



Guide d'administration

AWS Directory Service



Version 1.0

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directory Service: Guide d'administration

Copyright © 2025 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 Directory Service ?	1
AWS Directory Service options	1
Que choisir ?	5
Travailler avec Amazon EC2	6
AWS Microsoft AD géré	7
Lequel choisir ?	8
Rubriques	8
AWS Microsoft AD géré (édition hybride)	9
Conditions préalables requises pour un annuaire hybride	10
Création d'un annuaire hybride	18
Afficher et modifier un répertoire hybride	19
Supprimer un répertoire hybride	21
Évaluations des annuaires	22
Résolution de problème	26
Mise en route	63
AWS Conditions préalables à la gestion de Microsoft AD	64
AWS IAM Identity Center prérequis	65
Prérequis pour l'authentification multifactorielle	65
Création de votre AWS compte Microsoft AD géré	66
Qu'est-ce qui est créé avec votre Microsoft AD AWS géré	69
Compte administrateur et autorisations de groupe	81
Concepts clés et meilleures pratiques	84
Concepts clés	85
Bonnes pratiques	89
Cas d'utilisation	100
Cas d'utilisation 1 : connectez-vous aux AWS applications et aux services avec des informations d'identification Active Directory	101
Cas d'utilisation 2 : gestion EC2 des instances Amazon	106
Cas d'utilisation 3 : fournir des services d'annuaire à vos charges de travail compatibles avec Active Directory	106
Cas d'utilisation 4 : AWS IAM Identity Center vers Office 365 et d'autres applications cloud	106
Cas d'utilisation 5 : étendez votre Active Directory local au AWS Cloud	107

Cas d'utilisation 6 : partagez votre annuaire pour associer facilement EC2 des instances Amazon à un domaine sur plusieurs AWS comptes	107
Maintenance de votre annuaire	108
Affichage des informations du répertoire	109
Restauration de votre répertoire à l'aide de snapshots	111
Déploiement de contrôleurs de domaine supplémentaires	117
Mise à niveau de votre Microsoft AD AWS géré	122
Mise à jour du type de réseau d'annuaire	124
Ajouter d'autres suffixes UPN	126
Renommer le nom du site de votre annuaire	126
Suppression de votre Microsoft AD AWS géré	127
Sécuriser votre annuaire	129
Comprendre les politiques de mots de passe	130
Activation de l'authentification multi-facteurs	136
Activer le protocole LDAP ou LDAPS sécurisé	140
Gestion de la conformité de votre annuaire	154
Améliorer la sécurité du réseau	156
Modification des paramètres de sécurité du répertoire	172
Activer le chiffrement à clé publique pour l'authentification initiale (PKINIT)	185
Configurer le AWS CA privée connecteur pour AD	188
Surveillance de votre annuaire	194
Comprendre le statut de votre annuaire	195
Activation des notifications d'état des annuaires avec Amazon SNS	197
Comprendre les journaux de votre annuaire	200
Activation du transfert de CloudWatch journaux Amazon	202
Utilisation CloudWatch pour surveiller votre annuaire	206
Désactiver le transfert de CloudWatch journaux Amazon	210
Surveillance du serveur DNS avec Microsoft Event Viewer	211
Accès aux AWS applications et aux services	212
Compatibilité des applications	212
Permettre l'accès aux AWS applications et aux services	215
Permettre l'accès au AWS Management Console	218
Création d'une URL d'accès	221
Activation de l'authentification unique	222
Octroi de l'accès aux AWS ressources	231
Création d'un rôle	232

Modification de la relation d'approbation pour un rôle existant	233
Attribution d'utilisateurs et de groupes à un rôle existant	234
Affichage des utilisateurs et groupes attribués à un rôle	236
Suppression d'un utilisateur ou d'un groupe d'un rôle	237
Utilisation de politiques AWS gérées	238
Configuration de la réplication multirégionale	239
Comment ça marche	240
Avantages	243
Caractéristiques mondiales et régionales	243
Régions principales et régions supplémentaires	244
Ajouter une région répliquée	245
Supprimer une région répliquée	248
Partagez votre annuaire	249
Concepts clés	249
Considérations	251
Tutoriel : Partagez votre répertoire Microsoft AD AWS géré	252
Annulation du partage de votre répertoire	264
Migration des utilisateurs d'Active Directory vers AWS Managed Microsoft AD	265
Connectez votre infrastructure Active Directory existante	265
Création d'une relation d'approbation	266
Ajout de routes IP	273
Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.	273
Tutoriel : Création d'une relation de confiance entre les domaines Microsoft AD AWS gérés	285
Étendez le schéma de votre répertoire	292
Quand étendre votre schéma AWS Managed Microsoft AD	292
Tutoriel : extension de votre schéma Microsoft AD AWS géré	293
Méthodes pour joindre une instance à votre annuaire	300
Lancement d'une instance d'administration d'annuaire	301
Rejoindre une instance Windows	304
Rejoindre une instance Linux	313
Rejoindre une instance Mac	368
Délégation des privilèges d'adhésion à un annuaire	371
Création ou modification d'un ensemble d'options DHCP	373
Gestion des utilisateurs et des groupes	375

AWS Management Console	376
AWS CLI	377
Outils AWS pour PowerShell	378
Instance sur site ou Amazon EC2	378
Gérez les utilisateurs et les groupes à l'aide de la console, de la CLI ou PowerShell	379
Gérez les utilisateurs et les groupes avec une EC2 instance Amazon	424
Données du service de répertoire	436
Réplication et cohérence	437
AWS Attributs des données du service de répertoire	438
Type de groupe et étendue du groupe	444
Connexion à Microsoft Entra Connect Sync	446
Prérequis	446
Création d'un utilisateur de domaine Active Directory	447
Télécharger Entra Connect Sync	447
Exécuter PowerShell le script	447
Installer Entra Connect Sync	449
AWS Tutoriels de laboratoire de test Microsoft AD gérés	452
Tutoriel : Configuration de votre laboratoire de test Microsoft AD AWS géré de base	453
Tutoriel : créer une relation de confiance entre AWS Managed Microsoft AD et une installation AD autogérée sur EC2	472
Quotas	484
Résolution des problèmes	486
Problèmes liés à votre Microsoft AD AWS géré	486
Problèmes liés à Netlogon et aux communications par canal sécurisé	486
Vous recevez un message d'erreur « État de réponse : 400 mauvaise demande » lorsque vous tentez de réinitialiser le mot de passe d'un utilisateur	487
Récupération d'un mot de passe	487
Ressources supplémentaires	487
Erreurs de jointure de domaine d'instance Amazon EC2 Linux	488
Espace de stockage disponible bientôt saturé	491
Erreurs d'extension de schéma	495
Raisons liées aux statuts de création d'une relation d'approbation	497
AD Connector	503
Mise en route	504
Conditions préalables requises pour AD Connector	504
Création d'un AD Connector	521

Ce qui est créé avec votre AD Connector	523
Bonnes pratiques	524
Configuration : prérequis	524
Programmation de vos applications	527
Utilisation de votre annuaire	527
Maintenance de votre annuaire	528
Affichage des informations du répertoire	528
Mise à jour du type de réseau d'annuaire	528
Mettre à jour l'adresse DNS de votre AD Connector	530
Supprimer votre AD Connector	530
Sécurisation de votre annuaire	532
Activation de l'authentification multi-facteurs	533
Activation du protocole LDAPS côté client	535
Activation de l'authentification mTLS	542
Mettre à jour les informations d'identification de votre compte de service AD Connector	551
Configurer le AWS CA privée connecteur pour AD	552
Surveillance de votre annuaire	554
Comprendre le statut de votre annuaire	555
Activation des notifications d'état des annuaires avec Amazon SNS	556
Accès aux AWS applications et aux services	559
Compatibilité des applications	559
Permettre l'accès aux AWS applications et aux services depuis AD Connector	561
Comment joindre une EC2 instance Amazon à votre Active Directory	562
Quotas	563
Dépannage	563
Problèmes liés à la création	564
Problèmes de connectivité	566
Problèmes d'authentification	568
Problèmes de maintenance	577
Je ne parviens pas à supprimer mon AD Connector	578
Outils généraux pour enquêter sur les émetteurs d'AD Connector	578
Simple AD	580
Mise en route	581
Prérequis pour Simple AD	582
Créez votre Simple AD	584
Qu'est-ce qui est créé avec votre Simple AD	587

Bonnes pratiques	589
Configuration : prérequis	589
Configuration : création de votre annuaire	591
Programmation de vos applications	591
Maintenance de votre annuaire	592
Affichage des informations du répertoire	593
Mise à jour du type de réseau d'annuaire	593
Configuration des serveurs DNS	595
Restaurer votre répertoire avec un instantané	596
Supprimer votre Simple AD	598
Sécuriser votre annuaire	600
Réinitialiser le mot de passe du compte krbtgt	600
Surveillance de votre annuaire	605
Comprendre le statut de votre annuaire	606
Activation des notifications d'état des annuaires avec Amazon Simple Notification Service ..	608
Accès aux AWS applications et aux services	610
Compatibilité des applications	611
Permettre l'accès aux AWS applications et aux services	612
Permettre l'accès au AWS Management Console	613
Création d'une URL d'accès	616
Activation de l'authentification unique	616
Méthodes pour joindre une instance à votre annuaire	625
Rejoindre une instance Windows	626
Rejoindre une instance Linux	634
Délégation des privilèges d'adhésion à un annuaire	660
Création d'un jeu d'options DHCP	663
Gestion des utilisateurs et des groupes	665
Installation des outils d'administration AD	666
Création d'un utilisateur	668
Suppression d'un utilisateur	670
Réinitialisation du mot de passe utilisateur	671
Création d'un groupe	673
Ajouter un utilisateur à un groupe	674
Quotas	676
Résolution des problèmes	676
Récupération d'un mot de passe	677

Je reçois un message d'erreur « KDC ne peut pas répondre à l'option demandée » lors de l'ajout d'un utilisateur à Simple AD	677
Je ne parviens pas à mettre à jour le nom DNS ou l'adresse IP d'une instance jointe à mon domaine (mise à jour dynamique DNS)	677
Je ne parviens pas à me connecter à SQL Server à l'aide d'un compte SQL Server	678
Mon Simple AD est bloqué dans l'état « Demandé »	678
Je reçois un message d'erreur « AZ constrained » lorsque je crée un Simple AD	678
Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon Simple AD	678
Ressources supplémentaires	487
Résolution des messages d'état du répertoire	679
Sécurité	683
Gestion des identités et des accès	684
Authentification	685
Contrôle d'accès	685
Présentation de la gestion des accès	685
AWS politiques gérées	690
Utilisation des politiques basées sur une identité (politiques IAM)	695
Directory Service Référence des autorisations d'API	705
Clés de condition des données du Directory Service	708
Autorisation pour AWS les applications et les services utilisant Directory Service	714
Autoriser une AWS application sur un Active Directory	714
AWS autorisation d'application avec Directory Service Data	715
Utilisation des rôles liés aux services	717
Autorisations de rôle liées à un service pour Directory Service	717
Création d'un rôle lié à un service pour Directory Service	718
Modification d'un rôle lié à un service pour Directory Service	719
Supprimer un rôle lié à un service pour Directory Service	719
Régions prises en charge pour les rôles Directory Service liés à un service	720
Journalisation et surveillance	721
AWS Directory Service journaux	722
AWS Journaux de données du Directory Service	725
Validation de conformité	735
Résilience	735
Sécurité de l'infrastructure	736
Prévention du cas de figure de l'adjoint désorienté entre services	736
AWS PrivateLink	740

Considérations	740
Disponibilité	740
Création d'une interface (point de terminaison Amazon VPC)	741
Création d'une politique de point de terminaison	741
Contrat de niveau de service	744
Disponibilité dans les Régions	745
Pris en charge Régions AWS pour les données du Directory Service	752
Compatibilité des navigateurs	756
Qu'est-ce que TLS ?	756
Quelles sont les versions de TLS prises en charge par l'IAM Identity Center ?	756
Comment puis-je activer les versions de TLS prises en charge dans mon navigateur	757
Historique du document	758
.....	dcclxiii

Qu'est-ce que c'est AWS Directory Service ?

AWS Directory Service propose plusieurs manières d'utiliser Microsoft Active Directory (AD) avec d'autres AWS services. Les annuaires stockent des informations sur les utilisateurs, les groupes et les appareils, et les administrateurs les utilisent pour gérer l'accès aux informations et aux ressources. AWS Directory Service propose plusieurs choix d'annuaires aux clients qui souhaitent utiliser des applications compatibles Microsoft AD ou LDAP (Lightweight Directory Access Protocol) existantes dans le cloud. Il offre également ces mêmes possibilités pour les développeurs qui ont besoin d'un annuaire pour gérer des utilisateurs, des groupes, des appareils et des accès.

AWS Directory Service options

AWS Directory Service inclut plusieurs types de répertoires parmi lesquels choisir. Pour plus d'informations, sélectionnez l'un des onglets suivants :

AWS Directory Service for Microsoft Active Directory

Également connu sous le nom de AWS Managed Microsoft AD, AWS Directory Service for Microsoft Active Directory est alimenté par un véritable Microsoft Windows Server Active Directory (AD), géré AWS dans le AWS cloud. Il vous permet de migrer un large éventail d'applications compatibles avec Active Directory vers le cloud. AWS AWS Managed Microsoft AD fonctionne avec Microsoft SharePoint les groupes de disponibilité Microsoft SQL Server Always On et de nombreuses applications .NET. Il prend également en charge les applications et services AWS gérés WorkSpaces, notamment [Amazon WorkDocs](#), [Amazon](#), [Amazon Quick Suite](#), [Amazon Chime](#), [Amazon Connect](#) et [Amazon Relational Database Service pour \(Microsoft SQL Server\)](#) [Amazon RDS pour SQL Server](#), [Amazon RDS pour Oracle](#) et [Amazon RDS pour PostgreSQL](#).

