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de copie.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de copie.

Type : Chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupSizeInBytes

Taille, en octets, d'une tâche de copie.

Type : Long

Obligatoire : non

ChildJobsInState

Cela renvoie les statistiques des tâches de copie enfant (imbriquées) incluses.

Type : mappage chaîne/long

Clés valides : `CREATED` | `RUNNING` | `COMPLETED` | `FAILED` | `PARTIAL`

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'[ID logique](#) au sein d'une pile.

Type : chaîne

Obligatoire : non

CopyJobId

Identifie de manière unique une tâche de copie.

Type : chaîne

Obligatoire : non

CreatedBy

Contient des informations sur le plan de sauvegarde et la règle AWS Backup utilisés pour lancer la sauvegarde du point de restauration.

Type : objet [RecoveryPointCreator](#)

Obligatoire : non

CreatedByBackupJobId

ID de tâche de sauvegarde à l'origine de cette tâche de copie. Applicable uniquement aux tâches de copie planifiées et aux tâches de copie automatiques vers un coffre-fort logiquement espacé.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DestinationBackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de copie de destination ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

DestinationEncryptionKeyArn

Le nom de ressource Amazon (ARN) de la clé KMS utilisée pour chiffrer la sauvegarde copiée dans le coffre de destination. Il peut s'agir d'une clé gérée par le client ou d'une clé AWS gérée.

Type : chaîne

Obligatoire : non

DestinationRecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération de destination ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

DestinationRecoveryPointLifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Type : objet [Lifecycle](#)

Obligatoire : non

`DestinationVaultLockState`

État de verrouillage du coffre-fort de sauvegarde de destination. Pour les coffres-forts à espacement logique, cela indique si le coffre-fort est verrouillé en mode de conformité. Les valeurs valides sont `LOCKED` et `UNLOCKED`.

Type : chaîne

Obligatoire : non

`DestinationVaultType`

Type de coffre-fort de sauvegarde de destination dans lequel le point de restauration copié est stocké. Les valeurs valides concernent `BACKUP_VAULT` les coffres-forts de sauvegarde standard et les coffres-forts `LOGICALLY_AIR_GAPPED_BACKUP_VAULT` à espacement logique.

Type : chaîne

Obligatoire : non

`IamRoleArn`

Spécifie l'ARN du rôle IAM utilisé pour copier le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

`IsParent`

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'une tâche de copie parent (composite).

Type : booléen

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `InvalidParameters`. Voir [Surveillance](#) pour une liste de `MessageCategory` chaînes.

La valeur `ANY` renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme

Type : chaîne

Obligatoire : non

NumberOfChildJobs

Le nombre de tâches de copie secondaires (imbriquées).

Type : Long

Obligatoire : non

ParentJobId

Cela identifie de manière unique une demande vers AWS Backup pour copier une ressource. Le retour sera l'ID de tâche parent (composite).

Type : chaîne

Obligatoire : non

ResourceArn

La AWS ressource à copier ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource à copier ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

Obligatoire : non

SourceBackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de copie source ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

SourceRecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération source ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

State

L'état actuel d'une tâche de copie.

Type : Chaîne

Valeurs valides : `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de copie d'une ressource.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CopyJobSummary

Service : AWS Backup

Il s'agit d'un résumé des tâches de copie créées ou en cours d'exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État RestourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L'ID de compte qui possède les tâches figurant dans le résumé.

Type : String

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l'heure au format numérique de l'heure de fin d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir [Surveillance](#) pour une liste de `MessageCategory` chaînes.

La valeur `ANY` renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

Region

Les AWS régions figurant dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande `GetSupportedResourceTypes` renvoie des chaînes pour les types de ressources pris en charge

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur `1516925490,087` représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : String

Valeurs valides : CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

DateRange

Service : AWS Backup

Il s'agit d'un filtre de ressources contenant FromDate : DateTime et ToDate : DateTime. Les deux valeurs sont requises. Les DateTime valeurs futures ne sont pas autorisées.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives). Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Table des matières

FromDate

Cette valeur est la date de début incluse.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives).

Type : Timestamp

Obligatoire : oui

ToDate

Cette valeur est la date de fin incluse.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives).

Type : Timestamp

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Framework

Service : AWS Backup

Contient des informations détaillées sur un framework. Les frameworks contiennent des contrôles qui évaluent vos événements et ressources de sauvegarde et établissent des rapports. Les frameworks génèrent des résultats quotidiens en matière de conformité.

Table des matières

CreationTime

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, `2020-07-10T15:00:00.000-08:00` représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

Obligatoire : non

DeploymentStatus

Le statut du déploiement d'un framework. Les statuts sont les suivants :

`CREATE_IN_PROGRESS` | `UPDATE_IN_PROGRESS` | `DELETE_IN_PROGRESS` | `COMPLETED`
| `FAILED`

Type : chaîne

Obligatoire : non

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

FrameworkDescription

Une description facultative du cadre avec 1 024 caractères au maximum.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

FrameworkName

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : non

NumberOfControls

Le nombre de contrôles contenus dans le framework.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

FrameworkControl

Service : AWS Backup

Contient des informations détaillées sur tous les contrôles d'un cadre. Chaque cadre doit contenir au moins un contrôle.

Table des matières

ControlName

Le nom d'un contrôle. Ce nom contient de 1 à 256 caractères.

Type : String

Obligatoire : oui

ControlInputParameters

Les paires nom/valeur.

Type : tableau d'objets [ControlInputParameter](#)

Obligatoire : non

ControlScope

La portée d'un contrôle. La portée du contrôle définit ce que le contrôle va évaluer. Trois exemples de portées de contrôle sont : un plan de sauvegarde spécifique, tous les plans de sauvegarde avec une balise spécifique ou tous les plans de sauvegarde.

Pour de plus amples informations, [ControlScopeconsultez](#) .

Type : objet [ControlScope](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour Ruby V3](#)

IndexAction

Service : AWS Backup

Il s'agit d'un tableau facultatif au sein d'un BackupRule.

IndexAction se compose d'un ResourceTypes.

Table des matières

ResourceTypes

0 ou 1 action d'index sera acceptée pour chacune BackupRule.

Valeurs valides :

- EBS pour Amazon Elastic Block Store
- S3pour Amazon Simple Storage Service (Amazon S3)

Type : tableau de chaînes

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

IndexedRecoveryPoint

Service : AWS Backup

Il s'agit d'un point de restauration associé à un index de sauvegarde.

Seuls les points de restauration dotés d'un index de sauvegarde peuvent être inclus dans une recherche.

Table des matières

BackupCreationDate

Date et heure de création d'une sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

BackupVaultArn

Un ARN qui identifie de manière unique le coffre de sauvegarde dans lequel l'index du point de restauration est stocké.

Par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

IamRoleArn

Ceci indique l'ARN du rôle IAM utilisé pour cette opération.

Par exemple, `arn:aws:iam::123456789012:role/S3access`

Type : chaîne

Obligatoire : non

IndexCreationDate

Date et heure de création d'un index de sauvegarde, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

IndexStatus

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : PENDING | ACTIVE | FAILED DELETING

Un point de récupération dont l'index a le statut de ACTIVE peut être inclus dans une recherche.

Type : String

Valeurs valides : PENDING | ACTIVE | FAILED | DELETING

Obligatoire : non

IndexStatusMessage

Chaîne sous la forme d'un message détaillé expliquant l'état d'un index de sauvegarde associé au point de restauration.

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de manière unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Type : chaîne

Obligatoire : non

ResourceType

Type de ressource du point de restauration indexé.

- EBS pour Amazon Elastic Block Store
- S3 pour Amazon Simple Storage Service (Amazon S3)

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\]{1,50}$`

Obligatoire : non

SourceResourceArn

Chaîne contenant le nom de la ressource Amazon (ARN) qui identifie de manière unique la ressource source.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

KeyValue

Service : AWS Backup

Pair of two related strings. Les caractères autorisés sont les lettres, les espaces et les chiffres qui peuvent être représentés au format UTF-8, ainsi que les caractères suivants : + - = . _ : /

Table des matières

Key

Clé de la balise (chaîne). La clé ne peut pas commencer par aws :.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `^(?![aA]{1}[wW]{1}[sS]{1}:)([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]+)$`

Type : String

Obligatoire : oui

Value

Valeur de la clé.

Contraintes de longueur : longueur maximale de 256.

Modèle : `^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$`

Type : String

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

LatestMpaApprovalTeamUpdate

Service : AWS Backup

Contient des informations sur la dernière mise à jour d'une association d'équipes d'approbation MPA.

Table des matières

ExpiryDate

Date et heure auxquelles la mise à jour de l'équipe d'approbation de la MPA expirera.

Type : Timestamp

Obligatoire : non

InitiationDate

Date et heure auxquelles la mise à jour de l'équipe d'approbation de la MPA a été lancée.

Type : Timestamp

Obligatoire : non

MpaSessionArn

L'ARN de la session MPA associée à cette mise à jour.

Type : chaîne

Obligatoire : non

Status

Mise à jour de l'état actuel de l'équipe d'approbation de la MPA.

Type : String

Valeurs valides : PENDING | APPROVED | FAILED

Obligatoire : non

StatusMessage

Un message décrivant l'état actuel de la mise à jour de l'équipe d'approbation de la MPA.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

LatestRevokeRequest

Service : AWS Backup

Contient des informations sur la dernière demande de révocation de l'accès à un coffre-fort de sauvegarde.

Table des matières

ExpiryDate

Date et heure d'expiration de la demande de révocation.

Type : Timestamp

Obligatoire : non

InitiationDate

Date et heure auxquelles la demande de révocation a été initiée.

Type : Timestamp

Obligatoire : non

MpaSessionArn

L'ARN de la session MPA associée à cette demande de révocation.

Type : chaîne

Obligatoire : non

Status

État actuel de la demande de révocation.

Type : String

Valeurs valides : PENDING | FAILED

Obligatoire : non

StatusMessage

Message décrivant l'état actuel de la demande de révocation.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

LegalHold

Service : AWS Backup

Une conservation légale est un outil administratif qui permet d'empêcher la suppression de sauvegardes pendant une conservation. Tant que la conservation est en place, les sauvegardes sous conservation ne peuvent pas être supprimées et les politiques de cycle de vie susceptibles de modifier le statut des sauvegardes (comme le passage à un stockage à froid) sont retardées jusqu'à ce que la conservation légale soit levée. Une sauvegarde peut avoir plusieurs conservations légales. Des conservations légales sont appliquées à une ou plusieurs sauvegardes (également appelées points de récupération). Ces sauvegardes peuvent être filtrées par type de ressource et par ressource IDs.

Table des matières

CancellationDate

Heure à laquelle le blocage légal a été annulé.

Type : Timestamp

Obligatoire : non

CreationDate

Heure à laquelle la mise en attente légale a été créée.

Type : Timestamp

Obligatoire : non

Description

Description d'une détention légale.

Type : chaîne

Obligatoire : non

LegalHoldArn

L'Amazon Resource Name (ARN) du support légal ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

LegalHoldId

L'identifiant de la retenue légale.

Type : chaîne

Obligatoire : non

Status

Le statut de la suspension légale.

Type : String

Valeurs valides : CREATING | ACTIVE | CANCELING | CANCELED

Obligatoire : non

Title

Titre d'une détention légale.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Lifecycle

Service : AWS Backup

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et `DeleteAfterDays`.

Table des matières

DeleteAfterDays

Nombre de jours après sa création pendant lesquels un point de récupération est supprimé. Cette valeur doit être postérieure d'au moins 90 jours au nombre de jours spécifié dans `MoveToColdStorageAfterDays`.

Type : Long

Obligatoire : non

DeleteAfterEvent

Événement à la suite duquel un point de récupération est supprimé. Un point de récupération contenant les deux `DeleteAfterDays` et `DeleteAfterEvent` sera supprimé dès que la première condition sera satisfaite. Entrée non valide.

Type : Chaîne

Valeurs valides : `DELETE_AFTER_COPY`

Obligatoire : non

MoveToColdStorageAfterDays

Nombre de jours après sa création pendant lesquels un point de récupération est déplacé vers une chambre froide.

Type : Long

Obligatoire : non

OptInToArchiveForSupportedResources

Si la valeur est vraie, votre plan de sauvegarde fait passer les ressources prises en charge au niveau de stockage d'archivage (froid) conformément à vos paramètres de cycle de vie.

Type : booléen

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ProtectedResource

Service : AWS Backup

Structure contenant des informations sur une ressource sauvegardée.

Table des matières

LastBackupTime

Date et heure de la dernière sauvegarde d'une ressource, au format Unix et au format UTC (temps universel coordonné). La valeur de LastBackupTime est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastBackupVaultArn

L'ARN (Amazon Resource Name) du coffre de sauvegarde qui contient le point de restauration de sauvegarde le plus récent.

Type : chaîne

Obligatoire : non

LastRecoveryPointArn

L'ARN (Amazon Resource Name) du point de récupération le plus récent.

Type : chaîne

Obligatoire : non

ResourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ProtectedResourceConditions

Service : AWS Backup

Les conditions que vous définissez pour les ressources dans votre plan de test de restauration à l'aide de balises.

Table des matières

StringEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées avec la même valeur. Également appelé « correspondance exacte ».

Type : tableau d'objets [KeyValue](#)

Obligatoire : non

StringNotEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées qui n'ont pas la même valeur. Également appelé « correspondance négative ».

Type : tableau d'objets [KeyValue](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RecoveryPointByBackupVault

Service : AWS Backup

Contient des informations détaillées sur les points de récupération stockés dans un coffre-fort de sauvegarde.

Table des matières

AggregatedScanResult

Contient les derniers résultats d'analyse par rapport au point de récupération et inclut actuellementFailedScan,Findings,LastComputed.

Type : objet [AggregatedScanResult](#)

Obligatoire : non

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : Long

Obligatoire : non

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

CalculatedLifecycle

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet [CalculatedLifecycle](#)

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'[ID logique](#) au sein d'une pile.

Type : chaîne

Obligatoire : non

CreatedBy

Contient des informations d'identification relatives à la création d'un point de récupération, dont les `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour le créer.

Type : objet [RecoveryPointCreator](#)

Obligatoire : non

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple,

`arn:aws:kms:us-`

`west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab.`

Type : chaîne

Obligatoire : non

EncryptionKeyType

Type de clé de chiffrement utilisée pour le point de récupération. Les valeurs valides sont `CUSTOMER_MANAGED_KMS_KEY` pour les clés gérées par le client ou `_OWNED_KMS_KEY` pour les clés détenues par le client. AWS AWS

Type : Chaîne

Valeurs valides : `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple,

`arn:aws:iam::123456789012:role/S3Access.`

Type : chaîne

Obligatoire : non

IndexStatus

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Un point de récupération dont l'index a le statut de `ACTIVE` peut être inclus dans une recherche.

Type : Chaîne

Valeurs valides : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Obligatoire : non

IndexStatusMessage

Chaîne sous la forme d'un message détaillé expliquant l'état d'un index de sauvegarde associé au point de restauration.

Type : chaîne

Obligatoire : non

InitiationDate

Date et heure auxquelles la tâche de sauvegarde qui a créé ce point de restauration a été lancée, au format Unix et en temps universel coordonné (UTC).

Type : Timestamp

Obligatoire : non

IsEncrypted

Valeur booléenne renvoyée comme TRUE si le point de récupération spécifié était chiffré ou FALSE s'il n'était pas chiffré.

Type : booléen

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'un point de récupération parent (composite).

Type : booléen

Obligatoire : non

LastRestoreTime

Date et heure de la dernière restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de LastRestoreTime est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers une chambre froide doivent être stockées dans une chambre froide pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « nombre de jours avant transfert vers stockage à froid » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau [Disponibilité des fonctionnalités par ressource](#). AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet [Lifecycle](#)

Obligatoire : non

ParentRecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

ResourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource enregistrée comme point de récupération ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

SourceBackupVaultArn

Le coffre-fort de sauvegarde à partir duquel le point de récupération a été initialement copié. Si le point de récupération est restauré sur le même compte, cette valeur sera null.

Type : chaîne

Obligatoire : non

Status

Code de statut spécifiant l'état du point de récupération.

Type : Chaîne

Valeurs valides : COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

Obligatoire : non

StatusMessage

Un message expliquant l'état actuel du point de récupération.

Type : chaîne

Obligatoire : non

VaultType

Type de coffre-fort dans lequel le point de récupération décrit est stocké.

Type : Chaîne

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RecoveryPointByResource

Service : AWS Backup

Contient des informations détaillées sur un point de récupération enregistré.

Table des matières

AggregatedScanResult

Contient les derniers résultats d'analyse par rapport au point de récupération et inclut actuellement `FailedScan`, `Findings`, `LastComputed`.

Type : objet [AggregatedScanResult](#)

Obligatoire : non

BackupSizeBytes

Taille d'une sauvegarde, en octets.

Type : Long

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple,
`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

Obligatoire : non

EncryptionKeyType

Type de clé de chiffrement utilisée pour le point de récupération. Les valeurs valides sont `CUSTOMER_MANAGED_KMS_KEY` pour les clés gérées par le client ou `_OWNED_KMS_KEY` pour les clés détenues par le client. AWS AWS

Type : Chaîne

Valeurs valides : `AWS_OWNED_KMS_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Obligatoire : non

IndexStatus

Il s'agit de l'état actuel de l'index de sauvegarde associé au point de restauration spécifié.

Les statuts sont les suivants : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Un point de récupération dont l'index a le statut de `ACTIVE` peut être inclus dans une recherche.

Type : Chaîne

Valeurs valides : `PENDING` | `ACTIVE` | `FAILED` | `DELETING`

Obligatoire : non

IndexStatusMessage

Chaîne sous la forme d'un message détaillé expliquant l'état d'un index de sauvegarde associé au point de restauration.

Type : chaîne

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'un point de récupération parent (composite).

Type : booléen

Obligatoire : non

ParentRecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

Status

Code de statut spécifiant l'état du point de récupération.

Type : Chaîne

Valeurs valides : COMPLETED | PARTIAL | DELETING | EXPIRED | AVAILABLE | STOPPED | CREATING

Obligatoire : non

StatusMessage

Un message expliquant l'état actuel du point de récupération.