AWS Managed Microsoft AD est approuvé pour les applications dans le AWS cloud soumises à la conformité à la loi [américaine HIPAA \(Health Insurance Portability and Accountability Act\)](#) ou à la [norme de sécurité des données du secteur des cartes de paiement](#) (PCI DSS) lorsque vous [activez](#) la conformité pour votre annuaire.

Toutes les applications compatibles fonctionnent avec les informations d'identification utilisateur que vous stockez dans AWS Managed Microsoft AD, ou vous pouvez vous [connecter à votre infrastructure AD existante](#) en toute confiance et utiliser les informations d'identification d'un Active

Directory exécuté sur site ou EC2 sous Windows. Si vous [associez EC2 des instances à votre AWS Managed Microsoft AD](#), vos utilisateurs peuvent accéder aux charges de travail Windows dans le AWS cloud avec la même expérience d'authentification unique (SSO) Windows que lorsqu'ils accèdent aux charges de travail de votre réseau local.

AWS Managed Microsoft AD prend également en charge les cas d'utilisation fédérés à l'aide des informations d'identification Active Directory. Seul, AWS Managed Microsoft AD vous permet de vous connecter au [AWS Management Console](#). Vous pouvez également obtenir des informations d'identification à court terme à utiliser avec le AWS SDK et la CLI, et utiliser des intégrations SAML préconfigurées pour vous connecter à de nombreuses applications cloud. [AWS IAM Identity Center](#) En ajoutant Microsoft Entra Connect (anciennement connu sous le nom de Azure Active Directory Connect) et éventuellement Active Directory Federation Service (AD FS), vous pouvez vous connecter à Microsoft Office 365 d'autres applications cloud avec des informations d'identification stockées dans AWS Managed Microsoft AD.

Le service inclut les fonctions clés qui vous permettent d'[étendre votre schéma](#), de [gérer des stratégies de mot de passe](#) et d'[activer des communications LDAP sécurisées](#) via le protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security). Vous pouvez également [activer l'authentification multifactorielle \(MFA\) pour AWS Managed Microsoft AD](#) afin de fournir un niveau de sécurité supplémentaire lorsque les utilisateurs AWS accèdent à des applications depuis Internet. Active Directory est un annuaire LDAP, autrement dit vous pouvez également utiliser AWS Managed Microsoft AD pour l'authentification Secure Shell (SSH) Linux ainsi que pour d'autres applications compatibles LDAP.

AWS assure la surveillance, les instantanés quotidiens et la restauration dans le cadre du service : vous [ajoutez des utilisateurs et des groupes à Managed AWS Microsoft AD](#), et vous administrez la stratégie de groupe à l'aide d'outils Active Directory familiers exécutés sur un Windows ordinateur connecté au domaine Managed AWS Microsoft AD. Vous pouvez également mettre à l'échelle l'annuaire en [déployant des contrôleurs de domaine supplémentaires](#) et contribuer à améliorer les performances des applications en répartissant les demandes sur un plus grand nombre de contrôleurs de domaine.

AWS Managed Microsoft AD est disponible en deux éditions : Standard et Enterprise.

- Standard Edition : AWS Managed Microsoft AD (Standard Edition) est optimisé pour être utilisé comme annuaire principal dans les petites et moyennes entreprises comptant jusqu'à 5 000 employés. Il offre suffisamment de capacité de stockage pour prendre en charge jusqu'à 30 000* objets d'annuaire (par exemple, des utilisateurs, des groupes et des ordinateurs).

- Enterprise Edition : AWS Managed Microsoft AD (Enterprise Edition) s'adresse aux grandes entreprises qui ont à gérer jusqu'à 500 000* objets d'annuaire.

* Les plafonds indiqués sont fournis à titre indicatif. Votre annuaire peut prendre en charge plus ou moins d'objets d'annuaire, selon la taille de vos objets et le comportement et les besoins de performances de vos applications.

Quand l'utiliser

AWS Managed Microsoft AD est votre meilleur choix si vous avez besoin de fonctionnalités Active Directory réelles pour prendre en charge AWS des applications ou des Windows charges de travail, notamment Amazon Relational Database Service pour. Microsoft SQL Server C'est également la meilleure solution si vous recherchez un Active Directory autonome dans le AWS cloud compatible avec Office 365 ou si vous avez besoin d'un annuaire LDAP pour prendre en charge vos applications Linux. Pour de plus amples informations, veuillez consulter [AWS Microsoft AD géré](#).

AD Connector

AD Connector est un service proxy qui permet de connecter facilement des AWS applications compatibles, telles qu'Amazon WorkSpaces, Amazon Quick Suite et [Amazon EC2](#) pour les Windows Server instances, à votre Microsoft Active Directory sur site existant. Avec AD Connector, il vous suffit d'[ajouter un compte de service](#) à votre instance Active Directory. AD Connector vous évite aussi d'avoir à synchroniser vos annuaires et vous épargne le coût et la complexité associés à l'hébergement d'une infrastructure de fédération.

Lorsque vous ajoutez des utilisateurs à AWS des applications telles qu'Amazon Quick Suite, AD Connector lit votre Active Directory existant pour créer des listes d'utilisateurs et de groupes parmi lesquels sélectionner. Lorsque les utilisateurs se connectent aux AWS applications, AD Connector transmet les demandes de connexion à vos contrôleurs de domaine Active Directory locaux à des fins d'authentification. [AD Connector fonctionne avec de nombreuses AWS applications et services, notamment Amazon WorkSpaces WorkDocs, Amazon, Amazon Quick Suite, Amazon Chime, Amazon Connect et Amazon. WorkMail](#) Vous pouvez également [joindre vos EC2 Windows instances](#) à votre domaine Active Directory local via AD Connector en utilisant [une jointure de domaine fluide](#). AD Connector permet également à vos utilisateurs d'accéder aux AWS ressources AWS Management Console et de les gérer en se connectant avec leurs informations d'identification Active Directory existantes. AD Connector n'est pas compatible avec RDS SQL Server.

Vous pouvez également utiliser AD Connector pour [activer l'authentification multifactorielle](#) (MFA) pour les utilisateurs de AWS votre application en la connectant à votre infrastructure MFA existante basée sur Radius. Les utilisateurs bénéficient ainsi d'une couche de sécurité supplémentaire quand ils accèdent aux applications AWS .

AD Connector vous permet de continuer à gérer votre annuaire Active Directory comme vous le faites actuellement. Par exemple, vous pouvez ajouter des utilisateurs et des groupes, et mettre à jour les mots de passe en utilisant les outils d'administration Active Directory standard dans votre instance Active Directory. Cela vous permet d'appliquer de manière cohérente vos politiques de sécurité, telles que l'expiration des mots de passe, l'historique des mots de passe et le verrouillage des comptes, que les utilisateurs accèdent aux ressources sur site ou dans le AWS cloud.

Quand l'utiliser

AD Connector est votre meilleur choix lorsque vous souhaitez utiliser votre annuaire local existant avec des AWS services compatibles. Pour de plus amples informations, veuillez consulter [AD Connector](#).

Simple AD

Simple AD est un Microsoft annuaire compatible avec Active Directory AWS Directory Service développé par Samba 4. Simple AD prend en charge les fonctionnalités de base d'Active Directory telles que les comptes utilisateurs, les adhésions à des groupes, l'adhésion à un domaine Linux ou à des EC2 instances Windows basées sur Linux, l'authentification unique basée sur Kerberos et les politiques de groupe. AWS assure la surveillance, les instantanés quotidiens et la restauration dans le cadre du service.

Simple AD est un annuaire autonome hébergé dans le cloud, qui vous permet non seulement de créer et gérer des identités d'utilisateurs, mais également de gérer l'accès aux applications. Vous pouvez utiliser de nombreux outils et applications Active Directory familiers qui nécessitent des fonctionnalités Active Directory de base. Simple AD est compatible avec les AWS applications suivantes : [Amazon WorkSpaces](#), [Amazon WorkDocs](#), [Amazon Quick Suite](#) et [Amazon WorkMail](#). Vous pouvez également vous connecter à l' AWS Management Console aide de comptes utilisateur Simple AD et pour gérer les AWS ressources.

Simple AD ne prend pas en charge l'authentification multifactorielle (MFA), les relations de confiance, la mise à jour dynamique du DNS, les extensions de schéma, la communication via LDAPS PowerShell , les applets de commande AD ou le transfert de rôles FSMO. Simple AD

n'est pas compatible avec RDS SQL Server. Les clients qui ont besoin des fonctionnalités d'un véritable Microsoft Active Directory ou qui envisagent d'utiliser leur annuaire avec RDS SQL Server devraient plutôt utiliser Managed AWS Microsoft AD. Veuillez vous assurer que vos applications requises sont entièrement compatibles avec Samba 4 avant d'utiliser Simple AD. Pour plus d'informations, veuillez consulter <https://www.samba.org>.

Quand l'utiliser

Vous pouvez utiliser Simple AD en tant qu'annuaire autonome dans le cloud pour prendre en charge les Windows charges de travail nécessitant des fonctionnalités Active Directory de base, des AWS applications compatibles ou pour prendre en charge les charges de travail Linux nécessitant un service LDAP. Pour de plus amples informations, veuillez consulter [Simple AD](#).

Consultez [Disponibilité de la région pour Directory Service](#) pour obtenir la liste des types d'annuaires pris en charge par région.

Que choisir ?

Vous pouvez choisir des services d'annuaire qui offrent les fonctionnalités et la scalabilité correspondant le mieux à vos besoins. Utilisez le tableau suivant pour déterminer quelle option d'AWS Directory Service annuaire convient le mieux à votre organisation.

Que devez-vous faire ?	AWS Directory Service Options recommandées
J'ai besoin d'Active Directory ou de LDAP pour mes applications dans le cloud	Utilisez AWS Directory Service pour Microsoft Active Directory (édition standard ou édition Enterprise) si vous avez besoin d'un véritable Microsoft Active Directory dans le AWS cloud prenant en charge les charges de travail compatibles avec Active Directory, ou des AWS applications et services tels qu'Amazon et WorkSpaces Amazon Quick Suite, ou si vous avez besoin du support LDAP pour les applications Linux. Utilisez AWS Directory Service pour Microsoft Active Directory (édition hybride) pour étendre votre Active Directory autogéré existant à AWS Cloud AWS Directory Service

Que devez-vous faire ?	AWS Directory Service Options recommandées
	Utilisez AD Connector si vous devez uniquement autoriser vos utilisateurs locaux à se connecter aux AWS applications et aux services avec leurs informations d'identification Active Directory. Vous pouvez également utiliser AD Connector pour associer EC2 des instances Amazon à votre domaine Active Directory existant. Utilisez Simple AD si vous recherchez un annuaire de base à moindres coûts, qui offre une compatibilité de base avec Active Directory et qui prend en charge les applications compatibles Samba 4, ou si vous avez besoin d'une compatibilité LDAP pour vos applications LDAP.
Je développe des applications SaaS	Utilisez Amazon Cognito si vous développez des applications SaaS à grande échelle et si vous avez besoin d'un annuaire évolutif pour gérer et authentifier vos abonnés qui soit également capable de gérer les identités de réseaux sociaux.

Pour plus d'informations sur les options d' AWS Directory Service annuaire, voir [Comment choisir les solutions Active Directory sur AWS](#).

Travailler avec Amazon EC2

Une connaissance de base d'Amazon EC2 est essentielle pour pouvoir l'utiliser Directory Service. Nous vous recommandons de commencer par lire les rubriques suivantes :

- [Qu'est-ce qu'Amazon EC2 ?](#) dans le guide de EC2 l'utilisateur Amazon.
- [Lancez une EC2 instance Amazon](#) dans le guide de EC2 l'utilisateur Amazon.
- [Groupes EC2 de sécurité Amazon pour vos EC2 instances](#) dans le guide de EC2 l'utilisateur Amazon.
- [Qu'est-ce qu'Amazon VPC ?](#) dans le Guide de l'utilisateur Amazon VPC
- [Connectez votre VPC à des réseaux distants à l'aide](#) du guide AWS Virtual Private Network de l'utilisateur Amazon VPC.

AWS Microsoft AD géré

AWS Directory Service pour Microsoft Active Directory, également appelé AWS Managed Microsoft AD, s'exécute Microsoft Active Directory en tant que service géré alimenté par Windows Server 2019. Il crée une paire de contrôleurs de domaine à haute disponibilité dans votre Amazon VPC dans différentes zones de disponibilité, en gérant AWS automatiquement la surveillance de l'hôte, la restauration, la réplication des données, les instantanés et les mises à jour logicielles. Ce service vous permet d'exécuter des charges de travail adaptées aux annuaires, de gérer les utilisateurs et les groupes, de fournir une authentification unique, de créer et d'appliquer des politiques de groupe et de vous connecter en toute sécurité aux instances Amazon. EC2

Directory Service propose deux Microsoft Active Directory solutions : AWS Directory Service pour Microsoft Active Directory fournit un service Active Directory entièrement géré dans le AWS cloud, tandis que AWS Managed Microsoft AD (édition hybride) étend votre AD autogéré existant à AWS.

AWS Managed Microsoft AD (Standard Edition et Enterprise Edition) crée de nouveaux domaines AD gérés sur lesquels gérer les utilisateurs, les appareils et les ordinateurs AWS. Ces annuaires établissent des forêts de ressources qui créent des relations de confiance avec vos domaines AD existants sur site AWS, dans ou dans des environnements multicloud. Les utilisateurs peuvent accéder aux AWS ressources avec leurs informations d'identification existantes à partir de vos domaines AD actuels. Les identités des utilisateurs restent dans vos domaines AD existants tandis que la forêt de ressources gère vos AWS ressources, en maintenant l'isolation opérationnelle entre les environnements tout en fournissant une connexion unique fluide.

AWS Managed Microsoft AD (Hybrid Edition) connecte votre Active Directory autogéré à AWS Directory Service pour Microsoft Active Directory, créant ainsi un environnement d'identité intégré couvrant à la fois votre infrastructure et le AWS Cloud. Cette solution étend vos services d'annuaire AWS sans synchroniser les identités des utilisateurs, établit des relations de confiance entre les environnements et fournit un accès fluide à l'aide des informations d'identification existantes.

Avec AWS Managed Microsoft AD, vous pouvez exécuter des charges de travail basées sur des annuaires dans le AWS cloud, notamment des applications .NET Microsoft SharePoint et SQL Server personnalisées. Vous pouvez également configurer des relations de confiance entre AWS Managed Microsoft AD et votre Microsoft Active Directory autogéré existant, en fournissant aux utilisateurs et aux groupes l'accès aux ressources de l'un ou l'autre domaine en utilisant AWS IAM Identity Center.

Lequel choisir ?

Vous pouvez choisir entre deux AWS Directory Service services dotés des fonctionnalités et de l'évolutivité qui répondent le mieux à vos besoins. Le tableau suivant vous aide à déterminer quelle Directory Service option convient le mieux à votre organisation.

Cas d'utilisation	Solution recommandée
Exécutez des charges de travail, des applications ou des AWS applications Linux compatibles avec les annuaires nécessitant le support LDAP	AWS Managed Microsoft AD (Standard Edition et Enterprise Edition) crée de nouveaux domaines AD gérés sur lesquels gérer les utilisateurs, les appareils et les ordinateurs AWS. Ces annuaires établissent des forêts de ressources qui créent des relations de confiance avec vos domaines AD existants sur site AWS, dans ou dans des environnements multicloud. Les utilisateurs peuvent accéder aux AWS ressources avec leurs informations d'identification existantes à partir de vos domaines AD actuels. Les identités des utilisateurs restent dans vos domaines AD existants tandis que la forêt de ressources gère vos AWS ressources, en maintenant l'isolation opérationnelle entre les environnements tout en fournissant une connexion unique fluide.
Étendre Active Directory existant à AWS	AWS Managed Microsoft AD (Hybrid Edition) connecte votre Active Directory autogéré à AWS Directory Service pour Microsoft Active Directory, créant ainsi un environnement d'identité intégré couvrant à la fois votre infrastructure et le AWS Cloud. Cette solution étend vos services d'annuaire AWS sans synchroniser les identités des utilisateurs, établit des relations de confiance entre les environnements et fournit un accès fluide à l'aide des informations d'identification existantes.

Rubriques

- [Commencer à utiliser AWS Managed Microsoft AD](#)

- [Comprendre AWS Managed Microsoft AD \(édition hybride\)](#)

Comprendre AWS Managed Microsoft AD (édition hybride)

AWS Managed Microsoft AD (édition hybride) vous permet d'étendre votre Active Directory existant AWS Cloud à AWS Managed Microsoft AD. Cette fonctionnalité facilite le transfert de vos charges de travail dépendantes de la publicité AWS, l'adoption de AWS services et l'augmentation de la redondance de votre Active Directory. AWS exécutera régulièrement des évaluations de répertoire sur votre répertoire hybride, que vous pourrez consulter dans la Directory Service console.

Un annuaire hybride Directory Service connecte votre répertoire existant Microsoft Active Directory à AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Cela crée un environnement d'identité intégré qui couvre une infrastructure sur site et multicloud AWS, vous permettant de conserver une source d'identité unique tout en étendant vos services d'annuaire à AWS.

Une configuration d'annuaire hybride fournit plusieurs fonctionnalités importantes :

- Extension de l'AD autogéré au AWS Cloud sans qu'il soit nécessaire d'établir une relation de confiance
- Authentification et autorisation fluides dans tous les environnements à l'aide des informations d'identification Active Directory existantes
- Identifiants utilisateur et appartenances à des groupes cohérents dans vos deux environnements AD
- Gestion centralisée des politiques d'accès et des autorisations AD

Rubriques

- [Conditions préalables requises pour un annuaire hybride](#)
- [Création d'un annuaire hybride](#)
- [Afficher et modifier un répertoire hybride](#)
- [Supprimer un répertoire hybride](#)
- [Évaluations d'annuaires pour les annuaires hybrides](#)
- [Résolution des problèmes liés aux annuaires hybrides et évaluation des annuaires](#)

Conditions préalables requises pour un annuaire hybride

L'annuaire hybride étend votre Active Directory autogéré au AWS Cloud. Avant de créer un annuaire hybride, assurez-vous que votre environnement répond aux exigences suivantes :

Microsoft Active Directoryexigences relatives au domaine

Avant de créer un annuaire hybride, assurez-vous que votre environnement et votre infrastructure AD autogérés répondent aux exigences suivantes et collectez les informations nécessaires.

Exigences relatives au domaine

Votre environnement AD autogéré doit répondre aux exigences suivantes :

- Utilise un Windows Server 2012 R2 ou un niveau 2016 fonctionnel.
- Utilise des contrôleurs de domaine standard à évaluer pour la création d'annuaires hybrides. Les contrôleurs de domaine en lecture seule (RODC) ne peuvent pas être utilisés pour la création d'annuaires hybrides.
- Dispose de deux contrôleurs de domaine avec tous les services Active Directory en cours d'exécution.
- Le contrôleur de domaine principal (PDC) doit être routable à tout moment.

Plus précisément, l'émulateur PDC et le maître RID IPs de votre AD autogéré doivent appartenir à l'une des catégories suivantes :

- Partie des plages d'adresses IP RFC1918 privées (10.0.0.0/8, 172.16.0.0/12 ou 192.168.0.0/16)
- Dans le cadre de votre gamme VPC CIDR
- Associez le DNS IPs de vos instances autogérées à l'annuaire

Vous pouvez ajouter des routes IP supplémentaires pour le répertoire après la création de l'annuaire hybride.

Informations obligatoires

Rassemblez les informations suivantes sur votre AD autogéré :

- Nom de DNS de l'annuaire
- Répertoire DNS IPs

- Informations d'identification du compte de service avec autorisations d'administrateur pour votre AD autogéré
- AWS ARN secret pour stocker les informations d'identification de votre compte de service (voir [AWS ARN secret pour annuaire hybride](#))

AWS ARN secret pour annuaire hybride

Pour configurer un annuaire hybride avec votre AD autogéré, vous devez créer une clé KMS pour chiffrer votre AWS secret, puis créer le secret lui-même. Les deux ressources doivent être créées dans le même répertoire Compte AWS que celui qui contient le répertoire hybride.

Création d'une clé KMS

La clé KMS est utilisée pour chiffrer votre AWS secret.

Important

Pour Clé de chiffrement, n'utilisez pas la clé KMS par défaut AWS. Assurez-vous de créer la clé AWS KMS dans le même répertoire Compte AWS qui contient le répertoire hybride que vous souhaitez créer pour le joindre à votre AD autogéré.

Pour créer une clé AWS KMS

1. Dans la AWS KMS console, choisissez Create key.
2. Pour Type de clé, choisissez Symétrique.
3. Pour Utilisation de la clé, choisissez Chiffrer et déchiffrer.
4. Pour Options avancées :
 - a. Pour Origine des clés, choisissez KMS.
 - b. Pour Régionalité, choisissez la clé à région unique, puis cliquez sur Suivant.
5. Pour Alias, attribuez un nom à la clé KMS.
6. (Facultatif) Pour Description, fournissez une description de la clé KMS.
7. (Facultatif) Pour Tags, ajoutez des tags pour la clé KMS et choisissez Next.
8. Pour les administrateurs clés, sélectionnez un utilisateur IAM.
9. Pour la suppression de clés, conservez la sélection par défaut pour Autoriser les administrateurs de clés à supprimer cette clé et choisissez Suivant.

10. Pour les utilisateurs clés, sélectionnez le même utilisateur IAM à l'étape précédente et choisissez Next.
11. Passez en revue la configuration.
12. Pour la politique clé, ajoutez la déclaration suivante à la stratégie :
13. Choisissez Finish (Terminer).

Créez un AWS secret

Créez un secret dans Secrets Manager pour stocker les informations d'identification de votre compte utilisateur AD autogéré.

Important

Créez le secret dans celui-ci Compte AWS qui contient le répertoire hybride que vous souhaitez joindre à votre AD autogéré.

Pour créer un secret

- Dans Secrets Manager, choisissez Enregistrer un nouveau secret
 - Pour Type de secret, choisissez Autre type de secret
 - Pour Paires clé/valeur, ajoutez vos deux clés :
1. Ajoutez la clé du nom d'utilisateur
 - a. Pour la première clé, entrez `customerAdAdminDomainUsername`.
 - b. Pour la valeur de la première clé, entrez uniquement le nom d'utilisateur (sans le préfixe de domaine) de l'utilisateur AD. N'incluez pas le nom de domaine car cela entraîne l'échec de la création de l'instance.
 2. Ajoutez la clé du mot de passe
 - a. Pour la deuxième clé, entrez `customerAdAdminDomainPassword`.
 - b. Pour la valeur de la deuxième clé, saisissez le mot de passe que vous avez créé pour l'utilisateur AD sur votre domaine.

Terminez la configuration secrète

1. Pour Clé de chiffrement, sélectionnez la clé KMS que vous avez créée [Création d'une clé KMS](#) et choisissez Next.
2. Dans Nom du secret, entrez une description du secret.
3. (Facultatif) Dans Description, entrez une description pour le secret.
4. Choisissez Suivant.
5. Pour Configurer les paramètres de rotation, conservez les valeurs par défaut et choisissez Suivant.
6. Vérifiez les paramètres du secret et choisissez Store.
7. Choisissez le secret que vous avez créé et copiez la valeur de l'ARN du secret. Vous utiliserez cet ARN à l'étape suivante pour configurer votre Active Directory autogéré.

Exigences en matière d'infrastructure

Préparez les composants d'infrastructure suivants :

- Deux AWS Systems Manager nœuds dotés de privilèges d'administrateur pour les agents SSM
 - Si votre Active Directory est autogéré en dehors de AWS Cloud, vous aurez besoin de deux nœuds Systems Manager pour un environnement hybride et multicloud. Pour plus d'informations sur le provisionnement de ces nœuds, consultez la section [Configuration de Systems Manager pour les environnements hybrides et multicloud](#).
 - Si votre Active Directory est autogéré au sein du AWS Cloud, vous aurez besoin de deux EC2 instances gérées par Systems Manager. Pour plus d'informations sur le provisionnement de ces instances, consultez [la section Gestion des EC2 instances avec Systems Manager](#).

Services Active Directory requis

Assurez-vous que les services suivants sont exécutés sur votre AD autogéré :

- Services de domaine Active Directory (AD DS)
- Service Web Active Directory (ADWS)
- Système d'événements COM+
- Réplication de systèmes de fichiers distribués (DFSR)
- Système de nom de domaine (DNS)

- Serveur DNS
- Client de stratégie de groupe
- Messagerie intersites
- Appel de procédure à distance (RPC)
- Responsable des comptes de sécurité
- Serveur Windows Time

Note

Le répertoire hybride nécessite que le port UDP 123 soit ouvert et que le serveur Windows Time soit activé et fonctionnel. Nous synchronisons l'heure avec votre contrôleur de domaine pour garantir le bon fonctionnement de la réplication d'annuaires hybride.

Exigences d'authentification Kerberos

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Pour obtenir des instructions détaillées sur la façon d'activer ce paramètre, voir Vérifier [que la pré-authentification Kerberos est activée](#). Pour obtenir des informations générales sur ce paramètre, consultez la section [Préauthentification activée](#) Microsoft TechNet.

Types de chiffrement pris en charge

Un annuaire hybride prend en charge les types de chiffrement suivants lors de l'authentification via Kerberos auprès de vos contrôleurs de domaine Active Directory :

- AES-256-HMAC

Exigences relatives aux ports réseau

AWS Pour étendre vos contrôleurs de domaine Active Directory autogérés, le pare-feu de votre réseau existant doit disposer des ports suivants ouverts vers les deux sous-réseaux CIDRs de votre Amazon VPC :

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- UDP 123 - Serveur de temps

- TCP 135 - Appel de procédure à distance
- TCP/UDP 389 - LDAP
- TCP 445 - SMB
- TCP 636 : uniquement nécessaire pour les environnements dotés du protocole LDAPS (Lightweight Directory Access Protocol Secure)
- TCP 49152-65535 - Ports TCP élevés alloués aléatoirement par RPC
- TCP 3268 et 3269 - Catalogue mondial
- Services Web Active Directory TCP 9389 (ADWS)

Il s'agit des ports minimaux nécessaires pour créer un répertoire hybride. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

 Note

Les ports DNS IPs fournis à vos contrôleurs de domaine et aux détenteurs de rôles FSMO doivent être ouverts aux deux sous-réseaux CIDRs de l'Amazon VPC.

 Note

Le répertoire hybride nécessite que le port UDP 123 soit ouvert et que le serveur Windows Time soit activé et fonctionnel. Nous synchronisons l'heure avec votre contrôleur de domaine pour garantir le bon fonctionnement de la réplication d'annuaires hybride.