Type : chaîne

Obligatoire : non

VaultType

Type de coffre-fort dans lequel le point de récupération décrit est stocké.

Type : Chaîne

Valeurs valides : BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT |
RESTORE_ACCESS_BACKUP_VAULT

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RecoveryPointCreator

Service : AWS Backup

Contient des informations sur le plan de sauvegarde et la règle AWS Backup utilisés pour lancer la sauvegarde du point de restauration.

Table des matières

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

Obligatoire : non

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

BackupPlanName

Nom du plan de sauvegarde qui a créé ce point de restauration. Cela fournit un contexte lisible par l'homme indiquant quel plan de sauvegarde était responsable de la tâche de sauvegarde.

Type : chaîne

Obligatoire : non

BackupPlanVersion

IDs Les versions sont des chaînes uniques, générées aléatoirement, codées Unicode et UTF-8 d'une longueur maximale de 1 024 octets. Ils ne peuvent pas être modifiés.

Type : chaîne

Obligatoire : non

BackupRuleCron

Expression cron qui définit le calendrier de la règle de sauvegarde. Cela indique la fréquence et le moment auxquels les sauvegardes sont automatiquement déclenchées.

Type : chaîne

Obligatoire : non

BackupRuleId

Identifie de manière unique une règle utilisée pour planifier la sauvegarde d'une sélection de ressources.

Type : chaîne

Obligatoire : non

BackupRuleName

Nom de la règle de sauvegarde dans le plan de sauvegarde qui a créé ce point de restauration. Cela permet d'identifier la règle spécifique qui a déclenché la tâche de sauvegarde.

Type : chaîne

Obligatoire : non

BackupRuleTimezone

Fuseau horaire utilisé pour le calendrier des règles de sauvegarde. Cela fournit le contexte dans lequel les sauvegardes sont planifiées pour s'exécuter dans le fuseau horaire spécifié.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour Ruby V3](#)

RecoveryPointMember

Service : AWS Backup

Il s'agit d'un point de récupération qui est un point de récupération enfant (imbriqué) d'un point de récupération parent (composite). Ces points de récupération peuvent être dissociés de leur point de récupération parent (composite), auquel cas ils n'en seront plus membres.

Table des matières

BackupVaultName

Le nom du coffre de sauvegarde (le conteneur logique dans lequel les sauvegardes sont stockées).

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\]{2,50}$`

Obligatoire : non

RecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

ResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique une ressource enregistrée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource enregistré en tant que point de récupération.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RecoveryPointSelection

Service : AWS Backup

Cela spécifie les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Table des matières

DateRange

Il s'agit d'un filtre de ressources contenant FromDate : DateTime et ToDate : DateTime. Les deux valeurs sont requises. Les DateTime valeurs futures ne sont pas autorisées.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives). Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : objet [DateRange](#)

Obligatoire : non

ResourceIdentifiers

Il s'agit des ressources incluses dans la sélection des ressources (y compris le type de ressources et les coffres).

Type : tableau de chaînes

Obligatoire : non

VaultNames

Il s'agit des noms des coffres-forts dans lesquels sont contenus les points de récupération sélectionnés.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ReportDeliveryChannel

Service : AWS Backup

Contient des informations issues de votre plan de rapport sur l'endroit et la manière de diffuser vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Table des matières

S3BucketName

Nom unique du compartiment S3 dans lequel se trouvent vos rapports.

Type : String

Obligatoire : oui

Formats

Le format de vos rapports : CSVJSON, ou les deux. Si aucune valeur n'est spécifiée, le format par défaut est CSV.

Type : tableau de chaînes

Obligatoire : non

S3KeyPrefix

Le préfixe indiquant où AWS Backup Audit Manager envoie vos rapports à Amazon S3. Le préfixe est cette partie du chemin suivant : s3 ://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name. S'il n'est pas spécifié, il n'y a pas de préfixe.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour Ruby V3](#)

ReportDestination

Service : AWS Backup

Contient des informations issues de votre tâche de rapport concernant la destination de votre rapport.

Table des matières

S3BucketName

Nom unique du compartiment Amazon S3 qui reçoit vos rapports.

Type : chaîne

Obligatoire : non

S3Keys

Clé d'objet qui identifie de façon unique vos rapports dans votre compartiment S3.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ReportJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de rapport. Une tâche de rapport compile un rapport sur la base d'un plan de rapport et le publie sur Amazon S3.

Table des matières

CompletionTime

Date et heure de fin d'une tâche de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreationTime

Date et heure de création d'une tâche de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ReportDestination

Le nom du compartiment S3 et les clés S3 de la destination où la tâche de rapport publie le rapport.

Type : objet [ReportDestination](#)

Obligatoire : non

ReportJobId

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. Le travail de rapport IDs ne peut pas être modifié.

Type : chaîne

Obligatoire : non

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ReportTemplate

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

Type : chaîne

Obligatoire : non

Status

Statut d'une tâche de rapports. Les statuts sont les suivants :

CREATED | RUNNING | COMPLETED | FAILED

COMPLETED signifie que le rapport est disponible pour examen à la destination que vous avez désignée. Si le statut est FAILED, examinez le StatusMessage pour en connaître la raison.

Type : chaîne

Obligatoire : non

StatusMessage

Un message expliquant le statut de la tâche de rapport.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ReportPlan

Service : AWS Backup

Contient des informations détaillées sur un plan de rapport.

Table des matières

CreationTime

Date et heure de création d'un plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DeploymentStatus

Le statut de déploiement d'un plan de rapport. Les statuts sont les suivants :

`CREATE_IN_PROGRESS` | `UPDATE_IN_PROGRESS` | `DELETE_IN_PROGRESS` | `COMPLETED`

Type : chaîne

Obligatoire : non

LastAttemptedExecutionTime

Date et heure de la dernière tentative d'exécution d'une tâche de rapport associée à ce plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastAttemptedExecutionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastSuccessfulExecutionTime

Date et heure de la dernière exécution réussie d'une tâche de rapport associée à ce plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastSuccessfulExecutionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ReportDeliveryChannel

Contient des informations sur l'endroit et la manière de diffuser vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet [ReportDeliveryChannel](#)

Obligatoire : non

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ReportPlanDescription

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : .*\\S.*

Obligatoire : non

ReportPlanName

Le nom unique du plan de rapport. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : [a-zA-Z][_a-zA-Z0-9]*

Obligatoire : non

ReportSetting

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

Si le modèle de rapport est RESOURCE_COMPLIANCE_REPORT ou CONTROL_COMPLIANCE_REPORT, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet [ReportSetting](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ReportSetting

Service : AWS Backup

Contient des informations détaillées sur un paramètre de rapport.

Table des matières

ReportTemplate

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT |
SCAN_JOB_REPORT

Type : Chaîne

Obligatoire : oui

Accounts

Il s'agit des comptes à inclure dans le rapport.

Utilisez la valeur de chaîne de ROOT pour inclure toutes les unités organisationnelles.

Type : tableau de chaînes

Obligatoire : non

FrameworkArns

Les Amazon Resource Names (ARNs) des frameworks couverts par un rapport.

Type : tableau de chaînes

Obligatoire : non

NumberOfFrameworks

Le nombre de frameworks couverts par un rapport.

Type : Integer

Obligatoire : non

OrganizationUnits

Il s'agit des unités organisationnelles à inclure dans le rapport.

Type : tableau de chaînes

Obligatoire : non

Regions

Il s'agit des régions qui seront incluses dans le rapport.

Utilisez le caractère générique comme valeur de chaîne pour inclure toutes les régions.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ResourceSelection

Service : AWS Backup

Il contient des métadonnées relatives à la sélection des ressources pour les configurations de hiérarchisation.

Vous pouvez spécifier jusqu'à 5 sélections de ressources différentes par configuration de hiérarchisation. Les données transférées vers le niveau le moins coûteux y restent jusqu'à leur suppression (transition unidirectionnelle).

Table des matières

Resources

Tableau de chaînes contenant ARNs soit les ressources associées, soit un caractère générique * pour spécifier toutes les ressources. Vous pouvez spécifier jusqu'à 100 ressources spécifiques par configuration de hiérarchisation.

Type : tableau de chaînes

Obligatoire : oui

ResourceType

Type de AWS ressource ; par exemple, S3 pour Amazon S3. Pour les configurations de hiérarchisation, cela est actuellement limité à S3.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : oui

TieringDownSettingsInDays

Nombre de jours après sa création dans un coffre de sauvegarde pendant lesquels un objet peut passer au niveau de stockage chaud à faible coût. Doit être un entier positif compris entre 60 et 36 500 jours.

Type : Integer

Plage valide : Valeur minimum de 60. Valeur maximale de 36 500.

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreAccessBackupVaultListMember

Service : AWS Backup

Contient des informations sur un coffre de sauvegarde pour accès à la restauration.

Table des matières

ApprovalDate

Date et heure auxquelles le coffre de sauvegarde de l'accès à la restauration a été approuvé.

Type : Timestamp

Obligatoire : non

CreationDate

Date et heure de création du coffre de sauvegarde de l'accès à la restauration.

Type : Timestamp

Obligatoire : non

LatestRevokeRequest

Informations sur la dernière demande de révocation de l'accès à ce coffre-fort de sauvegarde.

Type : objet [LatestRevokeRequest](#)

Obligatoire : non

RestoreAccessBackupVaultArn

L'ARN du coffre de sauvegarde pour l'accès à la restauration.

Type : chaîne

Obligatoire : non

VaultState

État actuel du coffre de sauvegarde de l'accès à la restauration.

Type : String

Valeurs valides : CREATING | AVAILABLE | FAILED

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreJobCreator

Service : AWS Backup

Contient des informations sur le plan de test de la restauration utilisé par AWS Backup pour lancer la tâche de restauration.

Table des matières

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreJobsListMember

Service : AWS Backup

Contient des métadonnées relatives à une tâche de restauration.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de restauration.

Type : Chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupSizeInBytes

Taille, en octets, de la ressource restaurée.

Type : Long

Obligatoire : non

BackupVaultArn

Nom de ressource Amazon (ARN) du coffre de sauvegarde contenant le point de restauration. Cela permet d'identifier les politiques et les autorisations d'accès au coffre-fort.

Type : chaîne

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de restauration.

Type : objet [RestoreJobCreator](#)

Obligatoire : non

CreatedResourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DeletionStatus

Cela indique le statut des données générées par le test de la restauration. Le statut peut être `Deleting`, `Failed` ou `Successful`.

Type : Chaîne

Valeurs valides : `DELETING` | `FAILED` | `SUCCESSFUL`

Obligatoire : non

DeletionStatusMessage

Cela décrit le statut de suppression de la tâche de restauration.

Type : chaîne

Obligatoire : non

ExpectedCompletionTimeMinutes

Durée en minutes prévue d'une tâche de restauration d'un point de récupération.

Type : Long

Obligatoire : non

IamRoleArn

L'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant si la tâche de restauration est une tâche de restauration parent (composite).

Type : booléen

Obligatoire : non

ParentJobId

Il s'agit de l'identifiant unique de la tâche de restauration parent pour la tâche de restauration sélectionnée.

Type : chaîne

Obligatoire : non

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple,

`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

RecoveryPointCreationDate

Date à laquelle un point de récupération a été créé.

Type : Timestamp

Obligatoire : non

ResourceType

Le type de ressource des tâches de restauration répertoriées ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

RestoreJobId

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : chaîne

Obligatoire : non

SourceResourceArn

Le nom de ressource Amazon (ARN) de la ressource d'origine qui a été sauvegardée. Cela fournit un contexte sur la ressource en cours de restauration.

Type : chaîne

Obligatoire : non

Status

Code d'état spécifiant l'état de la tâche initiée par AWS Backup pour restaurer un point de restauration.

Type : Chaîne

Valeurs valides : PENDING | RUNNING | COMPLETED | ABORTED | FAILED

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de restauration d'un point de récupération.

Type : chaîne

Obligatoire : non

ValidationStatus

État de la validation exécutée sur la tâche de restauration indiquée.

Type : Chaîne

Valeurs valides : FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

Obligatoire : non

ValidationStatusMessage

Cela décrit le statut de la validation exécutée sur la tâche de restauration indiquée.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreJobSummary

Service : AWS Backup

Il s'agit d'un résumé des tâches de restauration créées ou en cours d'exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État ResourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L'ID de compte qui possède les tâches figurant dans le résumé.

Type : String

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l'heure au format numérique de l'heure de fin d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Region

Les AWS régions figurant dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande `GetSupportedResourceTypes` renvoie des chaînes pour les types de ressources pris en charge.

Type : String

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : String

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingPlanForCreate

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

RecoveryPointSelection

`RecoveryPointSelection` possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer `Algorithm` si vous voulez le dernier point de récupération dans votre répertoire `SelectionWindowDays` ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans `IncludeVaults` quels coffres-forts les points de récupération peuvent être choisis.

`Algorithm`(obligatoire) Valeurs valides : « LATEST_WITHIN_WINDOW » ou « RANDOM_WITHIN_WINDOW ».

`Recovery point types`(obligatoire) Valeurs valides : « SNAPSHOT » et/ou « CONTINUOUS ». Incluez SNAPSHOT pour restaurer uniquement les points de restauration des instantanés ; incluez CONTINUOUS pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de `Algorithm`.

`IncludeVaults`(obligatoire). Vous devez inclure un ou plusieurs coffres-forts de sauvegarde. Utilisez le caractère générique ["*"] ou spécifique ARNs.

`SelectionWindowDays`(facultatif) La valeur doit être un entier (en jours) compris entre 1 et 365. Si elle n'est pas incluse, la valeur par défaut est. 30

`ExcludeVaults`(facultatif). Vous pouvez choisir de saisir un ou plusieurs coffres-forts de sauvegarde spécifiques ARNs pour exclure le contenu de ces coffres-forts de l'éligibilité à la restauration. Vous pouvez également inclure une liste de sélecteurs. Si ce paramètre et sa valeur ne sont pas inclus, la valeur par défaut est une liste vide.

Type : objet [RestoreTestingRecoveryPointSelection](#)

Obligatoire : oui

RestoreTestingPlanName

RestoreTestingPlanName Il s'agit d'une chaîne unique qui est le nom du plan de test de restauration. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : String

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté. Lorsqu'aucune expression CRON n'est fournie, AWS Backup utilise l'expression `cron(0 5 ? * * *)` par défaut.

Type : String

Obligatoire : oui

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingPlanForGet

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

CreationTime

Date et heure de création d'un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

RecoveryPointSelection

Les critères spécifiés d'attribution d'un ensemble de ressources, tels que les types de point de récupération ou les coffres-forts de sauvegarde.

Type : objet [RestoreTestingRecoveryPointSelection](#)

Obligatoire : oui

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : String

Obligatoire : oui

RestoreTestingPlanName

Nom du plan de test de restauration.

Type : String

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté. Lorsqu'aucune expression CRON n'est fournie, AWS Backup elle utilise l'expression `cron(0 5 ? * * *)` par défaut.

Type : String

Obligatoire : oui

CreatorRequestId

Cela identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un `CreatorRequestId` qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « `-_.` » caractères.

Type : chaîne

Obligatoire : non

LastExecutionTime

La dernière fois qu'un test de la restauration a été exécuté avec le plan de test de la restauration spécifié. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastUpdateTime

Date et heure de mise à jour du plan de test de la restauration. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingPlanForList

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

CreationTime

Date et heure de création d'un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : String

Obligatoire : oui

RestoreTestingPlanName

Nom du plan de test de restauration.

Type : String

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté. Lorsqu'aucune expression CRON n'est fournie, AWS Backup elle utilise l'expression `cron(0 5 ? * * *)` par défaut.

Type : String

Obligatoire : oui

LastExecutionTime

La dernière fois qu'un test de la restauration a été exécuté avec le plan de test de la restauration spécifié. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastUpdateTime

Date et heure de mise à jour du plan de test de la restauration. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, `ScheduleExpressions` ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingPlanForUpdate

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

RecoveryPointSelection

Obligatoire : `Algorithm` ; `RecoveryPointTypes` ; `IncludeVaults` (un ou plusieurs).

Facultatif : `SelectionWindowDays`(« 30 » s'il n'est pas spécifié) ; `ExcludeVaults` (la valeur par défaut est une liste vide si elle n'est pas répertoriée).

Type : objet [RestoreTestingRecoveryPointSelection](#)

Obligatoire : non

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté. Lorsqu'aucune expression CRON n'est fournie, AWS Backup utilise l'expression `cron(0 5 ? * * *)` par défaut.

Type : chaîne

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, `ScheduleExpressions` ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingRecoveryPointSelection

Service : AWS Backup

RecoveryPointSelection possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer Algorithm si vous voulez le dernier point de récupération dans votre répertoire SelectionWindowDays ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans IncludeVaults quels coffres-forts les points de récupération peuvent être choisis.

Algorithm(obligatoire) Valeurs valides : « LATEST_WITHIN_WINDOW » ou « RANDOM_WITHIN_WINDOW ».

Recovery point types(obligatoire) Valeurs valides : « SNAPSHOT » et/ou « CONTINUOUS ». Incluez SNAPSHOT pour restaurer uniquement les points de restauration des instantanés ; incluez CONTINUOUS pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de Algorithm.

IncludeVaults(obligatoire). Vous devez inclure un ou plusieurs coffres-forts de sauvegarde. Utilisez le caractère générique ["*"] ou spécifique ARNs.

SelectionWindowDays(facultatif) La valeur doit être un entier (en jours) compris entre 1 et 365. Si elle n'est pas incluse, la valeur par défaut est. 30

ExcludeVaults(facultatif). Vous pouvez choisir de saisir un ou plusieurs coffres-forts de sauvegarde spécifiques ARNs pour exclure le contenu de ces coffres-forts de l'éligibilité à la restauration. Vous pouvez également inclure une liste de sélecteurs. Si ce paramètre et sa valeur ne sont pas inclus, la valeur par défaut est une liste vide.

Table des matières

Algorithm

Les valeurs acceptables incluent « LATEST_WITHIN_WINDOW » ou « RANDOM_WITHIN_WINDOW »

Type : String

Valeurs valides : LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW

Obligatoire : non

ExcludeVaults

Les valeurs acceptées incluent des sélecteurs spécifiques ARNs ou des listes de sélecteurs. La valeur par défaut est une liste vide si elle n'est pas répertoriée.