Compte AWS autorisations

Vous aurez besoin d'autorisations pour effectuer les actions suivantes dans votre Compte AWS :

- EC2 : AuthorizeSecurityGroupEgress
- EC2 : AuthorizeSecurityGroupIngress
- EC2 : CreateNetworkInterface
- EC2 : CreateSecurityGroup
- EC2 : DescribeNetworkInterfaces

- EC2 : DescribeSubnets
- EC2 : DescribeVpcs
- EC2 : CreateTags
- EC2 : CreateNetworkInterfacePermission
- SMS : ListCommands
- SMS : GetCommandInvocation
- SMS : GetConnectionStatus
- SMS : SendCommand
- responsable des secrets : DescribeSecret
- responsable des secrets : GetSecretValue
- iam : GetRole
- iam : CreateServiceLinkedRole

Exigences relatives au réseau Amazon VPC

Un VPC présentant les caractéristiques suivantes :

- Au moins deux sous-réseaux. Chacun des sous-réseaux doit se trouver dans une zone de disponibilité différente
- Le VPC doit avoir une location par défaut

Vous ne pouvez pas créer de répertoire hybride dans un VPC en utilisant les adresses de l'espace d'adressage 198.18.0.0/15.

Directory Service utilise une structure à deux VPC. Les EC2 instances qui composent votre répertoire s'exécutent en dehors de votre Compte AWS répertoire et sont gérées par AWS. Elles ont deux cartes réseau, ETH0 et ETH1. ETH0 est la carte de gestion et existe en dehors de votre compte. ETH1 est créé au sein de votre compte.

La plage d'adresses IP de gestion du réseau ETH0 pour votre annuaire est 198.18.0.0/15.

Pour plus d'informations, veuillez consulter les rubriques suivantes dans le Amazon VPC Guide de l'utilisateur :

- [Qu'est-ce qu'Amazon VPC ?](#)

- [Qu'est-ce qu'Amazon VPC ?](#)
- [VPCs et sous-réseaux](#)
- [Qu'est-ce qu' AWS Site-to-Site VPN ?](#)

Pour plus d'informations AWS Direct Connect, consultez la section [Qu'est-ce que c'est AWS Direct Connect ?](#)

AWS configuration du groupe de sécurité

Par défaut, AWS attache un groupe de sécurité pour autoriser l'accès réseau aux nœuds AWS Systems Manager gérés de votre VPC. Vous pouvez éventuellement fournir votre propre groupe de sécurité qui autorise le trafic réseau à destination et en provenance de vos contrôleurs de domaine autogérés en dehors de votre VPC.

Vous pouvez éventuellement fournir votre propre groupe de sécurité qui autorise le trafic réseau à destination et en provenance de vos contrôleurs de domaine autogérés en dehors de votre VPC. Si vous fournissez votre propre groupe de sécurité, vous devez :

- Autorisez la mise en liste de vos VPC CIDR plages et de vos plages autogérées.
- Assurez-vous que ces plages ne se chevauchent pas avec les [plages d'adresses IP AWS réservées](#)

Considérations relatives aux évaluations de répertoires

Les points suivants doivent être pris en compte lors de la création d'évaluations d'annuaires et du nombre d'évaluations que vous pouvez avoir dans votre répertoire Compte AWS :

- Une évaluation d'annuaire est automatiquement créée lorsque vous créez un annuaire hybride. Il existe deux types d'évaluations : CUSTOMER et SYSTEM. Votre Compte AWS a une limite de 100 évaluations d'CUSTOMERannuaire.
- Si vous tentez de créer un annuaire hybride et que vous avez déjà effectué 100 évaluations d'CUSTOMERannuaires, vous allez rencontrer une erreur. Supprimez les évaluations pour libérer de la capacité avant de réessayer.
- Vous pouvez demander une augmentation de votre quota d'évaluation du CUSTOMER répertoire en contactant Support ou en supprimant les évaluations du répertoire CLIENTS existantes afin de libérer de la capacité.

Création d'un annuaire hybride

Avant de créer un annuaire hybride, vous devez créer et réussir une évaluation de l'annuaire qui vérifie la connectivité et l'interopérabilité avec votre Active Directory autogéré

Création d'un annuaire hybride avec votre AD autogéré

Procédez comme suit pour créer un annuaire hybride avec votre AD autogéré :

Pour créer un annuaire hybride

1. Ouvrez la Directory Service console correspondant à la région de votre choix.
2. Sur la page Sélectionner le type de répertoire, choisissez AWS Managed Microsoft AD.
3. Sous Getting started with AWS Managed Microsoft AD, sélectionnez Étendre votre domaine AD avec un annuaire hybride — nouveau, puis cliquez sur Suivant. Cela vous dirige vers la page d'évaluation de la création d'un répertoire.
4. Avant de créer un annuaire hybride, vous devez d'abord créer et réussir une évaluation de l'annuaire. Pour créer une évaluation d'annuaire, suivez les étapes décrites dans [Création d'évaluations d'annuaires](#). Une fois que vous avez passé avec succès une évaluation de l'annuaire, vous pouvez poursuivre cette procédure.
5. Une fois que vous avez réussi une évaluation d'annuaire, accédez à la page Répertoires.
6. Sur la page Répertoires, sous Évaluations d'annuaires hybrides d'essai, choisissez un ID d'évaluation dont le statut est de SUCCESS. Sélectionnez ensuite Créer un répertoire hybride, qui vous dirige vers la page de détails de l'évaluation
7. Sur la page des détails de l'évaluation, confirmez cette action en sélectionnant Créer un répertoire hybride, qui ouvre la page Créer un répertoire hybride à l'aide d'un identifiant d'évaluation.
8. Sur la page Créer un annuaire hybride à l'aide d'un identifiant d'évaluation, passez en revue les informations Active Directory autogérées. Après avoir confirmé les informations, sélectionnez Créer un répertoire hybride.

Après avoir choisi Créer un annuaire hybride, AWS exécutez une autre évaluation de l'annuaire sur la base de ces informations pour confirmer que votre configuration AD autogérée est toujours valide. Si l'évaluation du répertoire réussit, nous créons le répertoire hybride.

9. Si vous choisissez Créer un répertoire hybride, vous revenez à la page Répertoires.
 - a. Une bannière verte apparaîtra une fois le répertoire hybride créé avec succès.

- b. Un bandeau rouge apparaît si la création du répertoire hybride échoue. Corrigez les échecs de création de répertoires hybrides en effectuant les opérations suivantes :
 1. Supprimez le répertoire hybride défaillant dans la console.
 2. Supprimez toutes les AWS réservations restantes OUs dans votre AD autogéré.

En savoir plus

- [Supprimer un répertoire hybride](#)
- [Résolution de problème](#)

Afficher et modifier un répertoire hybride

Utilisez les procédures suivantes pour afficher ou modifier votre répertoire hybride.

Afficher un annuaire hybride

Vous pouvez consulter un répertoire hybride dans la Directory Service console.

Pour afficher les informations détaillées de l'annuaire

1. Dans le panneau de navigation de la [console Directory Service](#), choisissez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire. Les informations relatives au répertoire apparaissent sur la page des détails du répertoire.

Informations Active Directory autogérées

Cette section fournit des informations sur votre Active Directory autogéré associé à l' AWS infrastructure.

- Type de répertoire
- ID de l'annuaire
- État du répertoire
- Détails du réseau pour votre AD autogéré, tels que :
 - VPC
 - Sous-réseaux
 - Adresses DNS

- Nœuds gérés par Systems Manager

Onglets de répertoire hybrides

Vous trouverez les informations suivantes concernant votre Microsoft AD AWS géré :

- Dans l'onglet Partager et partager, vous pouvez partager votre compte Microsoft AD AWS géré avec d'autres AWS comptes et consulter les détails du réseau de vos contrôleurs de domaine.
- Dans l'onglet Gestion des applications, vous pouvez activer une URL d'accès aux applications pour votre Microsoft AD AWS géré et activer AWS des applications et des services pour votre Microsoft AD AWS géré.
- Dans l'onglet Maintenance, vous pouvez permettre à SNS de recevoir des notifications concernant l'état de votre Microsoft AD AWS géré et de consulter des instantanés de votre AWS Microsoft AD géré.
- Pour de plus amples informations sur le champ Status (Statut), veuillez consulter [Comprendre le statut de votre annuaire Microsoft AD AWS géré](#).

Mettre à jour un annuaire hybride

Vous pouvez mettre à jour un répertoire hybride dans la Directory Service console pour modifier les paramètres DNS ou récupérer l'accès au compte administrateur.

Pour mettre à jour les informations de l'annuaire hybride

1. Dans le panneau de navigation de la [console Directory Service](#), choisissez Annuaire.
2. Choisissez le lien d'ID de répertoire correspondant à votre répertoire pour ouvrir la page des détails du répertoire.
3. Choisissez Actions, puis sélectionnez Mettre à jour les informations de l'annuaire hybride.
4. Sur la page d'informations de mise à jour de l'annuaire hybride, vous pouvez mettre à jour vos paramètres DNS ou récupérer votre compte administrateur.

Mettre à jour les paramètres DNS (facultatif)

Sous Informations Active Directory autogérées, vous pouvez modifier les éléments suivants :

- a. Nom DNS du répertoire
- b. Adresses IP DNS

Vous pouvez mettre à jour les deux paramètres ensemble ou individuellement. Au moins une modification est requise pour le processus de mise à jour.

5. Restaurer le compte d'administrateur d'annuaire hybride

Pour récupérer votre compte d'administrateur d'annuaire hybride, nous avons besoin d'un accès temporaire à un utilisateur. Cet accès est fourni par le biais d'un secret fourni par Secrets Manager. Nous n'utilisons ces informations d'identification qu'une seule fois lors de la restauration et nous ne les stockons pas. Si votre compte d'administrateur d'annuaire hybride existe, vous n'avez pas besoin de mettre à jour ce secret, même si vous avez mis à jour votre utilisateur administrateur Active Directory autogéré.

- Informations d'identification d'administrateur secrètes — Nous créons un compte d'administrateur d'annuaire hybride lorsque nous créons un annuaire hybride. Si vous avez supprimé ce secret, entrez le secret du Gestionnaire de Secrets pour votre utilisateur administrateur AD autogéré.

Supprimer un répertoire hybride

Lorsque vous supprimez un répertoire hybride, toutes les données et tous les instantanés du répertoire sont supprimés et ne peuvent pas être restaurés. Une fois le répertoire supprimé, toutes les instances jointes au répertoire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification du répertoire pour vous connecter à ces instances. Vous devez vous connecter à ces instances avec un compte utilisateur local.

Pour supprimer un annuaire

1. Dans le volet de navigation de la [console Directory Service](#), sélectionnez Directories (Annuaire). Assurez-vous que vous vous trouvez dans la Région AWS où votre annuaire hybride est déployé. Pour plus d'informations, consultez la section [Choix d'une région](#).
2. Assurez-vous qu'aucune AWS application n'est activée pour le répertoire que vous souhaitez supprimer. Les applications activées vous empêcheront de supprimer votre répertoire hybride.
3. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.

4. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre annuaire.
 - a. Désactivez AWS Management Console l'accès. Pour plus d'informations, consultez la section [Désactivation de l'accès à AWS la console de gestion](#).
 - b. Pour désactiver le serveur de fichiers Amazon FSx pour Windows, vous devez supprimer le système de FSx fichiers Amazon du domaine. Pour plus d'informations, consultez la section [Travailler avec Active Directory dans FSx un serveur de fichiers Windows](#) dans le guide de l'utilisateur d'Amazon FSx pour Windows File Server.
 - c. Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section [Managing a DB instance in a domain](#) (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
5. Dans le volet de navigation, choisissez Directories (Annuaire).
6. Sélectionnez uniquement le répertoire à supprimer, puis choisissez Supprimer. La suppression de l'annuaire prend plusieurs minutes. Lorsque l'annuaire a été supprimé, il est retiré de votre liste d'annuaires.
7. Supprimez manuellement tous les objets de contrôleur de domaine restants, y compris les objets AWS réservés OUs. Vous pouvez supprimer l'intégralité du répertoire AWS réservé pour terminer le nettoyage de votre environnement.

Évaluations d'annuaires pour les annuaires hybrides

Une évaluation d'annuaire examine votre environnement Active Directory autogéré afin de s'assurer qu'il répond aux exigences relatives à la création d'un annuaire hybride. Cette évaluation vérifie la connectivité réseau, la configuration du contrôleur de domaine et les services requis pour aider à identifier et à résoudre les problèmes potentiels avant d'établir une connexion entre votre AD autogéré et Directory Service.

Il existe deux types d'évaluations d'annuaires :

- **CUSTOMER**évaluations : initiées par vous dans la console lorsque vous commencez à configurer un annuaire hybride. Vous pouvez supprimer les évaluations du répertoire des clients, même lorsqu'elles sont en cours. Vous pouvez avoir jusqu'à 100 évaluations de clients.
- **SYSTEM**évaluations — Créées automatiquement par AWS et exécutées périodiquement après une création réussie. Vous ne pouvez pas supprimer les SYSTEM évaluations.

Les évaluations des annuaires fournissent des informations précieuses sur l'état de préparation de votre environnement, notamment :

- Connectivité entre votre AD autogéré et AWS
- Disponibilité des services requis sur vos contrôleurs de domaine
- Compatibilité de configuration avec les exigences du AWS Directory Service
- Problèmes potentiels susceptibles d'empêcher la création réussie d'un annuaire hybride

Une évaluation d'annuaire réussie (réussie) est requise avant de pouvoir créer un annuaire hybride. Si une évaluation échoue, vous pouvez consulter le rapport détaillé pour identifier et résoudre les problèmes avant de réessayer. AWS supprime les SYSTEM évaluations au bout de 30 jours.

Rubriques

- [Création d'évaluations d'annuaires](#)
- [Afficher les évaluations des annuaires](#)
- [Suppression des évaluations d'annuaires](#)

Création d'évaluations d'annuaires

Vous pouvez créer une évaluation d'annuaire dans le cadre de la création d'un annuaire hybride, ou vous pouvez en créer une manuellement. Pour créer une évaluation manuellement, ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>. Sur la page Répertoires, sous la section Évaluations des annuaires, choisissez Créer une évaluation.

Pour créer une évaluation d'annuaire

1. Sur la page d'évaluation de la création d'un annuaire, pour le nom DNS du répertoire, entrez votre nom DNS Active Directory autogéré.
2. Pour les adresses IP DNS, entrez deux adresses IP DNS pour votre AD autogéré.
3. L'annuaire hybride nécessite un Amazon VPC avec au moins deux sous-réseaux. Si vous ne les avez pas déjà, vous pouvez les créer. Dans la section Mise en réseau, fournissez les informations suivantes :
 - a. Pour VPC, choisissez votre identifiant VPC.

- b. Pour les sous-réseaux, choisissez l'identifiant de chacun des deux sous-réseaux. Chaque sous-réseau doit se trouver dans des zones de disponibilité différentes. Pour de plus amples informations, veuillez consulter [Exigences relatives au réseau Amazon VPC](#).
 - c. Pour Groupe de sécurité, choisissez l'identifiant du groupe de sécurité. Par défaut, AWS attache un groupe de sécurité pour autoriser l'accès réseau aux nœuds AWS Secrets Manager gérés de votre Amazon VPC. Vous pouvez éventuellement fournir votre propre groupe de sécurité qui autorise le trafic réseau à destination et en provenance de vos contrôleurs de domaine autogérés en dehors de votre Amazon VPC.
4. Dans la section AWS Systems Manager nœuds, choisissez deux nœuds ou instances de Systems Manager en fonction des exigences suivantes :
 - Si votre Active Directory est autogéré en dehors de AWS Cloud, vous aurez besoin de deux nœuds Systems Manager pour un environnement hybride et multicloud. Pour plus d'informations sur le provisionnement de ces nœuds, consultez la section [Configuration de Systems Manager pour les environnements hybrides et multicloud](#).
 - Si votre Active Directory est autogéré au sein du AWS Cloud, vous aurez besoin de deux EC2 instances gérées par Systems Manager. Pour plus d'informations sur le provisionnement de ces instances, consultez [la section Gestion des EC2 instances avec Systems Manager](#).
5. Choisissez Suivant pour ouvrir la page Révision et créer l'évaluation du répertoire.
6. Sur la page Réviser et créer une évaluation du répertoire, passez en revue les informations d'évaluation du répertoire et apportez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Créer une évaluation. La création de l'évaluation du répertoire prend environ 30 minutes. Vous êtes renvoyé à la page de détails des annuaires. Une bannière verte apparaît lorsque l'évaluation de l'annuaire aboutit.

Warning

Pour créer un annuaire hybride, l'évaluation de l'annuaire doit passer à l'état SUCCESS. Vous ne pouvez pas créer un annuaire hybride sans avoir d'abord passé avec succès une évaluation de l'annuaire.

Afficher les évaluations des annuaires

Vous pouvez consulter les évaluations du répertoire dans le AWS Management Console pour consulter les résultats des évaluations et gérer vos rapports d'évaluation.

Pour consulter une évaluation d'un annuaire

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Répertoires, sous la section Évaluations d'annuaires hybrides d'essai, choisissez l'évaluation que vous souhaitez consulter. Cela ouvre la page des détails de l'évaluation.
3. Sur la page des détails de l'évaluation, vous pouvez choisir :
 - Téléchargez pour télécharger le rapport d'évaluation du répertoire sous forme de fichier CSV.
 - Supprimer pour supprimer le rapport d'évaluation de l'annuaire.
 - Créez une évaluation pour créer une nouvelle évaluation de répertoire.
4. Sur la page des détails de l'évaluation, vous pouvez consulter les informations suivantes :
 - a. Informations d'évaluation, telles que l'identifiant de l'évaluation, son statut, s'il a été créé par le client ou par le système, et date de sa dernière mise à jour.
 - b. Informations AD autogérées, telles que le nom DNS, le VPC et les sous-réseaux.
 - c. AWS Systems Manager gère les informations des nœuds, telles que l'adresse IP, le statut de l'évaluation et le nombre de tests d'évaluation réussis et échoués.
 - d. État de l'évaluation pour les contrôleurs de domaine. Vous pouvez également consulter les détails des tests d'évaluation en choisissant les contrôleurs de domaine. Les codes d'erreur apparaissent dans la colonne État en cas d'échec des tests d'évaluation.

Suppression des évaluations d'annuaires

Vous pouvez supprimer les évaluations d'annuaire créées par le client dans le AWS Management Console. Vous ne pouvez pas supprimer les évaluations AWS créées automatiquement à l'initiative du système.

Pour supprimer une évaluation de l'annuaire des clients

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Répertoires, dans la section Évaluations des annuaires, choisissez l'évaluation client que vous souhaitez supprimer. Vous pouvez également cocher la case à côté des évaluations de répertoire que vous souhaitez supprimer, puis sélectionner Supprimer dans le menu Actions.

3. Vous êtes redirigé vers la page de détails des évaluations. Choisissez Actions, puis sélectionnez Supprimer l'évaluation. Une boîte de dialogue d'évaluation de la suppression du répertoire s'affiche. Sélectionnez Supprimer.

Résolution des problèmes liés aux annuaires hybrides et évaluation des annuaires

Une évaluation de l'annuaire est nécessaire pour créer un annuaire hybride. Les tests d'évaluation sont exécutés sur chaque contrôleur de domaine. Les tests d'évaluation examinent différents domaines et donnent le statut « réussi » ou « échec ». Si l'évaluation de votre annuaire échoue, vous pouvez consulter les tests d'évaluation de vos contrôleurs de domaine pour identifier les problèmes à l'origine de l'échec.

Important

Un annuaire hybride peut être créé lorsque le statut de l'évaluation du répertoire est transmis avec avertissement. Nous vous recommandons de résoudre le problème à l'origine de l'avertissement avant de créer un répertoire hybride

Rubriques

- [Résolution des problèmes liés à l'échec de l'évaluation de](#)
- [Erreurs d'état du répertoire](#)
- [Messages d'erreur d'évaluation de l'annuaire](#)
- [Messages d'erreur du test d'évaluation](#)
- [Messages d'avertissement relatifs aux tests d'évaluation](#)

Résolution des problèmes liés à l'échec de l'évaluation de

Vous pouvez résoudre les problèmes liés à l'échec de l'évaluation des annuaires à partir de la page Répertoires du AWS Management Console.

1. Connectez-vous à la Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans la section Évaluations du répertoire, sélectionnez l'évaluation de l'annuaire hybride qui a échoué.

3. Sur la page Détails de l'évaluation, passez en revue l'évaluation du répertoire et identifiez le ou les tests qui ont échoué.
 - Les tests d'évaluation du contrôleur de domaine contiendront plus d'informations sur les tests réussis ou échoués. La colonne État fournit plus de détails sur la cause de l'échec du test. Pour consulter les tests d'évaluation de votre contrôleur de domaine, consultez [Afficher les évaluations des annuaires](#).
4. Résolvez les problèmes à l'origine des défaillances de votre Active Directory autogéré ou de votre Microsoft AD AWS géré. Pour plus d'informations, consultez [Messages d'erreur d'évaluation de l'annuaire](#) et [Messages d'erreur du test d'évaluation](#).
5. Revenez à l'évaluation ayant échoué dans la Directory Service console. Choisissez Créer une évaluation dans le message d'avertissement rouge. Consultez [Création d'un annuaire hybride avec votre AD autogéré](#) pour plus d'informations sur la création d'une évaluation d'annuaire.

Erreurs d'état du répertoire

Directory Service les annuaires peuvent rencontrer différents états qui indiquent différents types de problèmes. La compréhension de ces états vous permet de déterminer les étapes de dépannage appropriées.

Types de statut de répertoire

Status	Description	Action requise
Actif	La création du répertoire s'est terminée correctement et fonctionne normalement.	Aucune action requise.
Dégradé	Le répertoire a été créé avec succès, mais le contrôleur de domaine a rencontré des problèmes par la suite. Le système tente une restauration automatique.	Surveillez l'état du répertoire. Si le problème persiste, contactez le AWS Support.
Échec	La création du répertoire a échoué et est irrécupérable.	Supprimez le répertoire défaillant et créez-en un nouveau.

Status	Description	Action requise
Inopérable (AD hybride uniquement)	AWS a détecté un problème de sécurité et a automatiquement isolé le répertoire à des fins de protection. Le répertoire devient complètement inutilisable tant qu'il n'est pas restauré.	Contactez immédiatement AWS Support le centre d'appels. Cet état nécessite une Support intervention pour examiner et restaurer le répertoire.

Messages d'erreur d'évaluation de l'annuaire

Pour créer un annuaire hybride, vous devez passer une évaluation d'annuaire réussie. Les évaluations d'annuaires peuvent échouer pour diverses raisons.

Le tableau suivant présente les messages d'erreur relatifs à l'évaluation des annuaires et indique comment les résoudre.

Messages d'erreur et résolutions relatifs à l'évaluation du répertoire

Message d'erreur d'évaluation du répertoire	Résolution
Cette évaluation a échoué à plusieurs tests sur les deux instances gérées. Examinez les tests qui ont échoué en sélectionnant chaque instance gérée et en les résolvant dans votre répertoire local. Créez ensuite une nouvelle évaluation.	Un ou plusieurs tests d'évaluation de l'annuaire ont échoué pour votre AD autogéré. Consultez le Messages d'erreur du test d'évaluation pour plus d'informations sur les échecs de test spécifiques et leurs solutions.
Cette évaluation a échoué en raison d'une exception de service interne. Réessayez en créant une nouvelle évaluation ou en contactant le service de dépannage.	Essayez de créer une nouvelle évaluation du répertoire. Si cette erreur persiste, contactez Support .
Cette évaluation a échoué en raison d'une autorisation manquante pour effectuer une action telle que <code>ec2:CreateSecurityGroup</code> <code>ec2:DeleteSecurityGroup</code> <code>ec2:CreateNetworkI</code>	Pour créer une évaluation du répertoire, vous Compte AWS avez besoin du nécessaire Compte AWS autorisations .

Message d'erreur d'évaluation du répertoire	Résolution
<pre> interface ,ec2:DeleteNetworkI interface ,ec2:DescribeSubnets ,, etec2:DescribeNetworkInterface . </pre>	
Cette évaluation a échoué en raison d'une autorisation manquante pour effectuer une action telle que <code>ssm:GetConnectionStatus</code> <code>ssm:GetCommandInvocation</code> <code>ssm:ListCommands</code> <code>ssm:SendCommand</code> .	Pour créer une évaluation d'annuaire, vous aurez besoin de deux nœuds Systems Manager dotés du matériel nécessaire Compte AWS autorisations.
Cette évaluation a échoué car vous avez atteint la limite du nombre d'interfaces réseau que vous pouvez créer. Pour plus d'informations, consultez Amazon VPC quotas (Quotas Amazon VPC).	Pour créer une évaluation d'annuaire, vous devez créer une interface réseau et des groupes de sécurité. Le nombre de ressources VPC que vous pouvez créer est limité, mais vous pouvez ajuster certaines de ces limites. Pour plus d'informations, consultez Amazon VPC quotas (Quotas Amazon VPC).
Cette évaluation a échoué car vous avez atteint la limite du nombre de groupes de sécurité que vous pouvez créer ou attribuer à une instance. Pour plus d'informations, consultez Amazon VPC quotas (Quotas Amazon VPC).	Pour créer une évaluation d'annuaire, vous devez créer une interface réseau et des groupes de sécurité. Le nombre de ressources VPC que vous pouvez créer est limité, mais vous pouvez ajuster certaines de ces limites. Pour plus d'informations, consultez Amazon VPC quotas (Quotas Amazon VPC).
Cette évaluation a échoué. Impossible de se connecter aux instances du client depuis AWS Systems Manager.	Pour créer une évaluation d'annuaire, vous aurez besoin de deux AWS Systems Manager nœuds dotés d'un statut connecté. Consultez la section Résolution des problèmes liés à l'agent SSM.

Message d'erreur d'évaluation du répertoire	Résolution
Cette évaluation a échoué à plusieurs tests critiques. Examinez les tests qui ont échoué en sélectionnant chaque instance gérée et résolvez-les dans votre répertoire local. Créez ensuite une nouvelle évaluation.	Un ou plusieurs tests d'évaluation de l'annuaire ont échoué pour votre AD autogéré. Consultez le Messages d'erreur du test d'évaluation pour plus d'informations.