Type : tableau de chaînes

Obligatoire : non

IncludeVaults

Les valeurs acceptées incluent le caractère générique ["*"] ou le remplacement d'un caractère générique spécifique ARNs ou ARN ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf »,...] ["arn:aws:backup : *: *: backup-vault:asdf-* »,...]

Type : tableau de chaînes

Obligatoire : non

RecoveryPointTypes

Il s'agit des types de points de récupération.

Incluez SNAPSHOT pour restaurer uniquement les points de restauration des instantanés ; incluez CONTINUOUS pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de `Algorithm`.

Type : tableau de chaînes

Valeurs valides : CONTINUOUS | SNAPSHOT

Obligatoire : non

SelectionWindowDays

Les valeurs acceptées sont des entiers compris entre 1 et 365.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingSelectionForCreate

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration spécifique.

ProtectedResourceType est requis, comme Amazon EBS ou Amazon EC2.

Cela comprend RestoreTestingSelectionName, ProtectedResourceType et l'un des éléments suivants :

- ProtectedResourceArns
- ProtectedResourceConditions

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour ProtectedResourceArns avec ProtectedResourceConditions. Vous pouvez également inclure jusqu'à 30 ressources protégées spécifiques ARNs dans ProtectedResourceArns.

Des exemples ProtectedResourceConditions incluent StringEquals et StringNotEquals.

Table des matières

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de test de restauration ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Les types de ressources pris en charge incluent :

- Aurora pour Amazon Aurora
- DocumentDB pour Amazon DocumentDB (compatible avec MongoDB)
- DynamoDB pour Amazon DynamoDB

- EBS pour Amazon Elastic Block Store
- EC2 pour Amazon Elastic Compute Cloud
- EFS pour Amazon Elastic File System
- FSx pour Amazon FSx
- Neptune pour Amazon Neptune
- RDS pour Amazon Relational Database Service
- S3 pour Amazon S3

Type : Chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique de la sélection de tests de restauration appartenant au plan de test de restauration associé.

Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

Obligatoire : oui

ProtectedResourceArns

Chaque ressource protégée peut être filtrée en fonction de ses caractéristiques spécifiques ARNs, telles que `ProtectedResourceArns`: `["arn:aws:...", "arn:aws:..."]` ou par un caractère générique `:ProtectedResourceArns: ["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Si vous avez inclus le caractère générique `ProtectedResourceArns`, vous pouvez inclure des conditions de ressource, telles que `ProtectedResourceConditions`: `{ StringEquals: [{ key: "XXXX", value: "YYYY" } ]}`.

Type : objet [ProtectedResourceConditions](#)

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des [métadonnées déduites des tests de la restauration](#).

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Il s'agit du nombre d'heures (0 à 168) disponibles pour exécuter un script de validation sur les données. Les données seront supprimées à la fin du script de validation ou à la fin de la période de rétention spécifiée, selon la première éventualité.

Type : Integer

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingSelectionForGet

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

CreationTime

Date et heure de création d'une sélection de tests de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de ressources destinée à tester ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : Chaîne

Obligatoire : oui

RestoreTestingPlanName

`RestoreTestingPlanName` Il s'agit d'une chaîne unique qui est le nom du plan de test de restauration.

Type : Chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique de la sélection de tests de restauration appartenant au plan de test de restauration associé.

Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

Obligatoire : oui

CreatorRequestId

Cela identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un `CreatorRequestId` qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_ » caractères.

Type : chaîne

Obligatoire : non

ProtectedResourceArns

Vous pouvez inclure des éléments spécifiques ARNs, tels que, `ProtectedResourceArns` : `["arn:aws:...","arn:aws:..."]` ou vous pouvez inclure un caractère générique : `ProtectedResourceArns` : `["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Dans une sélection de tests de ressources, ce paramètre filtre en fonction de conditions spécifiques telles que `StringEquals` ou `StringNotEquals`.

Type : objet [ProtectedResourceConditions](#)

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des [métadonnées déduites des tests de la restauration](#).

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Il s'agit du nombre d'heures (1 à 168) disponibles pour exécuter un script de validation sur les données. Les données seront supprimées à la fin du script de validation ou à la fin de la période de rétention spécifiée, selon la première éventualité.

Type : Integer

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingSelectionForList

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

CreationTime

Date et heure de création d'une sélection de tests de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de test de restauration ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : Chaîne

Obligatoire : oui

RestoreTestingPlanName

Chaîne unique qui est le nom du plan de test de la restauration.

Le nom ne peut pas être modifié après la création. Le nom doit contenir uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique d'une sélection de tests de la restauration.

Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : Chaîne

Obligatoire : oui

ValidationWindowHours

Cette valeur représente la durée, en heures, pendant laquelle les données sont conservées après un test de la restauration afin que la validation facultative puisse être effectuée.

La valeur acceptée est un entier compris entre 0 et 168 (l'équivalent horaire de sept jours).

Type : Integer

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

RestoreTestingSelectionForUpdate

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

ProtectedResourceArns

Vous pouvez inclure une liste de caractères spécifiques ARNs, par exemple, `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` ou vous pouvez inclure un caractère générique `:ProtectedResourceArns: ["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Les conditions que vous définissez pour les ressources dans votre plan de test de restauration à l'aide de balises.

Type : objet [ProtectedResourceConditions](#)

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des [métadonnées déduites des tests de la restauration](#).

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Cette valeur représente la durée, en heures, pendant laquelle les données sont conservées après un test de la restauration afin que la validation facultative puisse être effectuée.

La valeur acceptée est un entier compris entre 0 et 168 (l'équivalent horaire de sept jours).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanAction

Service : AWS Backup

Définit une action d'analyse qui indique le scanner de programmes malveillants et le mode de scan à utiliser.

Table des matières

MalwareScanner

Le scanner de logiciels malveillants à utiliser pour l'action d'analyse. Actuellement, seul GUARDDUTY est pris en charge.

Type : Chaîne

Valeurs valides : GUARDDUTY

Obligatoire : non

ScanMode

Mode de numérisation à utiliser pour l'action de numérisation.

Valeurs valides : FULL_SCAN | INCREMENTAL_SCAN.

Type : Chaîne

Valeurs valides : FULL_SCAN | INCREMENTAL_SCAN

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanJob

Service : AWS Backup

Contient des métadonnées relatives à une tâche de numérisation, notamment des informations sur le processus de numérisation, les résultats et les ressources associées.

Table des matières

AccountId

L'ID du compte propriétaire de la tâche de numérisation.

Type : Chaîne

Obligatoire : oui

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : Chaîne

Obligatoire : oui

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : Chaîne

Obligatoire : oui

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de numérisation.

Type : objet [ScanJobCreator](#)

Obligatoire : oui

CreationDate

Date et heure de création d'une tâche de numérisation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer la tâche d'analyse ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : Chaîne

Obligatoire : oui

MalwareScanner

Moteur d'analyse utilisé pour la tâche de numérisation. Actuellement, seul GUARDDUTY est pris en charge.

Type : Chaîne

Valeurs valides : GUARDDUTY

Obligatoire : oui

RecoveryPointArn

Un ARN qui identifie de manière unique le point de récupération analysé ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : Chaîne

Obligatoire : oui

ResourceArn

Un ARN qui identifie de manière unique la ressource source du point de récupération en cours d'analyse.

Type : Chaîne

Obligatoire : oui

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : Chaîne

Obligatoire : oui

ResourceType

Type de AWS ressource analysée ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : Chaîne

Valeurs valides : EBS | EC2 | S3

Obligatoire : oui

ScanJobId

Identifiant unique qui identifie la demande de tâche de numérisation adressée à AWS Backup.

Type : Chaîne

Obligatoire : oui

ScanMode

Spécifie le type de numérisation utilisé pour la tâche de numérisation.

Comprend :

FULL_SCAN Analysera l'intégralité du lignage de données dans la sauvegarde.

INCREMENTAL_SCAN Analysera la différence de données entre le point de récupération cible et l'ARN du point de récupération de base.

Type : Chaîne

Valeurs valides : FULL_SCAN | INCREMENTAL_SCAN

Obligatoire : oui

ScannerRoleArn

Spécifie l'ARN du rôle IAM du scanner utilisé pour la tâche de numérisation.

Type : Chaîne

Obligatoire : oui

CompletionDate

Date et heure auxquelles une tâche de numérisation est terminée, au format Unix et en temps universel coordonné (UTC). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ScanBaseRecoveryPointArn

Un ARN qui identifie de manière unique le point de récupération de base à scanner. Ce champ est renseigné lorsqu'une tâche d'analyse incrémentielle a eu lieu.

Type : chaîne

Obligatoire : non

ScanId

ID de scan généré par le scanner de malwares pour la tâche d'analyse correspondante.

Type : chaîne

Obligatoire : non

ScanResult

Contient les informations relatives aux résultats de l'analyse, notamment l'état des menaces détectées lors de l'analyse.

Type : objet [ScanResultInfo](#)

Obligatoire : non

State

État actuel de la tâche de numérisation.

Valeurs valides : CREATED | RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Type : Chaîne

Valeurs valides : CANCELED | COMPLETED | COMPLETED_WITH_ISSUES | CREATED | FAILED | RUNNING

Obligatoire : non

StatusMessage

Un message détaillé expliquant l'état de la tâche de numérisation.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanJobCreator

Service : AWS Backup

Contient des informations d'identification relatives à la création d'une tâche d'analyse, notamment le plan de sauvegarde et la règle à l'origine de l'analyse.

Table des matières

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : Chaîne

Obligatoire : oui

BackupPlanId

ID du plan de sauvegarde.

Type : Chaîne

Obligatoire : oui

BackupPlanVersion

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. La version IDs ne peut pas être modifiée.

Type : Chaîne

Obligatoire : oui

BackupRuleId

Identifie de manière unique la règle de sauvegarde à l'origine de la tâche d'analyse.

Type : Chaîne

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanJobSummary

Service : AWS Backup

Contient des informations récapitulatives sur les tâches de numérisation, notamment les dénombrements et les métadonnées pour une période et des critères spécifiques.

Table des matières

AccountId

L'ID du compte auquel appartiennent les tâches de numérisation incluses dans ce résumé.

Type : Chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

Le nombre de tâches de numérisation correspondant aux critères spécifiés.

Type : Integer

Obligatoire : non

EndTime

La valeur de l'heure au format numérique de l'heure de fin d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

MalwareScanner

Spécifie le scanner de programmes malveillants utilisé lors de la tâche d'analyse. Actuellement, seuls les supports GUARDDUTY.

Type : Chaîne

Valeurs valides : GUARDDUTY

Obligatoire : non

Region

AWS Région dans laquelle les tâches de numérisation ont été exécutées.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource pour les tâches d'analyse incluses dans ce résumé.

Type : Chaîne

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

ScanResultStatus

État des résultats d'analyse pour les tâches d'analyse incluses dans ce résumé.

Valeurs valides : THREATS_FOUND | NO_THREATS_FOUND.

Type : Chaîne

Valeurs valides : NO_THREATS_FOUND | THREATS_FOUND

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

État des tâches de numérisation incluses dans ce résumé.

Valeurs valides : CREATED | RUNNING | COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED.

Type : Chaîne

Valeurs valides : CREATED | COMPLETED | COMPLETED_WITH_ISSUES | RUNNING | FAILED | CANCELED | AGGREGATE_ALL | ANY

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanResult

Service : AWS Backup

Contient les résultats d'une analyse de sécurité, y compris les informations du scanner, l'état de l'analyse et tout résultat découvert.

Table des matières

Findings

Un ensemble de résultats découverts lors de l'analyse.

Type : tableau de chaînes

Valeurs valides : MALWARE

Obligatoire : non

LastScanTimestamp

Horodatage de la dernière analyse, au format Unix et en temps universel coordonné (UTC).

Type : Timestamp

Obligatoire : non

MalwareScanner

Le scanner de logiciels malveillants utilisé pour effectuer l'analyse. Actuellement, seul GUARDDUTY est pris en charge.

Type : Chaîne

Valeurs valides : GUARDDUTY

Obligatoire : non

ScanJobState

État final de la tâche de numérisation.

Valeurs valides : COMPLETED | FAILED | CANCELED.

Type : Chaîne

Valeurs valides : COMPLETED | COMPLETED_WITH_ISSUES | FAILED | CANCELED

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanResultInfo

Service : AWS Backup

Contient des informations sur les résultats d'une tâche d'analyse.

Table des matières

ScanResultStatus

État des résultats de l'analyse.

Valeurs valides : THREATS_FOUND | NO_THREATS_FOUND.

Type : Chaîne

Valeurs valides : NO_THREATS_FOUND | THREATS_FOUND

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScanSetting

Service : AWS Backup

Contient les paramètres de configuration pour l'analyse des programmes malveillants, notamment le type de scanner, les types de ressources cibles et le rôle du scanner.

Table des matières

MalwareScanner

Le scanner de malwares à utiliser pour l'analyse. Actuellement, seul GUARDDUTY est pris en charge.

Type : Chaîne

Valeurs valides : GUARDDUTY

Obligatoire : non

ResourceTypes

Un ensemble de types de ressources à analyser pour détecter les logiciels malveillants.

Type : tableau de chaînes

Modèle : `^[a-zA-Z0-9\-\_\.\.]{1,50}$`

Obligatoire : non

ScannerRoleArn

Le nom de ressource Amazon (ARN) du rôle IAM que le scanner utilise pour accéder aux ressources ; par exemple, `arn:aws:iam::123456789012:role/ScannerRole`.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ScheduledPlanExecutionMember

Service : AWS Backup

Contient des informations sur l'exécution d'un plan de sauvegarde planifié, notamment l'heure d'exécution, le type de règle et l'identifiant de règle associé.

Table des matières

ExecutionTime

Horodatage auquel l'exécution de la sauvegarde est planifiée, au format Unix et en temps universel coordonné (UTC). La valeur est précise en millisecondes.

Type : Timestamp

Obligatoire : non

RuleExecutionType

Type d'exécution de la règle de sauvegarde. Les valeurs valides sont CONTINUOUS (point-in-time restauration), SNAPSHOTS (sauvegardes instantanées) ou CONTINUOUS_AND_SNAPSHOTS (les deux types combinés).

Type : String

Valeurs valides : CONTINUOUS | SNAPSHOTS | CONTINUOUS_AND_SNAPSHOTS

Obligatoire : non

RuleId

Identifiant unique de la règle de sauvegarde qui s'exécutera à l'heure planifiée.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TieringConfiguration

Service : AWS Backup

Il contient des métadonnées relatives à une configuration de hiérarchisation.

Table des matières

BackupVaultName

Nom du coffre de sauvegarde auquel s'applique la configuration de hiérarchisation. *À utiliser pour s'appliquer à tous les coffres-forts de sauvegarde.

Type : Chaîne

Modèle : `^(\* | [a-zA-Z0-9\-\_\ ]{2,50})$`

Obligatoire : oui

ResourceSelection

Tableau d'objets de sélection de ressources qui spécifient les ressources incluses dans la configuration de hiérarchisation et leurs paramètres de hiérarchisation.

Type : tableau d'objets [ResourceSelection](#)

Obligatoire : oui

TieringConfigurationName

Nom unique de la configuration de hiérarchisation. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : Chaîne

Modèle : `^[a-zA-Z0-9_\ ]{1,200}$`

Obligatoire : oui

CreationTime

Date et heure de création d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Il s'agit d'une chaîne unique qui identifie la demande et permet aux demandes ayant échoué d'être réessayées sans risquer d'exécuter l'opération deux fois.

Type : chaîne

Obligatoire : non

LastUpdatedTime

Date et heure de mise à jour d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de LastUpdatedTime est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

TieringConfigurationArn

Un Amazon Resource Name (ARN) qui identifie de manière unique la configuration de hiérarchisation.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TieringConfigurationInputForCreate

Service : AWS Backup

Il contient des métadonnées relatives à une configuration de hiérarchisation pour les opérations de création.

Table des matières

BackupVaultName

Nom du coffre de sauvegarde auquel s'applique la configuration de hiérarchisation. *À utiliser pour s'appliquer à tous les coffres-forts de sauvegarde.

Type : Chaîne

Modèle : `^(\\*|[a-zA-Z0-9\\-\\_]){2,50})$`

Obligatoire : oui

ResourceSelection

Tableau d'objets de sélection de ressources qui spécifient les ressources incluses dans la configuration de hiérarchisation et leurs paramètres de hiérarchisation.

Type : tableau d'objets [ResourceSelection](#)

Obligatoire : oui

TieringConfigurationName

Nom unique de la configuration de hiérarchisation. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : Chaîne

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TieringConfigurationInputForUpdate

Service : AWS Backup

Il contient des métadonnées relatives à une configuration hiérarchisée pour les opérations de mise à jour.

Table des matières

BackupVaultName

Nom du coffre de sauvegarde auquel s'applique la configuration de hiérarchisation. *À utiliser pour s'appliquer à tous les coffres-forts de sauvegarde.

Type : Chaîne

Modèle : `^(\*|[a-zA-Z0-9\-\_\]{2,50})$`

Obligatoire : oui

ResourceSelection

Tableau d'objets de sélection de ressources qui spécifient les ressources incluses dans la configuration de hiérarchisation et leurs paramètres de hiérarchisation.

Type : tableau d'objets [ResourceSelection](#)

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TieringConfigurationsListMember

Service : AWS Backup

Il contient des métadonnées relatives à une configuration de hiérarchisation renvoyées dans une liste.

Table des matières

BackupVaultName

Nom du coffre de sauvegarde auquel s'applique la configuration de hiérarchisation. *À utiliser pour s'appliquer à tous les coffres-forts de sauvegarde.

Type : Chaîne

Modèle : `^(\\*|[a-zA-Z0-9\\-\\_]){2,50})$`

Obligatoire : non

CreationTime

Date et heure de création d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastUpdatedTime

Date et heure de mise à jour d'une configuration de hiérarchisation, au format Unix et en temps universel coordonné (UTC). La valeur de `LastUpdatedTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

TieringConfigurationArn

Un Amazon Resource Name (ARN) qui identifie de manière unique la configuration de hiérarchisation.

Type : chaîne

Obligatoire : non

TieringConfigurationName

Nom unique de la configuration de hiérarchisation.

Type : Chaîne

Modèle : `^[a-zA-Z0-9_]{1,200}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

AWS Backup gateway

Les types de données suivants sont pris en charge par AWS Backup gateway :

- [BandwidthRateLimitInterval](#)
- [Gateway](#)
- [GatewayDetails](#)
- [Hypervisor](#)
- [HypervisorDetails](#)
- [MaintenanceStartTime](#)
- [Tag](#)
- [VirtualMachine](#)
- [VirtualMachineDetails](#)
- [VmwareTag](#)

- [VmwareToAwsTagMapping](#)

BandwidthRateLimitInterval

Service : AWS Backup gateway

Décrit un intervalle limite de débit de bande passante pour une passerelle. Une planification de limite de débit de la bande passante comprend un ou plusieurs intervalles de limite de débit de bande passante. Un intervalle de limite de bande passante définit une période pendant un ou plusieurs jours de la semaine, pendant laquelle des limites de débit de bande passante sont spécifiées pour le chargement, le téléchargement ou les deux.

Table des matières

DaysOfWeek

Composante des jours de la semaine de l'intervalle limite de débit de bande passante, représentée par des nombres ordinaux compris entre 0 et 6, où 0 représente le dimanche et 6 le samedi.

Type : tableau d'entiers

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 7 éléments.

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : oui

EndHourOfDay

Heure de la journée pendant laquelle l'intervalle de limite de débit de bande passante est terminé.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

EndMinuteOfHour

Minute de l'heure à laquelle l'intervalle de limite de débit de bande passante est terminé.

Important

L'intervalle de limite de taux de bande passante prend fin à la fin de la minute. Pour terminer un intervalle à la fin d'une heure, utilisez la valeur 59.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

StartHourOfDay

Heure de la journée pendant laquelle l'intervalle de limite de débit de bande passante commence.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

StartMinuteOfHour

Minute de l'heure à laquelle l'intervalle de limite de débit de bande passante commence.

L'intervalle commence au début de cette minute. Pour commencer un intervalle exactement au début de l'heure, utilisez la valeur 0.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

AverageUploadRateLimitInBitsPerSec

La composante limite du débit de téléchargement moyen de l'intervalle limite de débit de bande passante, en bits par seconde. Ce champ n'apparaît pas dans la réponse si la limite de débit de téléchargement n'est pas définie.

Type : long

Plage valide : valeur minimum de 51 200. Valeur maximale de 8 000 000 000 000.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Gateway

Service : AWS Backup gateway

Une passerelle est une appliance de AWS Backup passerelle qui s'exécute sur le réseau du client pour fournir une connectivité fluide au stockage des sauvegardes dans le AWS cloud.

Table des matières

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette `ListGateways` opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9]+){3}\/[a-zA-Z0-9]+`

Obligatoire : non

GatewayDisplayName

Le nom d'affichage de la passerelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[a-zA-Z0-9-]*`

Obligatoire : non

GatewayType

Le type de passerelle.

Type : String

Valeurs valides : `BACKUP_VM`

Obligatoire : non

HypervisorId

L'ID d'hyperviseur de la passerelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Obligatoire : non

LastSeenTime

La dernière fois que la AWS Backup passerelle a communiqué avec la passerelle, au format Unix et à l'heure UTC.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

GatewayDetails

Service : AWS Backup gateway

Les détails de la passerelle.

Table des matières

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez l'opération `ListGateways` pour renvoyer une liste des passerelles pour votre compte et la Région AWS.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z0-9+){3}\/[a-zA-Z0-9]+`

Obligatoire : non

GatewayDisplayName

Le nom d'affichage de la passerelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `[a-zA-Z0-9-]*`

Obligatoire : non

GatewayType

Type de passerelle.

Type : String

Valeurs valides : `BACKUP_VM`

Obligatoire : non

HypervisorId

L'ID d'hyperviseur de la passerelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Obligatoire : non

LastSeenTime

Détails indiquant la dernière fois que la AWS Backup passerelle a communiqué avec le cloud, au format Unix et à l'heure UTC.

Type : Timestamp

Obligatoire : non

MaintenanceStartTime

Renvoie l'heure de début de la maintenance hebdomadaire de votre passerelle, en particulier le jour et l'heure de la semaine. Notez que les valeurs sont exprimées en termes de fuseau horaire de la passerelle. Cela peut être hebdomadaire ou mensuel.

Type : objet [MaintenanceStartTime](#)

Obligatoire : non

NextUpdateAvailabilityTime

Détails indiquant l'heure de disponibilité de la prochaine mise à jour de la passerelle.

Type : Timestamp

Obligatoire : non

VpcEndpoint

Nom de DNS du point de terminaison du cloud privé virtuel (VPC) utilisé par la passerelle de sauvegarde pour se connecter au cloud.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Hypervisor

Service : AWS Backup gateway

Représente les autorisations de l'hyperviseur auxquelles la passerelle se connectera.

Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Table des matières

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : . +

Obligatoire : non

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]{3})\/[a-zA-Z-0-9]{+}`

Obligatoire : non

KmsKeyArn

Le nom de ressource Amazon (ARN) AWS Key Management Service utilisé pour chiffrer l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : (^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)\$)|(^alias/(\S+)\$)

Obligatoire : non

Name

Le nom de l'hyperviseur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

State

L'état de l'hyperviseur.

Type : String

Valeurs valides : PENDING | ONLINE | OFFLINE | ERROR

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

HypervisorDetails

Service : AWS Backup gateway

Il s'agit des détails de l'hyperviseur spécifié. Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Table des matières

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : .+

Obligatoire : non

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : non

KmsKeyArn

Amazon Resource Name (ARN) de la AWS KMS utilisée pour chiffrer l'hyperviseur.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)`

Obligatoire : non

LastSuccessfulMetadataSyncTime

Il s'agit de l'heure à laquelle la dernière synchronisation réussie des métadonnées a eu lieu.

Type : Timestamp

Obligatoire : non

LatestMetadataSyncStatus

Il s'agit du statut le plus récent pour la synchronisation des métadonnées indiquée.

Type : String

Valeurs valides : CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

Obligatoire : non

LatestMetadataSyncStatusMessage

Il s'agit du statut le plus récent pour la synchronisation des métadonnées indiquée.

Type : chaîne

Obligatoire : non

LogGroupArn

Amazon Resource Name (ARN) du groupe de passerelles dans le journal demandé.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : `$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*`

Obligatoire : non

Name

Il s'agit du nom de l'hyperviseur spécifié.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

State

Il s'agit de l'état actuel de l'hyperviseur spécifié.

Les états possibles sont PENDING, ONLINE, OFFLINE ou ERROR.

Type : String

Valeurs valides : PENDING | ONLINE | OFFLINE | ERROR

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

MaintenanceStartTime

Service : AWS Backup gateway

Il s'agit de l'heure de début de la maintenance hebdomadaire de votre passerelle, en particulier le jour et l'heure de la semaine. Notez que les valeurs sont exprimées en termes de fuseau horaire de la passerelle. Cela peut être hebdomadaire ou mensuel.

Table des matières

HourOfDay

La composante horaire de l'heure de début de la maintenance est représentée par hh, où hh est l'heure (0 à 23). L'heure du jour correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

MinuteOfHour

La composante des minutes de l'heure de début de la maintenance est représentée par mm, où mm est la minute (0 à 59). La minute de l'heure correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

DayOfMonth

Le composant jour du mois de l'heure de début de la maintenance est représenté sous la forme d'un nombre ordinal compris entre 1 et 28, où 1 représente le premier jour du mois et 28 le dernier jour du mois.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 31.

Obligatoire : non

DayOfWeek

Nombre ordinal compris entre 0 et 6 qui représente le jour de la semaine, où 0 représente le dimanche et 6 le samedi. Le jour de la semaine correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Tag

Service : AWS Backup gateway

Une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres UTF-8, les chiffres et les caractères suivants : + - = . _ : /. Les espaces ne sont pas autorisés dans les valeurs des balises.

Table des matières

Key

Élément clé dans la paire clé-valeur d'une balise. La clé ne peut pas commencer par aws : .

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : ([\p{L}\p{Z}\p{N}_.: /+=\ -@] *)

Obligatoire : oui

Value

Élément valeur dans la paire clé-valeur d'une balise.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : [^\x00] *

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

VirtualMachine

Service : AWS Backup gateway

Machine virtuelle sur un hyperviseur.

Table des matières

HostName

Le nom d'hôte de la machine virtuelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

HypervisorId

ID de l'hyperviseur de la machine virtuelle.

Type : chaîne

Obligatoire : non

LastBackupDate

Date de sauvegarde la plus récente d'une machine virtuelle, au format Unix et en heure UTC.

Type : Timestamp

Obligatoire : non

Name

Le nom de la machine virtuelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

Path

Le chemin de la machine virtuelle.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 4096.

Modèle : `[^\x00]+`

Obligatoire : non

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle. Par exemple, `arn:aws:backup-gateway:us-west-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

VirtualMachineDetails

Service : AWS Backup gateway

Vos VirtualMachine objets, classés par leur nom de ressource Amazon (ARNs).

Table des matières

HostName

Le nom d'hôte de la machine virtuelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

HypervisorId

ID de l'hyperviseur de la machine virtuelle.

Type : chaîne

Obligatoire : non

LastBackupDate

Date de sauvegarde la plus récente d'une machine virtuelle, au format Unix et en heure UTC.

Type : Timestamp

Obligatoire : non

Name

Le nom de la machine virtuelle.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : [a-zA-Z0-9-]*

Obligatoire : non

Path

Le chemin de la machine virtuelle.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 4096.

Modèle : `[^\x00]+`

Obligatoire : non

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle. Par exemple, `arn:aws:backup-gateway:us-west-1:0000000000000000:vm/vm-0000ABCDEFGHIJKL`.

Type : String

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+`

Obligatoire : non

VmwareTags

Il s'agit des détails des VMware balises associées à la machine virtuelle spécifiée.

Type : tableau d'objets [VmwareTag](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

VmwareTag

Service : AWS Backup gateway

Un VMware tag est un tag attaché à une machine virtuelle spécifique. Une [balise](#) est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources.

Le contenu des VMware balises peut être associé aux AWS balises.

Table des matières

VmwareCategory

C'est la catégorie de VMware.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : non

VmwareTagDescription

Il s'agit d'une description d'un VMware tag définie par l'utilisateur.

Type : chaîne

Obligatoire : non

VmwareTagName

Il s'agit du nom défini par l'utilisateur pour un VMware tag.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

VmwareToAwsTagMapping

Service : AWS Backup gateway

Cela affiche le mappage des VMware balises avec les AWS balises correspondantes.

Table des matières

AwsTagKey

L'élément clé de la paire clé-valeur de la AWS balise.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `(?!aws:)[\p{L}\p{Z}\p{N}_.: / = + \ - @ ] +`

Obligatoire : oui

AwsTagValue

La partie valeur de la paire clé-valeur de la AWS balise.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `[^\x00]*`

Obligatoire : oui

VmwareCategory

C'est la catégorie de VMware.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : oui

VmwareTagName

Il s'agit du nom défini par l'utilisateur pour un VMware tag.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

AWS Backup

Les types de données suivants sont pris en charge par AWS Backup :

- [BackupCreationTimeFilter](#)
- [CurrentSearchProgress](#)
- [EBSItemFilter](#)
- [EBSResultItem](#)
- [ExportJobSummary](#)
- [ExportSpecification](#)
- [ItemFilters](#)
- [LongCondition](#)
- [ResultItem](#)
- [S3ExportSpecification](#)
- [S3ItemFilter](#)
- [S3ResultItem](#)
- [SearchJobBackupsResult](#)
- [SearchJobSummary](#)
- [SearchScope](#)
- [SearchScopeSummary](#)
- [StringCondition](#)

- [TimeCondition](#)

BackupCreationTimeFilter

Service : AWS Backup

Cela filtre par points de récupération dans les CreatedBefore horodatages CreatedAfter et.

Table des matières

CreatedAfter

Cet horodatage inclut les points de récupération créés uniquement après l'heure spécifiée.

Type : Timestamp

Obligatoire : non

CreatedBefore

Cet horodatage inclut les points de récupération créés uniquement avant l'heure spécifiée.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

CurrentSearchProgress

Service : AWS Backup

Il contient les résultats d'information extraits d'une tâche de recherche qui n'a peut-être pas été terminée.

Table des matières

ItemsMatchedCount

Ce nombre est la somme de tous les éléments qui correspondent aux filtres d'éléments d'une tâche de recherche en cours.

Type : long

Obligatoire : non

ItemsScannedCount

Ce nombre est la somme de tous les éléments qui ont été scannés jusqu'à présent lors d'une recherche.

Type : long

Obligatoire : non

RecoveryPointsScannedCount

Ce nombre est la somme de toutes les sauvegardes qui ont été analysées jusqu'à présent lors d'une tâche de recherche.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour Ruby V3](#)

EBSItemFilter

Service : AWS Backup

Cela contient des tableaux d'objets, qui peuvent inclure des objets de conditions CreationTimes temporelles, des objets de FilePaths chaîne, des objets de conditions LastModificationTimes temporelles,

Table des matières

CreationTimes

Vous pouvez inclure de 1 à 10 valeurs.

Si un article est inclus, les résultats ne renverront que les éléments correspondants.

Si plusieurs éléments sont inclus, les résultats renverront tous les éléments correspondant à l'une des valeurs incluses.

Type : tableau d'objets [TimeCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

FilePaths

Vous pouvez inclure de 1 à 10 valeurs.

Si un chemin de fichier est inclus, les résultats ne renverront que les éléments correspondant au chemin du fichier.

Si plusieurs chemins de fichier sont inclus, les résultats renverront tous les éléments correspondant à l'un des chemins de fichier.

Type : tableau d'objets [StringCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

LastModificationTimes

Vous pouvez inclure de 1 à 10 valeurs.

Si un article est inclus, les résultats ne renverront que les éléments correspondants.

Si plusieurs éléments sont inclus, les résultats renverront tous les éléments correspondant à l'une des valeurs incluses.

Type : tableau d'objets [TimeCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

Sizes

Vous pouvez inclure de 1 à 10 valeurs.

Si un article est inclus, les résultats ne renverront que les éléments correspondants.

Si plusieurs éléments sont inclus, les résultats renverront tous les éléments correspondant à l'une des valeurs incluses.

Type : tableau d'objets [LongCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

EBSResultItem

Service : AWS Backup

Il s'agit des éléments renvoyés dans les résultats d'une recherche dans les métadonnées de sauvegarde Amazon EBS.

Table des matières

BackupResourceArn

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs du nom de ressource Amazon (ARN) des points de récupération renvoyés lors d'une recherche de métadonnées de sauvegarde Amazon EBS.

Type : chaîne

Obligatoire : non

BackupVaultName

Nom du coffre de sauvegarde.

Type : chaîne

Obligatoire : non

CreationTime

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs des heures de création renvoyées lors d'une recherche dans les métadonnées de sauvegarde Amazon EBS.

Type : Timestamp

Obligatoire : non

FilePath

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs des chemins de fichiers renvoyés lors d'une recherche dans les métadonnées de sauvegarde Amazon EBS.

Type : chaîne

Obligatoire : non

FileSize

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs de taille de fichier renvoyées lors d'une recherche dans les métadonnées de sauvegarde Amazon EBS.

Type : long

Obligatoire : non

FileSystemIdentifier

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs des systèmes de fichiers renvoyées lors d'une recherche de métadonnées de sauvegarde Amazon EBS.

Type : chaîne

Obligatoire : non

LastModifiedTime

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs de la dernière modification renvoyées lors d'une recherche dans les métadonnées de sauvegarde Amazon EBS.

Type : Timestamp

Obligatoire : non

SourceResourceArn

Il s'agit d'un ou de plusieurs éléments des résultats qui correspondent aux valeurs du nom de ressource Amazon (ARN) des ressources source renvoyées lors d'une recherche de métadonnées de sauvegarde Amazon EBS.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)

- [AWS SDK pour Ruby V3](#)

ExportJobSummary

Service : AWS Backup

Il s'agit du résumé d'une tâche d'exportation.

Table des matières

ExportJobIdentifier

Il s'agit de la chaîne unique qui identifie une tâche d'exportation spécifique.

Type : String

Obligatoire : oui

CompletionTime

Il s'agit d'un horodatage de l'heure à laquelle la tâche d'exportation s'est terminée.

Type : Timestamp

Obligatoire : non

CreationTime

Il s'agit d'un horodatage de l'heure à laquelle la tâche d'exportation a été créée.

Type : Timestamp

Obligatoire : non

ExportJobArn

Il s'agit de l'ARN (Amazon Resource Name) unique qui appartient à la nouvelle tâche d'exportation.

Type : chaîne

Obligatoire : non

SearchJobArn

Chaîne unique qui identifie le nom de ressource Amazon (ARN) de la tâche de recherche spécifiée.

Type : chaîne

Obligatoire : non

Status

Le statut de la tâche d'exportation est l'un des suivants :

CREATED; RUNNING FAILED ; ouCOMPLETED.

Type : String

Valeurs valides : RUNNING | FAILED | COMPLETED

Obligatoire : non

StatusMessage

Un message d'état est une chaîne renvoyée pour une tâche d'exportation.

Un message d'état est inclus pour tout statut autre que « COMPLETED sans problème ».

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ExportSpecification

Service : AWS Backup

Il contient l'objet de spécification d'exportation.

Table des matières

Important

Ce type de données est une UNION, de sorte qu'un seul des membres suivants peut être spécifié lorsqu'il est utilisé ou renvoyé.

s3ExportSpecification

Cela indique le compartiment Amazon S3 de destination pour la tâche d'exportation. Et, s'il est inclus, il indique également le préfixe de destination.

Type : objet [S3ExportSpecification](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ItemFilters

Service : AWS Backup

Les filtres d'éléments représentent toutes les propriétés des éléments d'entrée spécifiées lors de la création de la recherche.

Contient des EBSItem filtres ou S3 ItemFilters

Table des matières

EBSItemFilters

Ce tableau peut contenir des objets CreationTimes FilePaths, LastModificationTimes, ou Sizes.

Type : tableau d'objets [EBSItemFilter](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 10 éléments.