Messages d'erreur du test d'évaluation

Le tableau suivant décrit les messages d'erreur qui peuvent apparaître lors des tests d'évaluation. Ces erreurs indiquent des problèmes de blocage qui doivent être résolus avant de procéder à la configuration de l'annuaire hybride.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Active Directory Services Tester	testActiveDirectoryServices	AD_CRITICAL_SERVICES_NOT_RUNNING	Critical AD Services: [service_list] not running on hostname.	Survient si les AD services requis ne s'exécutent pas dans votre AD autogéré.	Des AD services spécifiques requis doivent être exécutés dans votre AD autogéré. Pour de plus amples informations, veuillez consulter Services Active Directory requis .
Active Directory Services Tester	testActiveDirectoryServices	DOMAIN_CONTROLLER_NOT_FOUND	No domain controllers found for testActiveDirectoryServices.	Occurs if your self-managed AD domain controllers could not be both	Assurez-vous que vos contrôleurs de domaine AD autogérés sont opérationnels et joignables. Vérifiez la

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
				detected and queried during AD service validation.	connectivité réseau et DNS la résolution de vos contrôleurs de domaine AD autogérés.
ADTest de politique de mot de passe	testPasswordPolicies	PASSWORD_POLICY_VIOLATIONS	<i>ErrorMessage</i>	Se produit si votre politique de mot de passe AD autogérée ne répond pas aux exigences de AWS Managed Microsoft AD.	Votre politique de mot de passe AD autogérée doit satisfaire aux exigences relatives aux mots de passe Microsoft AD AWS gérés. Pour plus d'informations, voir Comprendre les politiques de mot de passe Microsoft AD AWS gérées .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test d'existence de l'utilisateur administrateur	testAwsAdminUserExists	ADMINISTRATOR_ACCOUNT_MISSING	AWS Admin user not found or invalid.	Se produit si l'utilisateur administrateur d'annuaire hybride n'existe pas dans le champ AWS Réserve OU sur votre AD autogéré.	Assurez-vous que l'utilisateur administrateur d'annuaire hybride existe dans le champ AWS Réserve OU sur votre AD autogéré. Si l'utilisateur est absent, vérifiez que le compte a été créé correctement lors du processus de configuration de l'annuaire hybride. Mettre à jour un annuaire hybride . Si l'état de votre annuaire hybride ne fonctionne pas, contactez. Support

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS SPNTest utilisateur administrateur	testNoSpnOnAwsAdminAccount	SPN_FOUND_ON_AWS_AD_MIN	Found <i>spnCount</i> Service Principal Names (SPNs) set on AWS admin user <i>Username</i> . Please remove all SPNs from this account.	Se produit si l'utilisateur administrateur d'annuaire hybride en a SPNs configuré un sur votre AD autogéré.	Supprimez tous les noms principaux de service (SPNs) du compte utilisateur de l'administrateur d'annuaire AWS hybride. L'utilisateur administrateur d'annuaire hybride ne doit pas en avoir SPNs configuré, car cela peut interférer avec l'authentification de l'annuaire hybride.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test du contrôleur de domaine non FSMO propriétaire	testAwsDomainNotFsmoOwner	AWS_DC_HOST_LDS_FSMO_ROLE	AWS Domain Controller owns FSMO roles: <i>rolesList</i> . Please remove these roles.	Se produit si vous avez transféré FSMO des rôles (PDC Emulator, RID Master, Infrastructure Master, ou Infrastructure Master) de votre AD autogéré vers le contrôleur de domaine d'annuaire hybride.	Transférez tous les FSMO rôles (PDC Emulator, RID Master, Infrastructure Master) vers vos contrôleurs de domaine AD autogérés avant de continuer. Pour plus d'informations, consultez Microsoft la documentation sur le transfert de FSMO rôles.
AWS Test d'adhésion à un groupe réservé	testValidateAwsReservedGroupMembership	AWS_RESERVED_OU_NOT_FOUND	AWS Reserved OU not found.	Survient si le AWS paramètre Réservé OU sur votre AD autogéré n'existe pas.	Le AWS Réservé OU doit exister sur votre AD autogéré afin de valider l'appartenance au groupe. Contactez Support .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test d'adhésion à un groupe réservé	testValidateAwsReservedGroupMembership	GROUP_MEMBERSHIP_MISMATCH	AWS Reserved OU Group [GroupNameA]: Missing User(s) [Object1], [Object2] and Extra user(s) [Object3].	Se produit si les groupes de la section AWS OU Réservé de votre AD autogéré contiennent des utilisateurs non autorisés.	Supprimez tous les utilisateurs non autorisés OU des groupes AWS réservés sur votre AD autogéré.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS OU ACLs Test réservé	testReservedOuAclsPermissions	RESERVED_OU_NON_COMPLIANT_ACL	AWS Reserved OU ACLs permissions are invalid.	Se produit si le AWS paramètre Réservé OU ACLs sur votre AD autogéré n'applique pas les autorisations de lecture seule aux entités non gérées AWS et n'empêche pas l'accès non autorisé aux AWS ressources gérées.	Vérifiez et corrigez les autorisations sur le champ AWS Réservé OU ACLs de votre AD autogéré. Assurez-vous que les AWS entités non entités n'ont que des autorisations de lecture (ListChildren, ReadProperty, ListObject, ReadControl, GenericRead, Synchronize) et supprimez les autorisations excessives.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test OU GPO des associations réservées	testReservedOuGPOs	AWS_RESERVED_OU_NO_N_RESERVED_GPO_FOUND	Found non-AWS GPOs attached to the AWS Reserved OU: AWS Reserved OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedAwsGpos</i>]. Domain Controllers OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedDcGpos</i>]. Please, remove extra GPOs from the AWS Reserved OU.	Se produit si les contrôleurs AWS OU réservés OU et de domaine de votre AD autogéré sont liés à des personnes non autorisées GPOs.	(Seuls les objets de stratégie de groupe AWS gérés (GPOs) peuvent y être liés OU. Supprimez tout GPOs lien non autorisé aux contrôleurs AWS réservés OU et aux contrôleurs de domaine OU sur votre AD autogéré.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test OU des ressources réservées	testAwsReservedOUResources	AWS_RESERVED_OU_NOT_FOUND	The AWS Reserved OU does not exist. Please contact AWS Support.	Se produit si le paramètre AWS Réservé OU n'existe pas dans votre Active Directory autogéré, ce qui est requis pour la fonctionnalité d'annuaire Microsoft AD AWS géré.	Le AWS Réservé OU doit être créé automatiquement lors de la configuration de l'annuaire hybride et ne doit pas être supprimé. Si cette erreur persiste, contactez Support .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS Test OU des ressources réservées	testAwsReservedOUs	AWS_RESERVED_OUSOURCES_MISMATCH	The following required resources are missing from AWS Reserved OU - Objects: <i>missing objects</i> , GPOs: <i>missing GPOs</i> . The following resources should not exist but were found in AWS Reserved OU: Objects: <i>unexpected objects</i> , GPOs: <i>unexpected GPOs</i>	Se produit si le AWS fichier Réservé OU créé sur votre AD autogéré ne contient pas les objets requis et ne permet pas un fonctionnement correct GPOs de l'annuaire hybride.	Assurez-vous que personne ne modifie le AWS Réservé. OU Il doit contenir les ressources AWS gérées requises. Supprimez tout objet non autorisé ou GPOs contactez Support si les ressources nécessaires sont manquantes.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
AWS OUTest réservé	testClean AwsReservedOU	AWS_RESERVED_RESOURCES_STILL_EXISTS	AWS Reserved OU or AWS Reserved GPO still exists, please delete.	Se produit si les ressources AWS réservées trouvées sur votre AD autogéré à partir d'une configuration d'annuaire hybride précédente existent toujours.	Supprimez le répertoire hybride défaillant existant de la console. Supprimez ensuite tout ce qui est AWS réservé OU et associé GPOs de votre AD autogéré avant de continuer.
BridgeheadTest du contexte de dénomination	testBridgeheadNamingContext	NAMING_CONTEXT_INCONSISTENT	<i>failureDetails</i>	Se produit si la réplication AD autogérée entre les sites utilisant le Bridgehead ne fonctionne pas comme prévu. Cela peut également se produire si les contextes de dénomination ne sont pas synchronisés entre les sites.	Votre bridgehead site AD autogéré doit fonctionner correctement. Vous pouvez approfondir le diagnostic avec <code>:repadmin /bridgehead /verbose</code> . Résolvez les problèmes soulevés par cette évaluation avant de poursuivre.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test de domaine pour enfants	testChildDomain	CHILD_DOMAIN_NOT_SUPPORTED	Child Domains are not supported for Hybrid Directory.	Se produit si votre forêt AD autogérée contient des domaines enfants qui ne sont pas pris en charge par les annuaires Microsoft AD AWS gérés.	AWS Les annuaires Microsoft AD gérés ne prennent pas en charge les domaines enfants. Vous devez utiliser une forêt à domaine unique pour votre AD autogéré. Pour de plus amples informations, veuillez consulter Microsoft Active Directory exigences relatives au domaine .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
DcDiagTester	testDcDiag	DCDIAG_TEST_FAILED	DCDiag test failed due to issue from [formattedFailedTests].	Survient si l'un Microsoft DCDiag des tests échoue sur votre AD autogéré.	AWS utilise DCDiag pour tester votre AD autogéré. S'il y a des erreurs, vous ne pouvez pas créer de répertoire hybride. Pour plus d'informations, consultez Microsoftla documentation.
DNSTest de correspondance IP	testDnsIpMatch	DNS_IP_MISMATCH	DNS IP address does not match expected IP addresses.	Se produit si les adresses DNS IP fournies pour votre AD autogéré ne correspondent pas aux adresses DNS IP de vos contrôleurs de domaine AD autogérés qui sont activés avec. AWS Systems Manager	Indiquez les adresses DNS IP correctes.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
DNSNom : Match Test	testDnsNameMatch	DOMAIN_DNS_NAME_MISMATCH	DNS name does not match expected domain name.	Se produit si le DNS nom fourni pour votre AD autogéré ne correspond pas au DNS nom indiqué sur vos contrôleurs de domaine AD autogérés activés avec AWS Systems Manager.	Entrez le DNS nom correct.
DNSTest des records	testDnsRecords	DNS_RECORD_MISSING	Unable to resolve the following DNS queries: <i>[missingRecordsString]</i> .	Se produit si les Windows DNS enregistrements ne sont pas définis pour le type A NS, SRV et peuvent être interrogés.	Les DNS enregistrements pour Address (A), Namespace (NS), State of Authority (SOA) et Service Record (SRV) doivent être définis et peuvent être interrogés. Pour plus d'informations, consultez Microsoftla documentation.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test du niveau fonctionnel de la forêt de domaines	testDomainForestFunctionalLevel	UNSUPPORTED_FUNCTIONAL_LEVEL	Detected unsupported domain functional level: <i>DomainFunctionalLevel</i> , we require minimum of <i>MinimumDomainMode</i> . Detected unsupported forest functional level: <i>ForestFunctionalLevel</i> , we require minimum of <i>MinimumForestMode</i> .	Se produit si les niveaux fonctionnels de votre domaine AD et de votre forêt autogérés ne répondent pas aux exigences minimales.	Votre AD autogéré doit utiliser notre Windows 2012 R2 niveau 2016 fonctionnel. Pour plus d'informations, consultez Microsoftla documentation .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Tests de santé du domaine	testOnPremDcNumber	DC_NUMBER_BELOW_LIMIT	On-Prem DC count is lower than required number. DC count is <i>NumberOfDc</i> , AWS required number is <i>DcMinimum</i> .	Se produit si votre AD autogéré ne dispose pas du nombre minimum requis de contrôleurs de domaine.	Assurez-vous que votre AD autogéré dispose d'au moins deux contrôleurs de domaine activés avec AWS Systems Manager. Pour de plus amples informations, veuillez consulter Microsoft Active Directory exigences relatives au domaine .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test de domaine existant	testDomainAlreadyJoined	DOMAIN_ALREADY_JOINED	Instance is already joined to a domain.	Se produit si votre domaine AD autogéré est déjà joint à un annuaire hybride existant.	Votre domaine AD autogéré est déjà joint à un annuaire hybride existant. Chaque domaine AD autogéré associé à un annuaire hybride doit être unique. Créez un nouveau domaine AD autogéré ou supprimez-le de la configuration d'annuaire hybride à laquelle il est joint.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
FSMOTest de connectivité	testFsmoConnectivity	FSMO_ROLE_HOLDER_NOT_ROUTABLE	(PDCEmulator Ip: 1.1.1.1, RIDMaster Ip: 1.1.1.1) is not in routable ranges: [2.2.0.0/16, 3.3.0.0/16, 4.4.0.0/16, 5.5.0.0/16, 6.6.0.0/16].	Se produit si FSMO les PDC Emulator rôles and/or RID Master IPs sur votre AD autogéré ne sont pas routables.	Le contrôleur de domaine principal (PDC) doit être routable à tout moment. Plus précisément, la PDC Emulator fin RID Master IPs de votre AD autogéré. Pour de plus amples informations, veuillez consulter Microsoft Active Directory exigences relatives au domaine.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
FSMOTest de connectivité	testFsmoConnectivity	FSMO_ROLE_MISSING	FSMO role(s): <i>[missingRolesString]</i> missing or DNS Record not found.	Se produit si vos contrôleurs de domaine AD autogérés ne peuvent pas accéder à vos FSMO rôles.	Votre rôle Flexible Single Master Operation (FSMO) dans votre AD autogéré doit être connecté à vos contrôleurs de domaine AD autogérés. Pour plus d'informations, consultez Microsoftla documentation.
Test de conflit IP	testIpConflict	IP_RANGE_CONFLICT	Conflicting IP address detected: <i>ipOverlaps</i>	Se produit si vos plages d'adresses IP AD autogérées se chevauchent avec des plages AWS réservées.	Votre AD autogéré ne peut pas utiliser une plage d'adresses IP qui chevauche les plages d' AWS adresses IP réservées. Pour de plus amples informations, veuillez consulter Microsoft Active Directory exigences relatives au domaine.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
KerberosTester	testKerberos	KERBEROS_AUTHENTICATION_FAILED	Unable to get kerberos TGT.	Survient s'il n'est pas configuré correctement et en cours d'utilisation.	Kerberos doit être activé sur votre AD autogéré. Pour plus d'informations, consultez la documentation Microsoft .
LDAPTest de connectivité	testLdapConnectivity	LDAP_TEST_FAILED	Unable to query LDAP with rootDSE call.	Se produit si LDAP cela ne fonctionne pas.	Le protocole Lightweight Directory Access (LDAP) doit être activé et fonctionner sur votre AD autogéré. Pour plus d'informations, consultez la documentation Microsoft .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Contrôleur de domaine non en lecture seule pour le FSMO test	testNotRdcForFsmo	FSMO_FOUN D_ON_RODC	FSMO Role Found on RODC	Survient si votre FSMO rôle de contrôleur de domaine AD autogéré est RODC.	Le contrôleur de domaine de votre AD autogéré ne doit pas utiliser de rôle de contrôleur de domaine en lecture seule (RODC) Flexible Single Master Operation (FSMO). Pour plus d'informations, consultez Microsoftla documentation.
Test de réplication du mot de passe du contrôleur de domaine en lecture seule	testRdcPasswordRe plication	RODC_REPL ICATE_ADM IN_PASSWO RD	ReadOnly Domain Controller password replication is not explicitly denied for following groups: [<i>missingGroupsString</i>].	RODCSurvient s'il est autorisé à répliquer les mots de passe d'administrateur.	RODCPour votre AD autogéré, l'autorisation de répliquer les mots de passe d'administrateur doit être explicitement refusée. Pour plus d'informations, consultez Microsoftla documentation.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test du contrôleur de domaine en lecture seule	testIsDCReadOnly	DC_READONLY_MODE	Provided Domain Controller is set to Read-Only mode.	Se produit si vos contrôleurs de domaine AD autogérés sont en ReadOnlyDC mode.	Votre AD autogéré doit être un contrôleur de domaine en lecture-écriture. Pour plus d'informations sur les types de contrôleurs de domaine, consultez Microsoftla documentation.
Test de connectivité des ports distants	testPortConnectivity	PORT_TEST_FAILED	Connection to <i>TargetDestination</i> failed for TCP ports [<i>failed TCP ports</i>]. UDP ports [<i>failed UDP ports</i>].	Se produit si les ports requis sur votre AWS sous-réseau et sur votre contrôleur de domaine AD autogéré ne sont pas ouverts.	Assurez-vous que tous les ports requis sont ouverts entre votre AWS sous-réseau et votre AD autogéré. Pour plus d'informations, consultez Exigences relatives aux ports réseau.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test de réplication	testRepli cation	REPLICATI ON_FAILED	Replication failed for [<i>failedDSA sString</i>].	Se produit en cas d'échec de la réplication de vos contrôleurs de domaine AD autogérés.	L'état de réplication de vos contrôleurs de domaine AD autogérés doit être réussi. Pour plus d'informations, consultez Microsoftla documentation.
SMBV1Tester	testSMBV1	INSECURE_ SETTING_S MB	SMBv1 is enabled on the system.	Se produit si AD autogéré est actuellement utilisé SMBv1 pour l'authentification.	SMBv1est connu pour être dangereux et doit être désactivé sur votre AD autogéré. Pour plus d'informations, consultez Microsoftla documentation.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
SSMTest des autorisations utilisateur	testSSMUserPermissions	INSUFFICIENT_PERMISSIONS	Systems Manager user does not have required elevated privileges.	Se produit si Windows l'utilisateur utilisé par ne SSM dispose pas de privilèges suffisants.	Vous aurez besoin d'autorisations d'Windows administrateur pour les agents AWS System Manager (SSM) sur votre AD autogéré. Pour de plus amples informations, veuillez consulter Compte AWS autorisations .
SysvolTest de réplication	testSysvolReplication	DFSR_FAILURE_DETECTED	Failed DFSR event logs: <i>failedLog sString</i> .	Se produit si votre AD autogéré ne dispose pas de la bonne méthode de sysvol réplication (DFSR) et si l'une d'entre elles DCs a échoué lors d'un événement de DFSR réplication.	Votre méthode de sysvol réplication AD autogérée (DFSR) doit être efficace. Pour plus d'informations, consultez Microsoftla documentation .