Obligatoire : non

S3ItemFilters

Ce tableau peut contenir des CreationTimes ETags, ObjectKeys, des tailles ou VersionIds des objets.

Type : tableau d'objets [S3ItemFilter](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 10 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

LongCondition

Service : AWS Backup

La condition longue contient un `Value` et peut éventuellement contenir un `Operator`.

Table des matières

Value

La valeur d'un élément inclus dans l'un des filtres d'éléments de recherche.

Type : long

Obligatoire : oui

Operator

Chaîne qui définit les valeurs qui seront renvoyées.

Si cela est inclus, évitez les combinaisons d'opérateurs qui renverront toutes les valeurs possibles. Par exemple, si vous incluez `EQUALS_TO` les deux `NOT_EQUALS_TO` avec la valeur de, toutes les valeurs 4 seront renvoyées.

Type : String

Valeurs valides : `EQUALS_TO` | `NOT_EQUALS_TO` | `LESS_THAN_EQUAL_TO` | `GREATER_THAN_EQUAL_TO`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ResultItem

Service : AWS Backup

Il s'agit d'un objet représentant l'élément renvoyé dans les résultats d'une recherche pour un type de ressource spécifique.

Table des matières

Important

Ce type de données est une UNION, de sorte qu'un seul des membres suivants peut être spécifié lorsqu'il est utilisé ou renvoyé.

EBSResultItem

Il s'agit d'articles renvoyés dans les résultats de recherche d'une recherche Amazon EBS.

Type : objet [EBSResultItem](#)

Obligatoire : non

S3ResultItem

Il s'agit d'éléments renvoyés dans les résultats de recherche d'une recherche Amazon S3.

Type : objet [S3ResultItem](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

S3ExportSpecification

Service : AWS Backup

Cette spécification contient une chaîne obligatoire du compartiment de destination ; vous pouvez éventuellement inclure le préfixe de destination.

Table des matières

DestinationBucket

Cela indique le compartiment Amazon S3 de destination pour la tâche d'exportation.

Type : String

Obligatoire : oui

DestinationPrefix

Cela spécifie le préfixe du compartiment Amazon S3 de destination pour la tâche d'exportation.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

S3ItemFilter

Service : AWS Backup

Il contient des tableaux d'objets, qui peuvent inclure des tailles ObjectKeys, CreationTimes VersionIds, et/ou des étiquettes.

Table des matières

CreationTimes

Vous pouvez inclure de 1 à 10 valeurs.

Si une valeur est incluse, les résultats ne renverront que les éléments correspondant à cette valeur.

Si plusieurs valeurs sont incluses, les résultats renverront tous les éléments correspondant à l'une des valeurs.

Type : tableau d'objets [TimeCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

ETags

Vous pouvez inclure de 1 à 10 valeurs.

Si une valeur est incluse, les résultats ne renverront que les éléments correspondant à cette valeur.

Si plusieurs valeurs sont incluses, les résultats renverront tous les éléments correspondant à l'une des valeurs.

Type : tableau d'objets [StringCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

ObjectKeys

Vous pouvez inclure de 1 à 10 valeurs.

Si une valeur est incluse, les résultats ne renverront que les éléments correspondant à cette valeur.

Si plusieurs valeurs sont incluses, les résultats renverront tous les éléments correspondant à l'une des valeurs.

Type : tableau d'objets [StringCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

Sizes

Vous pouvez inclure de 1 à 10 valeurs.

Si une valeur est incluse, les résultats ne renverront que les éléments correspondant à cette valeur.

Si plusieurs valeurs sont incluses, les résultats renverront tous les éléments correspondant à l'une des valeurs.

Type : tableau d'objets [LongCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

VersionIds

Vous pouvez inclure de 1 à 10 valeurs.

Si une valeur est incluse, les résultats ne renverront que les éléments correspondant à cette valeur.

Si plusieurs valeurs sont incluses, les résultats renverront tous les éléments correspondant à l'une des valeurs.

Type : tableau d'objets [StringCondition](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

S3ResultItem

Service : AWS Backup

Il s'agit des éléments renvoyés dans les résultats d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Table des matières

BackupResourceArn

Il s'agit d'éléments figurant dans les résultats renvoyés qui correspondent au point de restauration (ARN) saisi par Amazon Resource Names (ARN) lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : chaîne

Obligatoire : non

BackupVaultName

Nom du coffre de sauvegarde.

Type : chaîne

Obligatoire : non

CreationTime

Il s'agit d'un ou de plusieurs éléments figurant dans les résultats renvoyés qui correspondent aux valeurs d'heure de création des éléments saisies lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : Timestamp

Obligatoire : non

ETag

Il s'agit d'un ou de plusieurs éléments des résultats renvoyés qui correspondent aux valeurs à ETags saisis lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : chaîne

Obligatoire : non

ObjectKey

Il s'agit d'un ou de plusieurs éléments renvoyés dans les résultats d'une recherche dans les métadonnées de sauvegarde Amazon S3 qui correspondent aux valeurs saisies pour la clé d'objet.

Type : chaîne

Obligatoire : non

ObjectSize

Il s'agit d'éléments figurant dans les résultats renvoyés qui correspondent aux valeurs de taille (s) d'objet saisies lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : long

Obligatoire : non

SourceResourceArn

Il s'agit d'éléments figurant dans les résultats renvoyés qui correspondent à la source Amazon Resource Names (ARN) saisie lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : chaîne

Obligatoire : non

VersionId

Il s'agit d'un ou de plusieurs éléments des résultats renvoyés qui correspondent aux valeurs de IDs saisie de version lors d'une recherche dans les métadonnées de sauvegarde Amazon S3.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

SearchJobBackupsResult

Service : AWS Backup

Il contient les informations relatives aux points de récupération renvoyés dans les résultats d'une tâche de recherche.

Table des matières

BackupCreationTime

Il s'agit de l'heure de création de la sauvegarde (point de restauration).

Type : Timestamp

Obligatoire : non

BackupResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique les ressources de sauvegarde.

Type : chaîne

Obligatoire : non

IndexCreationTime

Il s'agit de l'heure de création de l'index de sauvegarde.

Type : Timestamp

Obligatoire : non

ResourceType

Il s'agit du type de ressource de la recherche.

Type : String

Valeurs valides : S3 | EBS

Obligatoire : non

SourceResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique les ressources sources.

Type : chaîne

Obligatoire : non

Status

Il s'agit de l'état du résultat de sauvegarde de la tâche de recherche.

Type : String

Valeurs valides : RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

Obligatoire : non

StatusMessage

Il s'agit du message d'état inclus dans les résultats.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

SearchJobSummary

Service : AWS Backup

Il s'agit d'informations relatives à une recherche d'emploi.

Table des matières

CompletionTime

Il s'agit de l'heure d'achèvement de la tâche de recherche.

Type : Timestamp

Obligatoire : non

CreationTime

Il s'agit de l'heure de création de la tâche de recherche.

Type : Timestamp

Obligatoire : non

Name

Il s'agit du nom de la tâche de recherche.

Type : chaîne

Obligatoire : non

SearchJobArn

Chaîne unique qui identifie le nom de ressource Amazon (ARN) de la tâche de recherche spécifiée.

Type : chaîne

Obligatoire : non

SearchJobIdentifier

Chaîne unique qui spécifie la tâche de recherche.

Type : chaîne

Obligatoire : non

SearchScopeSummary

Résumé renvoyé de l'étendue de la tâche de recherche spécifiée, y compris :

- TotalBackupsToScanCount, le nombre de points de récupération renvoyés par la recherche.
- TotalItemsToScanCount, le nombre d'éléments renvoyés par la recherche.

Type : objet [SearchScopeSummary](#)

Obligatoire : non

Status

Il s'agit de l'état de la tâche de recherche.

Type : String

Valeurs valides : RUNNING | COMPLETED | STOPPING | STOPPED | FAILED

Obligatoire : non

StatusMessage

Un message d'état sera renvoyé pour une tâche de recherche avec un statut de ERRORRED ou pour un statut de COMPLETED tâches présentant des problèmes.

Par exemple, un message peut indiquer qu'une recherche contient des points de récupération qui ne peuvent pas être analysés en raison d'un problème d'autorisation.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

SearchScope

Service : AWS Backup

L'étendue de la recherche comprend toutes les propriétés de sauvegarde saisies dans une recherche.

Table des matières

BackupResourceTypes

Les types de ressources inclus dans une recherche.

Les types de ressources éligibles incluent S3 et EBS.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Valeurs valides : S3 | EBS

Obligatoire : oui

BackupResourceArns

Le nom de ressource Amazon (ARN) qui identifie de manière unique les ressources de sauvegarde.

Type : tableau de chaînes

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

BackupResourceCreationTime

Il s'agit de l'heure à laquelle une ressource de sauvegarde a été créée.

Type : objet [BackupCreationTimeFilter](#)

Obligatoire : non

BackupResourceTags

Il s'agit d'une ou de plusieurs balises présentes sur la sauvegarde (point de restauration).

Type : mappage chaîne/chaîne

Obligatoire : non

SourceResourceArns

Le nom de ressource Amazon (ARN) qui identifie de manière unique les ressources sources.

Type : tableau de chaînes

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

SearchScopeSummary

Service : AWS Backup

Le résumé de l'étendue de la tâche de recherche spécifiée, y compris :

- TotalBackupsToScanCount, le nombre de points de récupération renvoyés par la recherche.
- TotalItemsToScanCount, le nombre d'éléments renvoyés par la recherche.

Table des matières

TotalItemsToScanCount

Il s'agit du nombre total d'éléments qui seront scannés lors d'une recherche.

Type : long

Obligatoire : non

TotalRecoveryPointsToScanCount

Il s'agit du nombre total de sauvegardes qui seront analysées lors d'une recherche.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

StringCondition

Service : AWS Backup

Il contient la valeur de la chaîne et peut contenir un ou plusieurs opérateurs.

Table des matières

Value

La valeur de la chaîne.

Type : String

Obligatoire : oui

Operator

Chaîne qui définit les valeurs qui seront renvoyées.

Si cela est inclus, évitez les combinaisons d'opérateurs qui renverront toutes les valeurs possibles. Par exemple, si vous incluez EQUALS_TO les deux NOT_EQUALS_TO avec la valeur de, toutes les valeurs 4 seront renvoyées.

Type : String

Valeurs valides : EQUALS_TO | NOT_EQUALS_TO | CONTAINS | DOES_NOT_CONTAIN | BEGINS_WITH | ENDS_WITH | DOES_NOT_BEGIN_WITH | DOES_NOT_END_WITH

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TimeCondition

Service : AWS Backup

Une condition temporelle indique l'heure de création, l'heure de la dernière modification ou une autre date.

Table des matières

Value

Il s'agit de la valeur d'horodatage de la condition temporelle.

Type : Timestamp

Obligatoire : oui

Operator

Chaîne qui définit les valeurs qui seront renvoyées.

Si cela est inclus, évitez les combinaisons d'opérateurs qui renverront toutes les valeurs possibles. Par exemple, si vous incluez EQUALS_TO les deux NOT_EQUALS_TO avec la valeur de, toutes les valeurs 4 seront renvoyées.

Type : String

Valeurs valides : EQUALS_TO | NOT_EQUALS_TO | LESS_THAN_EQUAL_TO | GREATER_THAN_EQUAL_TO

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des langages spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Paramètres communs

La liste suivante contient les paramètres que toutes les actions utilisent pour signer les demandes Signature Version 4 à l'aide d'une chaîne de requête. Tous les paramètres spécifiques d'une action particulière sont énumérées dans le sujet consacré à cette action. Pour plus d'informations sur la version 4 de Signature, consultez [la section Signing AWS API](#) du guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, exprimée dans le format YYYY-MM-DD.

Type : chaîne

Obligatoire : oui

X-Amz-Algorithm

Algorithme de hachage que vous avez utilisé pour créer la signature de la demande.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Valeurs valides : AWS4-HMAC-SHA256

Obligatoire : Conditionnelle

X-Amz-Credential

Valeur de la portée des informations d'identification, qui est une chaîne incluant votre clé d'accès, la date, la région cible, le service demandé et une chaîne de terminaison (« aws4_request »). Spécifiez la valeur au format suivant : access_key/AAAAMMJJ/région/service/aws4_request.

Pour plus d'informations, consultez la section [Création d'une demande d' AWS API signée](#) dans le guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Date

La date utilisée pour créer la signature. Le format doit être au format de base ISO 8601 (AAAAMMJJ'T'HHMMSS'Z'). Par exemple, la date et l'heure suivantes sont une X-Amz-Date valeur valide :20120325T120000Z.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour signer les demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date il n'est pas obligatoire. Lorsqu'il X-Amz-Date est utilisé, il remplace toujours la valeur de l'en-tête Date. Pour plus d'informations, consultez la section [Éléments d'une signature de demande d'AWS API](#) dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu par un appel à AWS Security Token Service (AWS STS). Pour obtenir la liste des services prenant en charge les informations d'identification de sécurité temporaires d' AWS STS, consultez [Services AWS qui fonctionnent avec IAM](#) dans le Guide de l'utilisateur IAM.

Condition : Si vous utilisez des informations d'identification de sécurité temporaires provenant de AWS STS, vous devez inclure le jeton de sécurité.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Signature

Spécifie la signature codée en hexadécimal qui a été calculée à partir de la chaîne à signer et de la clé de signature dérivée.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-SignedHeaders

Spécifie tous les en-têtes HTTP qui ont été inclus dans la demande canonique. Pour plus d'informations sur la spécification d'en-têtes signés, consultez la section [Créer une demande d'AWS API signée](#) dans le guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

Erreurs courantes

Cette section répertorie les erreurs communes aux actions d'API de tous les AWS services. Pour les erreurs spécifiques à une action d'API pour ce service, consultez la rubrique pour cette action d'API.

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 400

IncompleteSignature

La signature de la demande n'est pas conforme aux AWS normes.

Code d'état HTTP : 400

InternalFailure

Le traitement de la demande a échoué en raison d'une erreur, d'une exception ou d'un échec inconnu.

Code d'état HTTP : 500

InvalidAction

L'action ou l'opération demandée n'est pas valide. Vérifiez que l'action est entrée correctement.

Code d'état HTTP : 400

InvalidClientTokenId

Le certificat X.509 ou AWS l'ID de clé d'accès fourni n'existe pas dans nos archives.

Code d'état HTTP : 403

NotAuthorized

Vous ne disposez pas de l'autorisation nécessaire pour effectuer cette action.

Code d'état HTTP : 400

OptInRequired

L'ID de clé d' AWS accès nécessite un abonnement au service.

Code d'état HTTP : 403

RequestExpired

La demande est parvenue au service plus de 15 minutes après l'horodatage sur la demande ou plus de 15 minutes après la date d'expiration de la demande (par exemple pour les demandes pré-signées URLs), ou le horodatage sur la demande est daté dans plus de 15 minutes dans le futur.

Code d'état HTTP : 400

ServiceUnavailable

La requête a échoué en raison d'une défaillance temporaire du serveur.

HTTP Status Code: 503

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

Code d'état HTTP : 400

ValidationError

L'entrée ne satisfait pas les contraintes spécifiées par un AWS service.

Code d'état HTTP : 400

Historique du document pour AWS Backup

- Version de l'API : 19 novembre 2025
- Dernière mise à jour de la documentation : 19 novembre 2025

Le tableau suivant répertorie tous les AWS Backup lancements depuis le lancement du service en janvier 2019 jusqu'à aujourd'hui. Pour recevoir les notifications sur les mises à jour de cette documentation, vous pouvez vous abonner au flux RSS ci-dessus.

Modifier	Description	Date
Amazon GuardDuty Malware Protection pour AWS Backup	Amazon GuardDuty Malware Protection prend désormais en charge les sauvegardes EBS et S3 AWS Backup, en étendant les capacités de détection des malwares aux EC2 sauvegardes EBS et S3. Pour plus d'informations, consultez les pages de détail du produit.	19 novembre 2025
Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique AWSBackupGuardDutyRolePolicyForScans AWS gérée. Pour plus d'informations, consultez la section Politiques gérées pour AWS Backup.	19 novembre 2025
Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique AWSBackupServiceRolePolicyForScans AWS gérée.	19 novembre 2025

Modifier	Description	Date
	Pour plus d'informations, consultez la section Politiques gérées pour AWS Backup .	
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : • AWSBackupFullAccess • AWSBackupOperatorAccess Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	19 novembre 2025
Hiérarchisation des sauvegardes	AWS Backup introduit un niveau de stockage à chaud à faible coût pour les données de sauvegarde Amazon S3. Pour plus d'informations, consultez la section Hiérarchisation des sauvegardes.	18 novembre 2025

Modifier	Description	Date
Sauvegardes principales vers des coffres-forts à isolation logique	Logiquement, les coffres-forts ventilés sont désormais pris en charge en tant que cible de sauvegarde principale. Cette amélioration permet aux clients de tirer parti des avantages en matière de sécurité et de restauration des coffres-forts interconnectés de manière logique tout en ne conservant qu'une seule copie de sauvegarde, réduisant ainsi les coûts de stockage et d'exploitation. Auparavant, les coffres-forts à espace ment logique ne pouvaient stocker que des copies des sauvegardes existantes. Pour plus d'informations, consultez la section Sauvegardes principales vers des coffres-forts espacés de manière logique.	17 novembre 2025

Modifier	Description	Date
AWS Backup support pour les clusters Amazon Elastic Kubernetes Service	AWS Backup prend désormais en charge les clusters Amazon EKS. Les clients peuvent créer des sauvegardes et restaurer des points de restauration pour les clusters Amazon EKS et leurs ressources associées. Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par ressource et Mises à jour des politiques gérées pour AWS Backup.	10 novembre 2025

Modifier	Description	Date
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForRestores Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	10 novembre 2025
Support de coffre-fort ventilé de manière logique pour les clés gérées par le client AWS KMS	Les coffres-forts à espacement logique prennent désormais en charge le chiffrement à l'aide de clés gérées par le client. AWS KMS Pour plus d'informations, consultez la section Coffre-fort à espacement logique.	6 novembre 2025

Modifier	Description	Date
Prise en charge de la copie d'instantanés entre régions et entre comptes	Amazon RDS, Aurora, DocumentDB et Neptune prennent désormais en charge la copie d'instantanés entre régions et entre comptes en une seule action. Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par ressource.	23 octobre 2025
AWS Backup Extension du support régional pour Aurora DSQL	Le support de sauvegarde et de restauration Aurora DSQL est désormais disponible en Europe (Francfort). Pour plus d'informations, consultez les sections Services pris en charge par région et sauvegardes Aurora DSQL.	22 octobre 2025
AWS Backup Expansion régionale	AWS Backup, ainsi que bon nombre de ses fonctionnalités, est désormais disponible en Asie-Pacifique (Nouvelle Zélande). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	29 septembre 2025

Modifier	Description	Date
Amazon S3 (facultatif) ACLs et prise en charge de la sauvegarde des balises d'objet	AWS Backup prend désormais en charge l'exclusion facultative d'Amazon S3 ACLs et des balises d'objet, ce qui permet aux clients de réduire les coûts de sauvegarde. Pour plus d'informations, consultez Sauvegardes Amazon S3.	9 septembre 2025
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : • AWSBackupServiceLinkedRolePolicyForBackup Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	9 septembre 2025

Modifier	Description	Date
AWS Backup Audit Manager Expansion régionale	AWS Backup Audit Manager Les rapports interrégionaux et multicomptes sont désormais disponibles en plus Régions AWS, notamment en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Jakarta), en Asie-Pacifique (Melbourne), en Europe (Espagne), en Europe (Zurich) et au Moyen-Orient (Émirats arabes unis). Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par Région AWS et Création de plans de rapports.	5 septembre 2025
AWS Backup Support accru pour la restauration multirégionale Amazon Aurora DSQL	AWS Backup les utilisateurs peuvent désormais restaurer les clusters multirégionaux Aurora DSQL via la AWS Backup console ou via la CLI AWS Backup . Voir Restaurer un cluster multirégional Aurora DSQL pour plus d'informations.	29 juillet 2025

Modifier	Description	Date
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : • AWSBackupServiceRolePolicyForRestore Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	29 juillet 2025
AWS Backup support supplémentaire pour la restauration multirégionale Amazon Aurora DSQL Régions AWS	AWS Backup prend désormais en charge la restauration multirégionale Aurora DSQL en plus. Régions AWS Pour plus d'informations, consultez Restaurer un cluster multirégional Aurora DSQL et Services pris en charge par région.	3 juillet 2025

Modifier	Description	Date
AWS Backup fonctionnalité Expansion régionale	AWS Backup ajoute la prise en charge de la copie entre comptes et entre régions des sauvegardes Amazon S3 au sein AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Régions AWS Pour plus d'informations, consultez les sections Sauvegardes Amazon S3 et Sauvegarde et copie de balises.	26 juin 2025
AWS Backup support pour Amazon Aurora DSQL en Asie-Pacifique (Séoul)	AWS Backup supporte désormais Aurora DSQL en Asie-Pacifique (Séoul). Pour plus d'informations, consultez la section Services pris en charge par région.	26 juin 2025

Modifier	Description	Date
AWS Backup prise en charge de l'approbation multipartite	AWS Backup prend désormais en charge l'intégration optionnelle pour les coffres-forts à espacement logique afin d'utiliser l'approbation multipartite. Cette fonctionnalité est actuellement disponible pour les comptes situés dans l'est des États-Unis (Virginie du Nord). Pour en savoir plus, consultez : • Approbation multipartite pour les coffres-forts à espacement logique Guide de l'utilisateur pour l'approbation multipartite	17 juin 2025
AWS mise à jour des politiques gérées	AWS Backup a ajouté de nouvelles autorisations à la politique AWS gérée AWSBackupFullAccess. Pour plus d'informations et pour des modifications d'autorisation spécifiques, consultez les mises à jour des politiques.	17 juin 2025

Modifier	Description	Date
AWS Backup Audit Manager Expansion régionale	AWS Backup Audit Manager est désormais disponible en version supplémentaire Régions AWS, notamment : • Asie-Pacifique (Hyderabad) • Asie-Pacifique (Jakarta) • Asie-Pacifique (Melbourne) • Europe (Espagne) • Europe (Zurich) • Moyen-Orient (EAU) Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par région et Backup Audit Manager.	16 juin 2025
AWS Backup Expansion régionale	AWS Backup, ainsi que bon nombre de ses fonctionnalités, est désormais disponible en Asie-Pacifique (Taïpei) Région AWS. Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par région et Services pris en charge par région.	6 juin 2025

Modifier	Description	Date
Notification de l'index de sauvegarde et assistance aux événements	AWS Backup lance la prise en charge des notifications Amazon Simple Notification Service et des EventBridge événements Amazon pour les index de sauvegarde. AWS Backup la prise en charge des index de sauvegarde des notifications est disponible dans toutes les régions AWS commerciales et dans toutes les GovCloud régions où les index de sauvegarde, les réseaux sociaux et EventBridge les réseaux sociaux sont pris en charge. Pour plus d'informations, reportez-vous à la Notifications des utilisateurs console, à la EventBridge console, ainsi qu'à la recherche et à l'index des sauvegardes.	3 juin 2025

Modifier	Description	Date
Fonctionnalités supplémentaires pour Amazon EC2 Restore	Les configurations de volume peuvent être personnalisées lors d'une tâche de restauration. Vous pouvez définir des paramètres personnalisés pour les volumes Amazon EBS attachés à une EC2 AMI Amazon, notamment les métadonnées de restauration pour les mappages de périphériques en mode bloc. Pour plus d'informations, consultez Restore Amazon EC2 with AWS CLI et le guide de l'utilisateur d'Amazon Elastic Compute Cloud.	28 mai 2025

Modifier	Description	Date
AWS Backup prise en charge des clusters SQL Amazon Aurora	AWS Backup propose désormais une intégration avec Aurora DSQL dans plusieurs Régions AWS applications. Les clients peuvent créer des sauvegardes et restaurer des points de restauration pour les clusters Aurora DSQL à une ou plusieurs régions. Pour plus d'informations, consultez la restauration Amazon Aurora DSQL, la disponibilité des fonctionnalités par ressource et la gestion des clusters dans Aurora DSQL avec le. AWS CLI	27 mai 2025

Modifier	Description	Date
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : AWSBackupFullAccess , AWSBackupOperatorAccess , AWSBackupServiceLinkedRolePolicyForBackup , AWSBackupServiceRolePolicyForBackup , et AWSBackupServiceRolePolicyForRestores . Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	27 mai 2025
AWS Backup fonctionnalité Expansion régionale	AWS Backup la recherche est désormais disponible en Asie-Pacifique (Thaïlande), au Mexique (centre), (États-Unis de l'est) AWS GovCloud AWS GovCloud et (ouest des États-Unis). Régions AWS Pour plus d'informations, consultez Disponibilité des fonctionnalités par Région AWS et Recherche de sauvegardes.	22 avril 2025

Modifier	Description	Date
AWS Backup prise en charge des espaces de noms Amazon Redshift Serverless	Les clients ont désormais la possibilité de AWS Backup créer des sauvegardes instantanées manuelles Redshift Serverless et de les restaurer dans les espaces de noms Redshift Serverless. Pour plus d'informations, consultez la section Sauvegardes sans serveur Amazon Redshift.	31 mars 2025
Mise à jour de politiques gérées	AWS Backup a ajouté des autorisations supplémentaires aux politiques AWS gérées suivantes : • AWSBackupFullAccess • AWSBackupOperatorAccess • AWSBackupServiceLinkedRolePolicyForBackup • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForRestore Pour plus d'informations, consultez la section Mises à jour des politiques gérées pour AWS Backup.	31 mars 2025

Modifier	Description	Date
AWS Backup service soutenu Expansion régionale	AWS Backup le support FSx pour OpenZFS est désormais disponible dans les versions suivantes : Régions AWS • USA Ouest (Californie du Nord) • Afrique (Le Cap) • Asie-Pacifique (Hyderabad) • Asie-Pacifique (Jakarta) • Asie-Pacifique (Osaka) • Europe (Milan) • Europe (Paris) • Europe (Espagne) • Europe (Zurich) • Israël (Tel Aviv) • Middle East (Bahrain) • Moyen-Orient (EAU) • Amérique du Sud (São Paulo) Pour plus d'informations, consultez la section Services pris en charge par Régions AWS.	12 mars 2025

Modifier	Description	Date
Expansion des ressources du coffre logiquement espacée	Les points de restauration (sauvegardes) des ressources FSx pour Lustre, FSx pour Windows File Server et FSx pour OpenZFS peuvent désormais être copiés dans un coffre-fort isolé de manière logique. Pour en savoir plus, consultez : • Coffre-fort à isolation logique • Disponibilité des fonctionnalités par ressource	12 mars 2025
Nouvelle politique AWS gérée	AWS Backup a ajouté une nouvelle politique AWS gérée : AWSBackupSearchOperatorAccess. Pour plus d'informations, consultez AWSBackupSearchOperatorAccess le Guide des politiques AWS gérées.	27 février 2025

Modifier	Description	Date
AWS Backup Expansion régionale	AWS Backup, ainsi que bon nombre de ses fonctionnalités, est désormais disponible au Mexique (centre Région AWS). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	21 janvier 2025
AWS Backup Expansion régionale	AWS Backup, ainsi que bon nombre de ses fonctionnalités, est désormais disponible en Asie-Pacifique (Thaïlande). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	14 janvier 2025

Modifier	Description	Date
Mise à jour des stratégies gérées par AWS	AWS Backup a ajouté l'autorisation d'<code>rds:AddTagsToResource</code> accès à la politique gérée <code>AWSBackupServiceLinkedRolePolicyForBackup</code> . AWS Backup a ajouté les autorisations <code>rds:CreateTenantDatabase</code> et <code>rds>DeleteTenantDatabase</code> à la politique <code>AWSBackupServiceRolePolicyForRestores</code> . Pour plus d'informations, consultez la section Mises à jour des politiques.	8 janvier 2025
Support pour IPv6	AWS Backup prend désormais en charge les versions 6 (IPv6) et des protocoles Internet IPv4. Pour plus d'informations sur les fonctionnalités du double stack et les points de terminaison, consultez la section AWS Backup réseau.	18 décembre 2024

Modifier	Description	Date
AWS Backup service soutenu Expansion régionale	AWS Backup le support pour Amazon Timestream est désormais disponible AWS GovCloud en (ouest des États-Unis). Pour plus d'informations, consultez la section Services pris en charge par Régions AWS et les sauvegardes Amazon Timestream.	18 décembre 2024
Fonction de recherche ajoutée	AWS Backup introduit la possibilité de rechercher dans vos métadonnées de sauvegarde les propriétés au niveau des éléments afin de vous aider à trouver des points de récupération et d'autres fichiers ou objets que vous souhaitez restaurer. Voir Backup search pour plus de détails.	17 décembre 2024
Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique AWSBackupServiceRolePolicyForItemRestores AWS gérée. Pour plus d'informations, consultez la section Politiques gérées pour AWS Backup.	17 décembre 2024

Modifier	Description	Date
Ajout d'une nouvelle politique AWS gérée	AWS Backup a ajouté la politique AWSBackupServiceRolePolicyForIndexing AWS gérée. Pour plus d'informations, consultez la section Politiques gérées pour AWS Backup.	17 décembre 2024
AWS Backup fonctionnalité Expansion régionale	La gestion entre comptes pour surveiller les tâches de sauvegarde, de copie et de restauration par le biais AWS Backup de AWS Organizations l'intégration est désormais disponible Régions AWS lorsque l'inscription est requise. Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	12 décembre 2024
AWS Backup service soutenu Expansion régionale	AWS Backup le support pour Amazon Timestream est désormais disponible en Asie-Pacifique (Mumbai). Pour plus d'informations, consultez la section Services pris en charge par Régions AWS et les sauvegardes Amazon Timestream.	22 novembre 2024

Modifier	Description	Date
Fonctionnalités supplémentaires pour la restauration d'Amazon S3	AWS Backup ajoute une flexibilité supplémentaire lorsque vous restaurez des sauvegardes S3. Vous pouvez désormais restaurer des versions supplémentaires d'objets, y compris toutes les versions. Pour plus d'informations, consultez Restaurer les données S3 à l'aide de AWS Backup.	21 novembre 2024
AWS Backup fonctionnalité Expansion régionale	AWS Backup les clients peuvent désormais créer des copies interrégionales des sauvegardes Amazon Neptune dans un plus grand nombre de régions, notamment en Afrique (Le Cap), en Asie-Pacifique (Jakarta) et en Asie-Pacifique (Osaka). Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par région et Création de copies de sauvegarde dans toutes les régions Régions AWS.	13 novembre. 2024

Modifier	Description	Date
Expansion de copies entre régions	La copie interrégionale des sauvegardes Amazon S3 est désormais prise en charge Régions AWS lorsque l'opt-in est requis. Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par Région AWS.	13 novembre 2024
AWS Backup Audit Manager Expansion régionale	AWS Backup Audit Manager est désormais disponible Région AWS en Asie-Pacifique (Osaka). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région et Backup Audit Manager.	29 octobre 2024

Modifier	Description	Date
AWS Backup désormais disponible dans la région Asie-Pacifique (Malaisie)	La sauvegarde et la restauration de nombreux types de ressources sont désormais disponibles en Région AWS Asie-Pacifique (Malaisie). Pour connaître les fonctionnalités de sauvegarde compatibles, consultez la section Disponibilité des fonctionnalités par Région AWS. Pour les types de ressources pris en charge, consultez la section Services pris en charge par Région AWS.	10 octobre 2024
AWS Backup Contrôle Audit Manager pour un coffre-fort à espacement logique	AWS Backup Audit Manager propose désormais les ressources de contrôle dans un coffre à espacement logique pour aider à contrôler que les ressources ont été copiées dans un coffre-fort à espacement logique dans les délais spécifiés. Pour plus d'informations, consultez Contrôles et mesures correctives et Tests de restauration Audit.	12 septembre 2024

Modifier	Description	Date
AWS Backup fonctionnalité Expansion régionale	AWS Backup les clients peuvent désormais créer des copies interrégionales des sauvegardes Amazon Neptune dans un plus grand nombre de régions, notamment en Asie-Pacifique (Hong Kong), en Israël (Tel Aviv), au Moyen-Orient (Bahreïn) et au Moyen-Orient (Émirats arabes unis). Pour plus d'informations, consultez les sections Disponibilité des fonctionnalités par région et création de copies de sauvegarde pour chaque région Régions AWS.	29 août. 2024
AWS Backup prend en charge la copie entre régions et entre comptes pour les bases de données SAP HANA	Les utilisateurs qui ont sauvegardé des bases de données SAP HANA sur des EC2 instances Amazon peuvent désormais copier des instantanés à partir de sauvegardes complètes vers d'autres régions et d'autres comptes. Pour plus d'informations, consultez les bases de données SAP HANA sur les EC2 instances Amazon.	20 août 2024

Modifier	Description	Date
AWS Backup propose désormais un nouveau type de coffre-fort sécurisé	AWS Backup a introduit un type de coffre-fort secondaire pour le stockage des copies des sauvegardes. Les coffres-forts à espacement logique offrent des fonctionnalités de sécurité améliorées ainsi que la possibilité de partager l'accès aux coffres-forts avec les comptes via ce service. AWS RAM Pour plus d'informations, consultez la section Coffre-fort à espacement logique.	7 août 2024
AWS Backup fonctionnalité Expansion régionale	AWS Backup le support pour Amazon Simple Storage Service (Amazon S3) est désormais disponible dans l'ouest du Canada (Calgary). Les clients peuvent désormais sauvegarder et restaurer les ressources dans la région de l'Ouest du Canada (Calgary) . Pour plus d'informations sur la disponibilité dans la région AWS Backup Amazon S3, consultez la section Services pris en charge par Région AWS.	27 juin 2024
Fermeture d'aperçu du coffre logiquement espacée	Logiquement, l'aperçu du coffre-fort ventilé est terminé.	27 juin 2024

Modifier	Description	Date
AWS Backup fonctionnalité Expansion régionale	AWS Backup la prise en charge du niveau d'archivage des instantanés Amazon EBS est désormais disponible dans les régions suivantes : • Chine (Beijing) • Chine (Ningxia) • AWS GovCloud (US-Ouest) • AWS GovCloud (USA Est)	3 juin 2024
Mise à jour des stratégies gérées par AWS	AWS Backup autorisation ajoutée backup : TagResource pour les politiques gérées suivantes : • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForSauvegarde S3 • AWSBackupServiceLinkedRolePolicyForBackup Pour plus d'informations, consultez la section Mises à jour des politiques.	17 mai 2024

Modifier	Description	Date
AWS Backup maintenant disponible dans la région du Canada Ouest (Calgary)	La sauvegarde et la restauration de nombreux types de ressources sont désormais disponibles dans la Région AWS Canada-Ouest (Calgary). Pour connaître les fonctionnalités de sauvegarde compatibles, consultez la section Disponibilité des fonctionnalités par Région AWS. Pour les types de ressources pris en charge, consultez la section Services pris en charge par Région AWS.	14 mars 2024
Autorisations ajoutées à la politique gérée	AWS Backup a mis à jour la politique AWSServiceRolePolicyForBackupRestoreTesting en ajoutant des autorisations pour prendre en charge des types de ressources supplémentaires dans le cadre de la fonctionnalité de test de restauration. Pour plus d'informations sur les autorisations spécifiques ajoutées, consultez la section Mises à jour des politiques.	14 février 2024

Modifier	Description	Date
Support de sauvegarde et de restauration FSx pour les volumes ONTAP FlexGroup	AWS Backup prend désormais en charge la sauvegarde et la restauration FSx des FlexGroup volumes ONTAP dans la plupart des Régions AWS cas. Pour plus d'informations, consultez Restaurer un système de FSx fichiers Amazon.	10 janvier 2024
Support pour la sauvegarde et la restauration de SAP HANA HA	AWS Backup offre désormais un support aux bases de données SAP HANA High Availability sur Amazon EC2 Backup and Restore. Pour plus d'informations, consultez les sections EC2 Sauvegardes SAP HANA sur Amazon et restauration d'un système de haute disponibilité SAP HANA.	21 décembre 2023