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
GPOTest de haut niveau	testTopLevelEnforcedGPO	TOP_LEVEL_ENFORCED_GPO_FOUND	GroupPolicy cannot be set to Enforced at the Domain Root, Found GPOs: [GposEnforced] set as Enforced.	Se produit si le niveau supérieur de votre AD autogéré est GPOs défini comme appliqué.	Assurez-vous que l'objet de politique de groupe de premier niveau (GPO) de votre domaine AD autogéré n'est pas défini sur Appliqué. Pour plus d'informations, consultez Microsoftla documentation.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test des types de confiance	testTrustTypes	INVALID_TRUST_TYPE	Invalid trust types detected: <i>[InvalidTrustString]</i> , only Uplevel (Microsoft AD) is currently supported.	Se produit si votre AD autogéré possède des types de confiance non pris en charge.	Uplevel est le seul type de confiance pris en charge par l'annuaire hybride. Votre AD autogéré ne peut pas avoir les types de confiance suivants : DCE, MIT, Downlevel . Pour plus d'informations sur les types de confiance , consultez Microsoft la documentation.

Nom du test	Nom court	Code d'erreur	Message d'erreur	Description	Résolution
Test de contrôleur de domaine valide	testValidDC	COMPUTER_NOT_DC	Provided instance is not a domain controller.	Se produit si les instances AD autogérées que vous avez fournies ne sont pas des contrôleurs de domaine ou si elles font déjà partie d'un autre annuaire hybride.	Fournissez des contrôleurs de domaine AD autogérés uniques à cet annuaire hybride. Réessayez avec un nouveau répertoire. Assurez-vous d'avoir supprimé le répertoire hybride défaillant et tout autre répertoire AWS OU de votre AD autogéré.

Messages d'avertissement relatifs aux tests d'évaluation

Le tableau suivant décrit les messages d'avertissement qui peuvent apparaître lors des tests d'évaluation. Ces avertissements constituent des recommandations pour une configuration optimale mais n'empêchent pas la configuration d'annuaires hybrides.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
Tests de santé du domaine	testDisabledStaleUserNumber	STALE_USERS_FOUND	<i>StaleUser Count</i> users were found to be stale,	Cela se produit si certains comptes d'utilisateurs de votre	Nettoyez les comptes utilisateurs périmés.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
			they have not logged in for <i>StaleThreshold</i> days.	AD autogéré ne se sont pas connectés pendant une longue période et peuvent être considérés comme obsolètes ou inactifs.	
Test de la source horaire du contrôleur de domaine	testDCTimeSource	DC_BAD_TIME_SOURCE	Time sources not properly configured for PDC, should use an authoritative source. Time sources not properly configured for <i>dcHostName</i> , should use PDC as source	Se produit si AD autogéré possède la configuration de source de temps correcte et qu'il n'y a pas d'asymétrie temporelle importante par rapport à une AWS source de temps.	Le serveur de temps de votre contrôleur de domaine principal (PDC) est dirigé vers 169.254.169.123. Vos contrôleurs de domaine non principaux doivent être pointés vers le PDC comme source. Pour plus d'informations, consultez Keeping time with Amazon Time Sync Service .

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
Test d'espace libre	testFreeSpace	DISK_SPACE_EXCEEDED	Supported service max capacity of 7 GB exceeded; SysVol + NTDS is currently using: 24 GB)	Survient si votre AD Combined autogéré NTDS et que son Sysvol utilisation dépasse le quota pris en charge.	Votre AD autogéré doit disposer de 24 Go d'espace disque pour les annuaires hybrides.
FSMO RolesTester	testFSMORoles	FSMO_ROLE_TEST_FAILED	PDC Emulator (<i>dc1.example.com</i>) is not among the provided domain controllers. RID Master (<i>dc1.example.com</i>) is not among the provided domain controllers.	Se produit si les rôles FSMO (émulateur PDC et maître RID) ne figurent pas parmi les deux contrôleurs de domaine fournis lorsque vous créez un répertoire hybride.	Votre répertoire hybride doit avoir les deux rôles FSMO (émulateur PDC et maître RID) parmi les deux contrôleurs de domaine que vous fournissez lorsque vous créez un répertoire hybride. Pour plus d'informations, consultez Comment afficher et transférer FSMO des rôles .

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
SSPTest du canal S	testSchannelSSP	TLS_1_2_NOT_ENABLED	Disabled protocol <i>DisabledProtocol</i> is still enabled.	Se produit si un AD autogéré n'utilise pas TLS1.2 de AES256 chiffrement.	Votre AD autogéré doit utiliser TLS 1.2 et AES256 pour les annuaires hybrides.
Test de corruption du disque	testDiskCorruption	DISK_CORRUPTION	Disk corruption detected on <i>Drive</i> .	Se produit en cas de corruption du disque sur votre AD autogéré.	Vos disques AD autogérés ne doivent pas être corrompus.
Test des spécifications du contrôleur de domaine	testDcSpecs	INSUFFICIENT_RESOURCES	<i>numAvailableCores</i> cores detected when <i>requiredCores</i> cores recommended. <i>gbAvailableRam</i> GB ram detected when <i>requiredRam</i> GB recommended.	Se produit si vos contrôleurs de domaine AD autogérés ne répondent pas aux spécifications requises.	Vos contrôleurs de domaine AD autogérés doivent disposer d'au moins 7 Go de RAM et de 2 cœurs de processeur pour les annuaires hybrides.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
DllTest du plugin au niveau du serveur	testServerLevelPluginDll	SERVER_LEVEL_PLUGIN_DLL_IS_SET	ServerLevelPluginDll registry configuration is not permitted.	Se produit si ServerLevelPluginDll est défini sur vos contrôleurs de domaine AD autogérés.	Vos contrôleurs de domaine AD autogérés ne devraient pas avoir été ServerLevelPluginDll configurés.
Autoriser le test NT4 cryptographique	testAllowNT4Crypto	NT4_CRYPTO_NOT_ALLOWED	Registry key AllowNt4Crypto is not allowed.	Se produit si AD autogéré autorise la NT4 cryptographie.	Votre AD autogéré ne doit pas utiliser la NT4 cryptographie. Pour plus d'informations, consultez la documentation Microsoft.
Test des utilisateurs administrateurs orphelins	testOrphanedAdminUsers	ORPHANED_ADMIN_USERS_FOUND	<i>OrphanedUsersCount</i> Orphaned Admin Users Found: [<i>OrphanedUserNames</i>].	Se produit si des utilisateurs administrateurs orphelins existent dans votre AD autogéré.	Supprimez les utilisateurs orphelins de votre AD autogéré avant de continuer.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
Test du nombre d'utilisateurs privilégiés	testPrivilegedUserCount	DOMAIN_ADMIN_COUNT_EXCEEDED	Number of Domain Admins (<i>daCount</i>) exceeded allowance of (<i>allowedDomainAdminCount</i>).	Se produit si le nombre total de vos administrateurs intégrés, administrateurs de domaine et administrateurs d'entreprise sur votre AD a autogéré est supérieur à 5.	Votre environnement AD autogéré ne doit pas comporter plusieurs comptes privilégiés. Vous devez supprimer le nombre excessif de comptes d'administrateur avant de continuer.
Test du nombre d'utilisateurs privilégiés	testPrivilegedUserCount	ENTERPRISE_ADMIN_COUNT_EXCEEDED	Number of Enterprise Admins (<i>eaCount</i>) exceeded allowance of (<i>allowedEnterpriseAdminCount</i>).	Se produit si le nombre total de vos administrateurs intégrés, administrateurs de domaine et administrateurs d'entreprise sur votre AD a autogéré est supérieur à 5.	Votre environnement AD autogéré ne doit pas comporter plusieurs comptes privilégiés. Vous devez supprimer le nombre excessif de comptes d'administrateur avant de continuer.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
Test du nombre d'utilisateurs privilégiés	testPrivilegedUserCount	BUILTIN_ADMINISTRATORS_T_EXCEEDED	Number of Built-in Admins (<i>baCount</i>) exceeded allowance of (<i>allowedAdminCount</i>).	Se produit si le nombre total de vos administrateurs intégrés, administrateurs de domaine et administrateurs d'entreprise sur votre AD a autogéré est supérieur à 5.	Votre environnement AD autogéré ne doit pas comporter plusieurs comptes privilégiés. Vous devez supprimer le nombre excessif de comptes d'administrateur avant de continuer.
NTLMTester	testNTLM	INSECURE_SETTING_NTLM	NTLMv1 is enabled.	Se produit si l'authentification NTLMv1 est activée sur votre AD autogéré.	NT LAN Manager la version 1 (NTLMv1) présente des failles de sécurité connues et ne doit pas être utilisée. NTLMv1 Désactivez-le sur votre AD autogéré. Pour plus d'informations, consultez Microsoft la documentation.

Nom du test	Nom court	Code d'avertissement	Message d'avertissement	Description	Résolution
Test de durée de vie de Tombstone	testTombstoneLifetime	TOMBSTONE _LIFETIME _ABOVE_LIMIT	Tombstone Lifetime is too long. DC Tombstone Lifetime is <i>Tombstone LifeTime</i> , AWS suggested number is <i>Tombstone Maximum</i> days.	Se produit si la durée de vie de Tombstone sur votre annonce autogérée est supérieure à 180 jours.	La durée de vie de la pierre tombale est le nombre de jours avant le retrait d'un objet suppriméAD. La durée de vie de Tombstone pour votre annonce autogérée doit être de 180 jours ou moins. Pour plus d'informations, consultez Microsoftla documentation.

Commencer à utiliser AWS Managed Microsoft AD

AWS Managed Microsoft AD crée un environnement entièrement géré, Microsoft Active Directory dans le AWS Cloud et est alimenté par Windows Server 2019 et fonctionne aux niveaux fonctionnels de la forêt et du domaine R2 R2 2012. Lorsque vous créez un annuaire avec AWS Managed Microsoft AD, vous Directory Service créez deux contrôleurs de domaine et ajoutez le service DNS en votre nom. Les contrôleurs de domaine sont créés dans différents sous-réseaux d'un Amazon VPC. Cette redondance permet de garantir que votre répertoire reste accessible même en cas de panne. Si vous avez besoin de contrôleurs de domaine supplémentaires, vous pouvez les ajouter ultérieurement. Pour de plus amples informations, veuillez consulter [Déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré.](#)

Pour une démonstration et une présentation de AWS Managed Microsoft AD, visionnez la YouTube vidéo suivante.