Modifier	Description	Date
AWS Backup Contrôle Audit Manager pour les tests de restauration	AWS Backup Audit Manager permet désormais de contrôler le temps de restauration pour que les ressources atteignent l'objectif afin de faciliter le suivi des temps de restauration. Ce contrôle vérifie si le temps de restauration d'une ressource correspond à la durée cible. Pour plus d'informations, consultez Contrôles et mesures correctives et Tests de restauration Audit.	18 décembre 2023
Support pour le stockage à froid Amazon EBS	AWS Backup prend désormais en charge la transition des sauvegardes EBS d'un stockage à chaud vers un stockage à froid. Pour plus d'informations, consultez Amazon EBS Archive Tier pour le stockage à froidCycle de vie et niveaux de stockage, et Création d'un plan de sauvegarde.	27 novembre 2023

Modifier	Description	Date
Présentation des tests de la restauration	AWS Backup introduit les tests de restauration, qui permettent une évaluation automatique et périodique de la viabilité de la restauration, ainsi que la possibilité de surveiller la durée des tâches de restauration. Pour plus d'informations, consultez Tests de restauration.	27 novembre 2023

Modifier	Description	Date
Mise à jour des stratégies gérées par AWS	AWS Backup a ajouté les autorisations <code>ec2:DescribeSnapshotTierStatus</code> et <code>ec2:ModifySnapshotTier</code> aux politiques gérées AWSBackup <code>ServiceRolePolicyForBackups</code> et AWSBackup <code>ServiceLinkedRolePolicyForBackup</code>. AWS Backup a également ajouté les autorisations <code>ec2:DescribeSnapshotTierStatus</code> et <code>ec2:RestoreSnapshotTier</code> à la politique gérée AWSBackup <code>ServiceRolePolicyForRestores</code>. Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives et de restaurer les ressources depuis le niveau de stockage d'archives. Pour plus d'informations, consultez Mises à jour des politiques.	27 novembre 2023

Modifier	Description	Date
Ajout d'une autorisation de transmission de rôle pour prendre en charge les tests de la restauration.	AWS Backup ajoutés <code>restore-testing.backup.amazonaws.com</code> à <code>IamPassRolePermissions</code> et <code>IamCreateServiceLinkedRolePermissions</code> . Cet ajout est nécessaire pour AWS Backup effectuer des tests de restauration pour le compte des clients.	27 novembre 2023

Modifier	Description	Date
Ajout d'un nouveau rôle lié à un service	AWS Backup a ajouté le nouveau rôle lié au service nommé AWSServiceRoleForBackupRestoreTesting, qui fournit des autorisations de sauvegarde pour effectuer des tests de restauration. Ce nouveau rôle lié à un service fournit AWS Backup les autorisations nécessaires pour effectuer des tests de restauration. Les autorisations incluent les actions <code>list</code>, <code>read</code>, and <code>write</code> relatives aux services suivants à inclure dans les tests de restauration : Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon, EC2 Amazon EFS, pour Lustre, pour Windows File Server FSx , pour ONTAP FSx , pour OpenZFS FSx , Amazon Neptune, FSx Amazon RDS et Amazon S3.	27 novembre 2023

Modifier	Description	Date
Nouveau tableau de bord des métriques relatives aux tâches dans la AWS Backup console	La AWS Backup console affiche désormais un tableau de bord des tâches, simplifiant la surveillance de l'état des sauvegardes à grande échelle grâce à une nouvelle interface utilisateur visuelle et à des mesures agrégées de sauvegarde, de copie et de restauration pour les services pris en charge par AWS Backup. Le tableau de bord des offres d'emploi est disponible dans toutes les régions où AWS Backup Audit Manager est disponible. Les régions non répertoriées pourront toujours accéder au CloudWatch tableau de bord. Pour plus d'informations, consultez Tableaux de bord de la console AWS Backup.	15 novembre 2023

Modifier	Description	Date
Prise en charge des sauvegardes de piles imbriquées	AWS Backup a étendu sa prise en charge des sauvegardes de CloudFormation ressources. Vos piles CloudFormation d'applications contenant des piles imbriquées peuvent être incluses dans vos sauvegardes. Pour plus d'informations, consultez Sauvegardes de piles CloudFormation.	8 novembre 2023
Prise en charge d'Amazon S3 dans les régions Chine (Beijing) et Chine (Ningxia).	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	26 octobre 2023
Support pour les sauvegardes et Point-in-time restaurations continues d'Amazon Aurora	AWS Backup prend désormais en charge les sauvegardes et point-in-time restaurations continues (PITR) pour les ressources Aurora. Pour plus d'informations, consultez la section Sauvegardes et Point-in-time restaurations continues.	7 septembre 2023

Modifier	Description	Date
CloudFormation les piles soutiennent l'exclusion des ressources	AWS Backup prend désormais en charge l'option d'exclure les ressources choisies de votre CloudFormation pile. Pour plus d'informations, consultez Sauvegardes de piles CloudFormation.	6 septembre 2023
Les règles du plan de sauvegarde introduisent la flexibilité du fuseau horaire	AWS Backup les règles du plan peuvent désormais avoir un fuseau horaire spécifié pour les fenêtres de sauvegarde. Pour plus d'informations, consultez Gestion des plans de sauvegarde.	28 août 2023
AWS Backup désormais disponible dans la région Israël (Tel Aviv)	De nombreuses AWS Backup fonctionnalités sont désormais disponibles dans la nouvelle région d'Israël (Tel Aviv). Pour connaître les ressources prises en charge, consultez Disponibilité des fonctionnalités par Région AWS.	22 août 2023

Modifier	Description	Date
AWS Backup Audit Manager prend désormais en charge les comptes d'administrateurs délégués	AWS Backup La génération de rapports Audit Manager est désormais accessible par les comptes d'administrateurs délégués. Pour plus d'informations, consultez Audit des sauvegardes et création de rapports avec AWS Backup Audit Manager , Utilisation des rapports d'audit et Administrateur délégué .	16 août 2023
AWS Backup améliore les sauvegardes Amazon S3	AWS Backup dispose de capacités accrues en termes de performances, de taille et de rapidité pour les sauvegardes de compartiments S3. Pour plus d'informations, consultez Sauvegardes Amazon S3 .	1er août 2023
Fonctionnalité de restauration des balises désormais disponible dans les régions de Chine	Les balises qui font partie d'une sauvegarde peuvent désormais être copiées lorsque vous créez une tâche de restauration dans les régions Chine (Beijing) ou Chine (Ningxia). Pour plus d'informations, consultez Copie de balises lors d'une restauration .	17 juillet 2023

Modifier	Description	Date
AWS Backup prend désormais en charge Amazon S3 dans d'autres régions	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	6 juillet 2023
La copie entre comptes s'étend à d'autres régions	AWS Backup prend désormais en charge la copie de sauvegarde entre comptes de la plupart des ressources dans les régions suivantes : Asie-Pacifique (Jakarta), Moyen-Orient (Bahreïn), Asie-Pacifique (Hong Kong), Afrique (Le Cap), Europe (Milan), Asie-Pacifique (Osaka), Moyen-Orient (Émirats arabes unis), Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	5 juillet 2023

Modifier	Description	Date
Backup Audit Manager disponible dans GovCloud les régions	AWS Backup a étendu AWS Backup Audit Manager à AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	29 juin 2023
La gestion entre comptes est désormais disponible dans les régions GovCloud	AWS Backup prend désormais en charge la gestion intercomptes des ressources en AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Pour plus d'informations, consultez Gestion des ressources AWS Backup sur plusieurs comptes AWS.	29 juin 2023
Prise en charge des copies entre régions d'Amazon Aurora dans des régions supplémentaires	AWS Backup prend désormais en charge les copies de sauvegarde interrégionales pour les clusters Aurora à destination et en provenance des régions suivantes : Asie-Pacifique (Jakarta), Moyen-Orient (Bahreïn), Asie-Pacifique (Hong Kong), Afrique (Le Cap), Europe (Milan), Moyen-Orient (Émirats arabes unis), Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne).	5 juin 2023

Modifier	Description	Date
Copie des balises lors de la restauration	Les balises qui font partie d'une sauvegarde peuvent désormais être copiées lorsque vous créez une tâche de restauration. Pour plus d'informations, consultez Copie de balises lors d'une restauration.	22 mai 2023
AWS Backup s'intègre aux notifications AWS utilisateur	Vous pouvez désormais choisir de recevoir des notifications relatives aux événements de sauvegarde, de copie et de restauration via la console de notifications utilisateur AWS. Pour plus d'informations, voir Commencer à utiliser les notifications AWS utilisateur.	10 mai 2023
Sauvegardes entre régions disponibles dans quatre nouvelles régions	AWS Backup prend désormais en charge la sauvegarde interrégionale dans les régions du Moyen-Orient (Émirats arabes unis), de l'Europe (Espagne), de l'Europe (Zurich) et de l'Asie-Pacifique (Hyderabad).	28 avril 2023

Modifier	Description	Date
Support de AWS Backup copie étendu entre régions	Les sauvegardes interrégionales des ressources Amazon EFS et DynamoDB peuvent désormais être effectuées dans les régions suivantes : Asie-Pacifique (Jakarta), Moyen-Orient (Bahreïn), Asie-Pacifique (Hong Kong), Afrique (Le Cap) et Europe (Milan). VMware	28 avril 2023
Sauvegarde et restauration Amazon S3 dans la région Amérique du Sud (São Paulo)	AWS Backup le support pour Amazon S3 (Amazon Simple Storage Service) est désormais disponible dans la région Amérique du Sud (São Paulo). Pour plus d'informations, consultez Sauvegardes Amazon S3.	20 avril 2023
AWS Backup s'étend à la région Asie-Pacifique (Melbourne)	AWS Backup est désormais disponible dans la région Asie-Pacifique (Melbourne). Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par AWS région.	20 avril 2023

Modifier	Description	Date
Prise en charge régionale étendue pour Amazon S3	AWS Backup le support pour Amazon S3 (Amazon Simple Storage Service) est désormais disponible dans les AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest) Pour plus d'informations, consultez Sauvegardes Amazon S3.	19 avril 2023
Backup et restauration des bases de données SAP HANA sur les instances Amazon EC2	AWS Backup permet désormais de sauvegarder et de restaurer des bases de données SAP HANA exécutées sur des EC2 instances Amazon dans la plupart des régions. Pour plus d'informations, consultez la section Bases de données SAP HANA sur la sauvegarde EC2 des instances Amazon.	17 avril 2023

Modifier	Description	Date
AWS Backup désormais disponible dans les régions d'Europe (Espagne), d'Europe (Zurich) et d'Asie-Pacifique (Hyderabad)	AWS Backup le support s'est étendu à de nouvelles régions, notamment l'Europe (Espagne), l'Europe (Zurich) et l'Asie-Pacifique (Hyderabad). Les ressources prises en charge peuvent être sauvegardées et restaurées dans ces régions. Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par AWS région.	13 avril 2023
Politique AWS gérée mise à jour AWSBackupAuditAccess	Politique AWS gérée mise à jour AWSBackupAuditAccess. AWS Backup a remplacé la sélection de ressources dans l'API <code>config:DescribeComplianceByConfigRule</code> par une ressource générique. Pour plus d'informations, consultez Mises à jour de politiques pour AWS Backup.	11 avril 2023

Modifier	Description	Date
Hyperviseurs avec Amazon Logs CloudWatch	AWS Backup les utilisateurs de la passerelle peuvent désormais intégrer des hyperviseurs aux CloudWatch journaux pour gérer les journaux. Pour plus d'informations, reportez-vous aux sections Modification de la configuration d'un hyperviseur et CloudWatch Journaux .	29 mars 2023
Prise en charge régionale étendue pour Amazon S3	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions Asie-Pacifique (Jakarta) et Moyen-Orient (Émirats arabes unis).	22 mars 2023
Amélioration de la sauvegarde incrémentielle des machines virtuelles	VMware Les sauvegardes de machines virtuelles (machines virtuelles) présentant des problèmes de données CBT (Changed Block Tracking) contiennent désormais des informations supplémentaires pour aider à y remédier et à résoudre les problèmes. Pour plus d'informations, consultez Sauvegardes de machines virtuelles incrémentielles et Dépannage de vos machines virtuelles.	15 mars 2023

Modifier	Description	Date
AWS Backup prise en charge de plusieurs adaptateurs réseau	AWS Backup la passerelle prend désormais en charge la configuration de plusieurs adaptateurs réseau Pour plus d'informations sur la configuration de vos adaptateurs réseau, voir Configurer votre passerelle pour plusieurs NICs VMware dans le Guide du AWS Backup développeur.	8 mars 2023
AWS Backup prise en charge de vSphere 8	AWS Backup prend désormais en charge la sauvegarde et la restauration des machines virtuelles qui s'exécutent sur VMware vSphere 8. Pour plus d'informations sur les VMware options prises en charge, consultez Supportées VMs dans le guide du AWS Backup développeur.	8 mars 2023
AWS Backup Audit Manager prend en charge les sauvegardes Amazon RDS Multi-AZ	Backup Audit Manager prend désormais en charge les sauvegardes à plusieurs zones de disponibilité d'Amazon Relational Database Service. Pour plus d'informations, découvrez comment auditer les sauvegardes et créer des rapports avec AWS Backup Audit Manager.	1er février 2023

Modifier	Description	Date
AWS Backup propose une sauvegarde incrémentielle pour les tables Amazon Timestream	AWS Backup propose désormais des fonctionnalités de sauvegarde étendues pour les sauvegardes Timestream. Les plans de sauvegarde peuvent désormais prendre en charge des sauvegardes incrémentielles afin de réduire le temps nécessaire à la sauvegarde des ressources Timestream et les coûts de stockage. Pour plus d'informations, consultez Sauvegardes Amazon Timestream.	23 janvier 2023
AWS Backup désormais disponible à Dubaï	AWS Backup s'est étendu à la région du Moyen-Orient (EAU). Les ressources prises en charge peuvent être sauvegardées et restaurées dans cette région.	17 janvier 2023

Modifier	Description	Date
Copie entre régions disponible dans d'autres régions	AWS Backup propose désormais des sauvegardes interrégionales dans la région Asie-Pacifique (Jakarta), le Moyen-Orient (Bahreïn), la région Asie-Pacifique (Hong Kong), la région Afrique (Le Cap) et la région Europe (Milan) pour la plupart des ressources. Pour plus d'informations, consultez Création de copies de sauvegardes entre Régions AWS.	21 décembre 2022

Modifier	Description	Date
Limites et limitation de la bande passante de Backup Gateway	AWS Backup Gateway permet désormais de limiter le débit de téléchargement depuis les passerelles AWS Backup afin de contrôler la quantité de bande passante réseau utilisée par la passerelle. Pour prendre en charge cette fonctionnalité, AWS Backup a créé et mis à jour des politiques gérées, notamment <code>AWSSBackupFullAccess</code> et <code>AWSSBackupOperatorAccess</code>. Pour plus d'informations, consultez Limitation de la bande passante de Backup Gateway.	15 décembre 2022

Modifier	Description	Date
Support des VMware balises Backup Gateway	AWS Backup Gateway prend désormais en charge les VMware balises. Les utilisateurs ont la possibilité supplémentaire de créer des AWS balises correspondant aux balises utilisées pour les machines virtuelles. Pour prendre en charge cette fonctionnalité, AWS Backup a créé et mis à jour des politiques gérées <code>AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync</code> , notamment <code>AWSBackupFullAccess</code> , et <code>AWSBackupOperatorAccess</code> . Pour plus d'informations, consultez la section VMware Tags.	15 décembre 2022
AWS Backup support pour Amazon Timestream	AWS Backup prend désormais en charge la sauvegarde et la restauration des tables Amazon Timestream. Pour plus d'informations, consultez Sauvegardes Amazon Timestream.	13 décembre 2022

Modifier	Description	Date
AWS Backup offres Legal Hold	AWS Backup introduit un nouvel outil destiné à protéger les points de récupération grâce à une mise en détention légale. Pour plus d'informations, consultez Conservation légale .	27 novembre 2022
AWS Backup Audit Manager : rapports interrégionaux et multicomptes	AWS Backup Audit Manager apporte des fonctionnalités supplémentaires à la conformité et aux rapports de travail. Les utilisateurs peuvent générer des rapports incorporant plusieurs régions et comptes. Pour plus d'informations, consultez Utilisation des rapports d'audit .	27 novembre 2022
AWS Backup prend en charge Amazon Redshift	AWS Backup offre désormais un support pour la sauvegarde des clusters Amazon Redshift et pour la restauration des clusters et des tables Amazon Redshift. Pour plus d'informations, consultez la page Amazon Redshift backups (Sauvegardes Amazon Redshift).	27 novembre 2022

Modifier	Description	Date
AWS Backup prend en charge les piles d' AWS CloudFormation applications de sauvegarde	AWS Backup permet de sauvegarder CloudFormation et de restaurer des applications contenant plusieurs ressources en sauvegardant une pile et en restaurant les ressources qu'elle contient. Pour plus d'informations, consultez Sauvegardes de pile d'applications.	27 novembre 2022
AWS Backup propose des comptes d'administrateur délégués et une délégation des politiques de sauvegarde	AWS Backup les comptes inscrits AWS Organizations peuvent désigner les comptes des membres comme des comptes d'administrateur délégué. Pour plus d'informations, consultez la section Gestion de plusieurs comptes avec AWS Organizations.	27 novembre 2022

Modifier	Description	Date
Aperçu public de la sauvegarde et de la restauration de SAP HANA sur Amazon EC2 Instances	AWS Backup et AWS Backint proposent un aperçu public intégré des fonctionnalités de sauvegarde et de restauration des bases de données SAP HANA sur les EC2 instances. Pour plus d'informations, consultez notre version préliminaire publique de SAP HANA sur les EC2 instances Amazon. Pour soutenir cette version préliminaire, AWS Backup a fourni des mises à jour des politiques et de nouvelles politiques AWS gérées pour ces fonctionnalités.	20 novembre 2022

Modifier	Description	Date
Restaurer VMware sur des EC2 instances Amazon	AWS Backup offre désormais la possibilité de restaurer des machines virtuelles sur des EC2 instances Amazon, en plus de la possibilité de restaurer des machines sur EBS VMware, VMware Cloud on AWS et VMware Cloud on AWS Outposts. Pour plus d'informations, consultez la documentation sur l'utilisation de la AWS Backup console pour restaurer les points de restauration des machines virtuelles.	9 novembre 2022
Fonctionnalité étendue de AWS Backup Vault Lock	AWS Backup Vault Lock peut désormais être créé en mode gouvernance pour des protections IAM supplémentaires ou en mode conformité pour garantir l'immuabilité. En savoir plus sur AWS Backup Vault Lock.	4 octobre 2022

Modifier	Description	Date
AWS Backup Audit Manager est désormais disponible dans les régions Afrique (Le Cap) et Europe (Milan)	AWS Backup Audit Manager s'est étendu à la région Afrique (Le Cap) et à la région Europe (Milan). Pour plus d'informations sur Backup Audit Manager, consultez Audit les sauvegardes et création de rapports avec AWS Backup Audit Manager .	14 septembre 2022
AWS Backup intègre CloudWatch les métriques Amazon au tableau de bord de la console Backup	AWS Backup améliore le tableau de bord de sa console Backup afin d'afficher CloudWatch les métriques Amazon intégrées pour les tâches de sauvegarde et de restauration afin de renforcer les capacités de surveillance et de flexibilité.	8 septembre 2022
Prise en charge d'une flexibilité de chiffrement Amazon EBS supplémentaire lors de la restauration	AWS Backup propose désormais des options de chiffrement supplémentaires lors de la restauration des instantanés Amazon EBS.	1er septembre 2022
AWS Backup prend en charge la copie de sauvegarde entre comptes Amazon S3 et entre régions	AWS Backup propose désormais la copie de sauvegarde entre régions et entre comptes pour les sauvegardes Amazon S3. Pour plus d'informations, consultez Sauvegardes Amazon S3 .	28 juillet 2022

Modifier	Description	Date
AWS Backup Audit Manager offre un support de contrôle supplémentaire FSx pour ONTAP	AWS Backup Audit Manager propose désormais des contrôles supplémentaires FSx pour prendre en charge la surveillance et l'audit des volumes ONTAP, notamment l'inclusion des ressources de sauvegarde dans au moins un plan de sauvegarde et le dernier point de restauration créé. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	22 juillet 2022
AWS Backup ajoute la prise en charge de la sauvegarde et de la restauration des clusters multi-AZ Amazon RDS pour les clusters PostgreSQL et MySQL	AWS Backup a ajouté une option de sauvegarde et de restauration de clusters de zones de disponibilité multiples avec une instance de base de données principale et deux instances de base de données de secours lisibles. Pour en savoir plus, consultez Sauvegardes Amazon RDS Multi-AZ.	20 juillet 2022

Modifier	Description	Date
AWS Backup Audit Manager ajoute un nouveau contrôle pour la création de points de restauration	AWS Backup Audit Manager propose un nouveau contrôle d'audit pour une meilleure prise en charge de la conformité. Last recovery point created est un contrôle supplémentaire facultatif permettant de garantir que les points de récupération sont créés dans les délais spécifiés . Pour en savoir plus, consultez Contrôle créé par le dernier point de récupération.	29 juin 2022
Exemple de point de terminaison AWS Backup Gateway ajouté	AWS Backup Gateway a fourni un exemple de point de terminaison pour aider les utilisateurs à se connecter à VPNs (réseaux privés virtuels) .	14 juin 2022

Modifier	Description	Date
AWS Backup propose désormais des points de terminaison Amazon VPC pour VMware	AWS Backup prend désormais en charge les points de terminaison Amazon VPC pour VMware, ce qui vous permet d'utiliser un réseau privé virtuel entre vos VMware environnements et d'utiliser. AWS AWS PrivateLink Pour plus d'informations, consultez Création d'une passerelle et AWS Backup et AWS PrivateLink.	1er juin 2022
AWS Backup Audit Manager offre un support de contrôle supplémentaire pour Amazon S3	Backup Audit Manager prend désormais en charge le contrôle de conformité Ressources de sauvegarde protégées par des plans de sauvegarde pour les types de ressources S3. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	25 mai 2022

Modifier	Description	Date
AWS Backup Audit Manager offre un support de contrôle supplémentaire pour Storage Gateway	Backup Audit Manager prend désormais en charge le contrôle de conformité Ressources de sauvegarde protégées par des plans de sauvegarde pour les types de ressources Storage Gateway. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager .	25 mai 2022
Support d'Amazon FSx pour OpenZFS	AWS Backup offre désormais une gestion supplémentaire de la protection des données pour la sauvegarde et la restauration des systèmes FSx de fichiers OpenZFS.	18 mai 2022
AWS Backup Assistance d'Audit Manager pour VMware	AWS Backup fournit désormais un support pour les machines virtuelles dans les contrôles et les mesures correctives de Backup Audit Manager. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager .	11 mai 2022

Modifier	Description	Date
Amazon FSx est désormais pris en charge dans la région Asie-Pacifique (Osaka)	AWS Backup propose désormais la sauvegarde d'Amazon FSx dans la région Asie-Pacifique (Osaka) ainsi que des copies interrégionales à destination et en provenance de celle-ci.	26 avril 2022
Support pour Amazon FSx pour Lustre Persistent_2	AWS Backup offre désormais un support général pour Amazon FSx for Lustre, qui prend en charge des niveaux de débit par unité de stockage supérieurs à ceux des systèmes de fichiers Persistent_1.	5 avril 2022
VMware Améliorations	AWS Backup propose désormais la restauration sur Amazon EBS Volume, la restauration au niveau du disque et la prise en charge de VMware l' AWS Outposts activation. Pour plus d'informations, consultez Restauration d'une machine virtuelle .	31 mars 2022
AWS Backup Disponibilité pour l'Asie-Pacifique (Jakarta)	AWS Backup est désormais disponible pour les clients de la région Asie-Pacifique (Jakarta).	17 mars 2022

Modifier	Description	Date
Nouveaux contrôles pour AWS Backup Audit Manager	AWS Backup Audit Manager introduit trois nouveaux contrôles d'audit : la copie entre régions, la copie entre comptes et Backup Vault Lock. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager .	17 mars 2022
Support pour AWS PrivateLink	Avec AWS PrivateLink for AWS Backup, vous pouvez vous connecter directement à AWS Backup l'aide d'un point de terminaison d'interface dans votre VPC au lieu de vous connecter via l'Internet public. Les points de terminaison de l'interface sont directement accessibles depuis des applications qui se trouvent sur site ou dans une autre AWS région. Pour plus d'informations, consultez AWS Backup et AWS PrivateLink .	28 février 2022

Modifier	Description	Date
Prise en charge d'Amazon Simple Storage Service (Amazon S3)	La disponibilité générale de AWS Backup pour Amazon S3 Régions AWS est disponible dans tous les domaines sauf pour les régions Chine (Pékin), Chine (Ningxia), AWS GovCloud (ouest des États-Unis) et AWS GovCloud (est des États-Unis). Pour plus d'informations, consultez Utilisation avec des données Amazon S3 .	14 février 2022
Support pour la sauvegarde DynamoDB avancée dans les régions de Chine AWS	La sauvegarde DynamoDB avancée est désormais disponible dans les régions Chine (Beijing) et Chine (Ningxia). Pour plus d'informations, consultez Sauvegarde DynamoDB avancée .	18 janvier 2022
Version préliminaire publique de la prise en charge d'Amazon S3	AWS Backup propose un aperçu public des sauvegardes Amazon S3. Pour de plus amples informations, veuillez consulter Utilisation avec les données Amazon S3 .	30 novembre 2021

Modifier	Description	Date
Support pour les machines VMware virtuelles (VMs)	Vous pouvez désormais l'utiliser AWS Backup pour effectuer une sauvegarde automatique VMware VMs. Pour de plus amples informations, veuillez consulter Sauvegardes de machines virtuelles .	30 novembre 2021
Prise en charge de la sauvegarde DynamoDB avancée	Vous pouvez désormais utiliser AWS Backup les fonctionnalités suivantes pour toutes les nouvelles sauvegardes de tables DynamoDB que vous créez : hiérarchisation du stockage à froid, balisage de répartition des coûts, copie entre régions, copie entre comptes, chiffrement indépendant et copie de balises depuis les tables DynamoDB sources. Pour plus d'informations, consultez Sauvegarde DynamoDB avancée le guide du développeur Amazon DynamoDB et son utilisation avec AWS Backup DynamoDB.	23 novembre 2021

Modifier	Description	Date
Support à l'amélioration de l'affectation des AWS Backup ressources dans les régions de AWS Chine	AWS Backup l'amélioration de l'affectation des ressources est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez Affectation de ressources à un plan de sauvegarde .	16 novembre 2021
Lancement de l'amélioration de l'affectation des AWS Backup ressources	L'amélioration de l'attribution des ressources de sauvegarde vous offre des contrôles supplémentaires et précis ainsi que de nouveaux processus rationalisés pour déployer des plans de sauvegarde qui protègent des centaines de milliers de AWS ressources. Utilisez cette fonctionnalité pour plus de vitesse, de flexibilité et de précision lors de la protection des données avec AWS Backup. Pour plus d'informations, consultez Affectation de ressources à un plan de sauvegarde .	10 novembre 2021
Prise en charge d'Amazon Neptune	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder des clusters Amazon Neptune. Pour en savoir plus, consultez Qu'est-ce qu' AWS Backup ?	5 novembre 2021

Modifier	Description	Date
Prise en charge d'Amazon DocumentDB	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder des clusters Amazon DocumentDB. Pour en savoir plus, consultez Qu'est-ce qu' AWS Backup ?	5 novembre 2021
Support pour AWS Backup Vault Lock dans les régions de AWS Chine	AWS Backup Vault Lock est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez AWS Backup Vault Lock .	03 novembre 2021
Lancement de AWS Backup Vault Lock	Avec AWS Backup Vault Lock, vous pouvez empêcher la suppression des sauvegardes stockées dans un coffre-fort AWS Backup de sauvegarde. Pour plus d'informations, consultez AWS Backup Vault Lock .	7 octobre 2021
Lancement des rapports de conformité AWS Backup d'Audit Manager	Grâce aux rapports de conformité, vous pouvez générer des rapports quotidiens sur la conformité de votre activité de sauvegarde et de vos ressources par rapport aux contrôles que vous avez définis dans vos frameworks AWS Backup Audit Manager. Pour plus d'informations, consultez Modèles de rapport de conformité .	5 octobre 2021

Modifier	Description	Date
CloudFormation support pour AWS Backup Audit Manager	Avec CloudFormation, vous pouvez désormais déployer les frameworks, les contrôles et les plans de rapports d'AWS Backup Audit Manager de manière sûre et reproductible à grande échelle. Pour plus d'informations, consultez la section Audit et rapports de sauvegarde avec AWS Backup Audit Manager .	4 octobre 2021
Lancement d' AWS Backup Audit Manager	Avec AWS Backup Audit Manager, vous pouvez désormais définir des contrôles pour votre activité et vos ressources de sauvegarde, et identifier les activités et les ressources qui ne sont pas conformes à vos contrôles . Vous pouvez également utiliser AWS Backup Audit Manager pour générer des rapports quotidiens et à la demande qui prouvent la conformité avec les contrôles que vous avez définis au fil du temps. Pour plus d'informations, consultez la section Audit et rapports de sauvegarde avec AWS Backup Audit Manager .	24 août 2021

Modifier	Description	Date
Prise en charge de nouvelles opérations de point de récupération asynchrones	AWS Backup assume désormais un rôle lié au service pour gérer les règles du cycle de vie de vos sauvegardes au cas où vous modifieriez ou supprimeriez votre rôle IAM d'origine. Pour plus d'informations, consultez Suppression des sauvegardes .	23 août 2021
Prise en charge de sauvegardes multi-volumes en cas de panne sur Amazon EBS	Désormais, lorsque vous protégez AWS Backup vos EC2 instances Amazon, vous effectuez des AWS Backup sauvegardes multivolumes cohérentes en cas de crash de tous les volumes Amazon EBS attachés à chaque instance Amazon par défaut. EC2 Pour plus d'informations, consultez Création d'une sauvegarde Amazon EBS multi-volume en cas de panne .	14 juin 2021

Modifier	Description	Date
Support supplémentaire pour Amazon FSx Régions AWS	Vous pouvez désormais les utiliser AWS Backup pour protéger vos systèmes de FSx fichiers Amazon dans les régions suivantes : AWS GovCloud (US) région Europe (Milan), région Afrique (Le Cap) et région du Moyen-Orient (Bahreïn). Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	15 avril 2021

Modifier	Description	Date
Support pour les sauvegardes FSx entre régions et comptes Amazon	Vous pouvez désormais les utiliser AWS Backup pour copier des FSx sauvegardes Amazon sur des comptes Régions AWS et des comptes. Pour plus d'informations, consultez Création d'une copie de sauvegarde. Si vous utilisez des politiques gérées par le client, vous devez ajouter la nouvelle autorisation <code>fsx:CopyBackup</code> pour éviter l'échec des tâches de sauvegarde existantes. Pour obtenir cette autorisation, consultez la dernière déclaration de la politique de FSx sauvegarde d'Amazon dans les politiques gérées par le client.	12 avril 2021
Prise en charge des balises de répartition des coûts pour les sauvegardes Amazon EFS	Vous pouvez désormais utiliser des balises de répartition des coûts pour suivre les coûts de vos sauvegardes Amazon EFS de manière détaillée, ainsi que pour afficher et filtrer ces balises à l'aide de ces balises AWS Cost Explorer. Pour plus d'informations, consultez Utilisation des balises de répartition des coûts.	7 avril 2021

Modifier	Description	Date
Autorisation de FedRAMP High	AWS Backup est désormais autorisé à prendre en charge les charges de travail élevées de FedRAMP. Pour plus d'informations, consultez les Services AWS concernés par le programme de conformité .	25 mars 2021
Nouveau Région AWS	AWS Backup est désormais disponible dans la région Asie-Pacifique (Osaka). Dans cette région, Storage Gateway, Amazon FSx et la sauvegarde entre comptes ne sont AWS Backup actuellement pas pris en charge dans cette région. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	25 mars 2021
Prise en charge des opérations par lots du point de récupération	Vous pouvez désormais utiliser la AWS Backup console pour automatiser les opérations par lots afin de nettoyer les points de restauration dans vos coffres-forts de sauvegarde. Pour plus d'informations, consultez Suppression des sauvegardes .	23 mars 2021

Modifier	Description	Date
Prise en charge des restaurations vers la classe de stockage Amazon EFS One Zone	Vous pouvez désormais restaurer vos sauvegardes Amazon EFS dans la classe de stockage Amazon EFS One Zone. Pour plus d'informations, consultez Restauration d'un système de fichiers Amazon EFS .	12 mars 2021
Support pour la restauration et la sauvegarde continue d'Amazon Relational Database point-in-time Service	Vous pouvez désormais utiliser AWS Backup pour automatiser les sauvegardes continues d'Amazon RDS et effectuer des point-in-time restaurations (PITR), en plus d'orchestrer vos sauvegardes de snapshots. Pour plus d'informations, voir Restauration à une heure spécifiée à l'aide de point-in-time la restauration .	10 mars 2021
Support pour Amazon CloudWatch	Vous pouvez désormais utiliser CloudWatch pour surveiller AWS Backup les métriques. Pour plus d'informations, consultez la section Surveillance des événements et des mesures avec Amazon CloudWatch et Amazon EventBridge .	3 février 2021

Modifier	Description	Date
Support pour Amazon EventBridge	Vous pouvez désormais l'utiliser EventBridge pour surveiller les AWS Backup événements. Pour plus d'informations, consultez la section Surveillance des événements et des mesures avec Amazon CloudWatch et Amazon EventBridge .	3 février 2021
Prise en charge des sauvegardes entre comptes	Vous pouvez désormais l'AWS Backup utiliser pour sauvegarder vos ressources sur plusieurs Comptes AWS. Pour plus d'informations, consultez la section Création de copies de sauvegarde entre AWS comptes .	18 novembre 2020
Support pour la sauvegarde et la restauration des systèmes de FSx fichiers Amazon	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder les systèmes de FSx fichiers Amazon. Pour plus d'informations, consultez Travailler avec les systèmes de FSx fichiers Amazon .	9 novembre 2020
Nouveau Régions AWS	AWS Backup est désormais disponible en Afrique (Le Cap) et en Europe (Milan) Régions AWS. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	21 octobre 2020

Modifier	Description	Date
Prise en charge de la sauvegarde Windows compatible avec VSS	Vous pouvez désormais sauvegarder et restaurer les applications Windows compatibles VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2 . Pour plus d'informations, consultez Création de sauvegardes Windows VSS .	22 septembre 2020
Prise en charge de la sauvegarde automatique d'Amazon EFS	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder automatiquement les systèmes de fichiers Amazon EFS. Pour plus d'informations, consultez Mise en route 4 : création de sauvegardes automatiques Amazon EFS .	16 juillet 2020
Nouveau Région AWS	AWS Backup est désormais disponible dans le AWS GovCloud (US) Region. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	24 juin 2020

Modifier	Description	Date
Support pour la gestion des sauvegardes sur plusieurs Comptes AWS	Vous pouvez désormais gérer les sauvegardes sur plusieurs Comptes AWS en utilisant AWS Organizations . Pour de plus amples informations, veuillez consulter Fonctionnement de la gestion inter-comptes .	24 juin 2020
Support pour Amazon Aurora ajouté à AWS Backup	Vous pouvez désormais configurer AWS Backup pour sauvegarder les ressources d'Amazon Aurora. Pour plus d'informations, consultez Présentation de la sauvegarde et de la restauration d'un cluster de bases de données Aurora dans le Guide de l'utilisateur Amazon Aurora.	10 juin 2020
Support pour la configuration des services à utiliser AWS Backup	Vous pouvez désormais configurer AWS Backup pour sauvegarder les ressources de AWS services spécifiques. Pour plus d'informations, voir Activer la gestion des services avec AWS Backup .	20 mai 2020

Modifier	Description	Date
Support pour la sauvegarde des EC2 instances Amazon et ajout de la prise en charge de la sauvegarde entre régions	Vous pouvez désormais sauvegarder des EC2 instances Amazon entières et également y copier des ressources Régions AWS. Pour plus d'informations, consultez Création de copies de sauvegardes entre Régions AWS .	13 janvier 2020
Nouveau guide	AWS AWS Backup les lancements et le guide du AWS Backup développeur.	15 janvier 2019

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.