AWS Démo et présentation de Managed Microsoft AD

Rubriques

- [Conditions préalables à la création d'un Microsoft AWS AD géré](#)
- [AWS IAM Identity Center prérequis](#)
- [Prérequis pour l'authentification multifactorielle](#)
- [Création de votre AWS compte Microsoft AD géré](#)
- [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#)
- [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#)

Conditions préalables à la création d'un Microsoft AWS AD géré

Pour créer un annuaire Microsoft AD Active Directory AWS géré, vous avez besoin d'un Amazon VPC avec les éléments suivants :

- Au moins deux sous-réseaux. Chacun des sous-réseaux doit se trouver dans une zone de disponibilité différente et doit être du même type de réseau.

Vous pouvez l'utiliser IPv6 pour votre VPC. Pour plus d'informations, consultez la section relative à [la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

- Le VPC doit avoir la location matérielle par défaut.
- Vous ne pouvez pas créer un Microsoft AD AWS géré dans un VPC à l'aide des adresses de l'espace d'adressage 198.18.0.0/15.

Si vous devez intégrer votre domaine Microsoft AD AWS géré à un domaine Active Directory local existant, les niveaux fonctionnels de forêt et de domaine de votre domaine local doivent être définis sur Windows Server 2003 ou une version ultérieure.

Directory Service utilise une structure à deux VPC. Les EC2 instances qui composent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, ETH0 et ETH1. ETH0 est la carte de gestion et existe en dehors de votre compte. ETH1 est créé au sein de votre compte.

La plage IP de gestion du réseau ETH0 de votre annuaire est 198.18.0.0/15.

Pour un didacticiel sur la création de l' AWS environnement et sur AWS Managed Microsoft AD, consultez [AWS Tutoriels de laboratoire de test Microsoft AD gérés](#).

AWS IAM Identity Center prérequis

Si vous envisagez d'utiliser IAM Identity Center avec AWS Managed Microsoft AD, vous devez vous assurer que les conditions suivantes sont réunies :

- Votre répertoire Microsoft AD AWS géré est configuré dans le compte de gestion de votre AWS organisation.
- Votre instance d'IAM Identity Center se trouve dans la même région que celle dans laquelle votre répertoire Microsoft AD AWS géré est configuré.

Pour plus d'informations, consultez les [conditions requises pour IAM Identity Center](#) dans le guide de l'AWS IAM Identity Center utilisateur.

Prérequis pour l'authentification multifactorielle

Pour prendre en charge l'authentification multifactorielle avec votre annuaire Microsoft AD AWS géré, vous devez configurer votre serveur RADIUS ([Remote Authentication Dial-In User Service](#)) sur site ou basé sur le cloud de la manière suivante afin qu'il puisse accepter les demandes provenant de votre annuaire AWS Microsoft AD géré dans AWS

1. Sur votre serveur RADIUS, créez deux clients RADIUS pour représenter les deux contrôleurs de domaine Microsoft AD AWS gérés (DCs) dans AWS. Vous devez configurer les deux clients à l'aide des paramètres communs suivants (votre serveur RADIUS peut être différent) :
 - Adresse (DNS ou IP) : il s'agit de l'adresse DNS de l'un des AWS services Microsoft AD gérés DCs. Les deux adresses DNS se trouvent dans la console AWS Directory Service sur la page Détails de l'annuaire Microsoft AD AWS géré dans lequel vous prévoyez d'utiliser le MFA. Les adresses DNS affichées représentent les adresses IP des deux AWS services Microsoft AD DCs gérés utilisés par AWS.
- 
- ### Note
- Si votre serveur RADIUS prend en charge les adresses DNS, vous ne devez créer qu'une seule configuration du client RADIUS. Dans le cas contraire, vous devez créer une configuration client RADIUS pour chaque Microsoft AD DC AWS géré.
- Port number : configurez le numéro de port sur lequel votre serveur RADIUS accepte les connexions client RADIUS. Le port RADIUS standard est 1812.

- **Shared secret** : entrez ou générez un secret partagé qui sera utilisé par le serveur RADIUS pour se connecter aux clients RADIUS.
 - **Protocole** : vous devrez peut-être configurer le protocole d'authentification entre le AWS Managed Microsoft AD DCs et le serveur RADIUS. Les protocoles pris en charge sont PAP, CHAP MS- CHAPv1 et MS-. CHAPv2 MS- CHAPv2 est recommandé car il offre la plus grande sécurité des trois options.
 - **Application name** : ce paramètre facultatif sur certains serveurs RADIUS, identifie généralement l'application dans des messages ou des rapports.
2. Configurez votre réseau existant pour autoriser le trafic entrant depuis les clients RADIUS (adresses DCs DNS Microsoft AD AWS gérées, voir étape 1) vers le port de votre serveur RADIUS.
 3. Ajoutez une règle au groupe de EC2 sécurité Amazon dans votre domaine Microsoft AD AWS géré qui autorise le trafic entrant depuis l'adresse DNS et le numéro de port du serveur RADIUS définis précédemment. Pour plus d'informations, consultez la section [Ajout de règles à un groupe de sécurité](#) dans le Guide de EC2 l'utilisateur.

Pour plus d'informations sur l'utilisation de AWS Managed Microsoft AD avec MFA, consultez.

[Activation de l'authentification multifactorielle pour AWS Managed Microsoft AD](#)

Création de votre AWS compte Microsoft AD géré

Pour créer un nouveau répertoire Microsoft AD Active Directory AWS géré, effectuez les étapes suivantes. Avant de commencer cette procédure, assurez-vous que vous avez terminé les prérequis identifiés dans [Conditions préalables à la création d'un Microsoft AWS AD géré](#).

Pour créer un Microsoft AD AWS géré

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire, puis Configurer un annuaire.
2. Sur la page Select directory type (Sélectionner un type d'annuaire), choisissez AWS Managed Microsoft AD, puis Next (Suivant).
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

Edition

Choisissez entre l'édition Standard ou l'édition Entreprise de AWS Managed Microsoft AD. Pour plus d'informations sur les éditions, veuillez consulter [AWS Directory Service for Microsoft Active Directory](#) (français non garanti).

Nom de DNS de l'annuaire

Nom complet de l'annuaire, par exemple `corp.example.com`.

Note

Si vous prévoyez d'utiliser Amazon Route 53 pour le DNS, le nom de domaine de votre AWS Managed Microsoft AD doit être différent de votre nom de domaine Route 53. Des problèmes de résolution DNS peuvent survenir si Route 53 et AWS Managed Microsoft AD partagent le même nom de domaine.

Nom NetBIOS de l'annuaire

Nom court de l'annuaire, par exemple `CORP`.

Description de l'annuaire

Description facultative de l'annuaire. Cette description peut être modifiée après avoir créé votre AWS Managed Microsoft AD.

Mot de passe administrateur

Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom utilisateur `Admin` et ce mot de passe. Vous pouvez modifier le mot de passe administrateur après avoir créé votre AWS Managed Microsoft AD.

Ce mot de passe ne peut pas contenir le terme « admin ».

Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)

- Chiffres (0-9)
- Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[];:'"<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

(Facultatif) Gestion des utilisateurs et des groupes

Pour activer la AWS gestion des utilisateurs et des groupes Microsoft AD depuis le AWS Management Console, sélectionnez Gérer la gestion des utilisateurs et des groupes dans le AWS Management Console. Pour plus d'informations sur l'utilisation de la gestion des utilisateurs et des groupes, consultez [the section called “Gérez les utilisateurs et les groupes à l'aide de la console, de la CLI ou PowerShell”](#).

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

VPC

Sélectionnez le VPC pour l'annuaire.

Network type (Type de réseau)

Le système d'adressage IP (Internet Protocol) associé à votre VPC et à vos sous-réseaux.

Sélectionnez le bloc CIDR associé à votre VPC existant. Les ressources de votre sous-réseau peuvent être configurées pour être utilisées IPv4 uniquement, IPv6 uniquement ou les deux IPv4 et IPv6 (double pile). Pour plus d'informations, consultez la section [Comparer IPv4 et IPv6](#) le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Sous-réseaux

Sélectionnez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend entre 20 et 40 minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Pour plus d'informations sur ce qui est créé avec votre Microsoft AD AWS géré, consultez ce qui suit :

- [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#)
- [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#)

Articles AWS de blog sur la sécurité connexes

- [Comment déléguer l'administration de votre annuaire Microsoft AD AWS géré à vos utilisateurs Active Directory locaux](#)
- [Comment configurer des politiques de mot de passe encore plus strictes pour répondre à vos normes de sécurité à l'aide Directory Service de AWS Managed Microsoft AD](#)
- [Comment augmenter la redondance et les performances de AWS Microsoft AD Directory Service pour Managed en ajoutant des contrôleurs de domaine](#)
- [Comment activer l'utilisation de postes de travail distants en déployant le gestionnaire de licences de postes de travail Microsoft distants sur AWS Managed Microsoft AD](#)
- [Comment y accéder à l' AWS Management Console aide de AWS Managed Microsoft AD et de vos informations d'identification locales](#)
- [Comment activer l'authentification multifactorielle pour les AWS services à l'aide de AWS Managed Microsoft AD et d'informations d'identification locales](#)
- [Comment vous connecter facilement aux AWS services à l'aide de votre Active Directory local](#)

Qu'est-ce qui est créé avec votre Microsoft AD AWS géré

Lorsque vous créez un Active Directory avec AWS Managed Microsoft AD, Directory Service vous effectuez les tâches suivantes en votre nom :

- Crée et associe automatiquement une interface réseau Elastic (ENI) à chacun de vos contrôleurs de domaine. Chacun d'entre ENIs eux est essentiel pour la connectivité entre votre VPC et les contrôleurs de Directory Service domaine et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, consultez [Elastic Network Interfaces](#) dans le guide de EC2 l'utilisateur Amazon. Le serveur DNS par défaut de l'annuaire Microsoft AD Active Directory AWS géré est le serveur DNS VPC avec Classless Inter-Domain Routing (CIDR) +2. Pour plus d'informations, consultez le [serveur Amazon DNS](#) dans le guide de l'utilisateur Amazon VPC.

 Note

Les contrôleurs de domaine sont déployés par défaut dans deux zones de disponibilité d'une région et connectés à votre Amazon VPC (VPC). Les sauvegardes sont effectuées automatiquement une fois par jour, et les volumes Amazon EBS (EBS) sont chiffrés pour garantir la sécurité des données au repos. Les contrôleurs de domaine qui échouent sont automatiquement remplacés dans la même zone de disponibilité à l'aide de la même adresse IP, et une reprise après sinistre complète peut être effectuée avec la dernière sauvegarde.

- Met en service Active Directory dans votre VPC à l'aide de deux contrôleurs de domaine pour la tolérance aux pannes et la haute disponibilité. Des contrôleurs de domaine supplémentaires peuvent être mis en service pour une résilience et des performances supérieures une fois que l'annuaire a été créé avec succès et qu'il est [actif](#). Pour de plus amples informations, veuillez consulter [Déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré](#).

 Note

AWS n'autorise pas l'installation d'agents de surveillance sur les contrôleurs de domaine Microsoft AD AWS gérés.

- Crée un [groupe AWS de sécurité](#) `sg-1234567890abcdef0` qui établit des règles réseau pour le trafic entrant et sortant de vos contrôleurs de domaine. La règle de trafic sortant par défaut autorise tout le trafic vers toutes les IPv4 adresses. Les règles entrantes par défaut autorisent uniquement le trafic via les ports requis par Active Directory à partir du bloc IPv4 CIDR principal associé à l'hébergement VPC pour votre Microsoft AD géré AWS. Pour plus de sécurité, ENIs les fichiers créés ne sont pas IPs associés à Elastic et vous n'êtes pas autorisé à y associer une adresse IP élastique ENIs. Par conséquent, par défaut, le seul trafic entrant capable de communiquer avec votre Microsoft AD AWS géré est le VPC local. Vous pouvez modifier les règles du groupe de sécurité pour autoriser des sources de trafic supplémentaires, par exemple en provenance d'autres pairs VPCs ou CIDRs accessibles via un VPN. Soyez extrêmement attentif si vous tentez de modifier ces règles, car vous risquez de ne plus pouvoir communiquer avec vos contrôleurs de domaine. Pour plus d'informations, consultez [AWS Meilleures pratiques en matière de gestion de Microsoft AD](#) et [Amélioration de la configuration de sécurité de votre réseau AWS Managed Microsoft AD](#).

Vous pouvez utiliser des [listes de préfixes](#) pour gérer vos blocs CIDR dans le cadre des règles du groupe de sécurité. Les listes de préfixes facilitent la gestion et la configuration des groupes de sécurité et des tables de routage. Vous pouvez consolider plusieurs blocs CIDR avec le même port et les mêmes protocoles afin d'adapter le trafic réseau.

- Dans un Windows environnement, les clients communiquent souvent via le [serveur SMB \(Server Message Block\)](#) ou le port 445. Ce protocole facilite diverses actions telles que le partage de fichiers et d'imprimantes et la communication réseau générale. Vous verrez le trafic des clients sur le port 445 vers les interfaces de gestion de vos contrôleurs de domaine Microsoft AD AWS gérés.

Ce trafic se produit lorsque les clients SMB s'appuient sur la résolution de noms DNS (port 53) et NetBIOS (port 138) pour localiser les ressources de votre domaine Microsoft AD AWS géré. Ces clients sont dirigés vers n'importe quelle interface disponible sur les contrôleurs de domaine lors de la localisation des ressources du domaine. Ce comportement est normal et se produit souvent dans les environnements dotés de plusieurs adaptateurs réseau et dans lesquels [SMB Multicanal](#) permet aux clients d'établir des connexions via différentes interfaces afin d'améliorer les performances et la redondance.

Les règles AWS de groupe de sécurité suivantes sont créées par défaut :

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
ICMP	N/A	AWS Microsoft AD VPC CIDR IPv4 géré	Ping	LDAP Keep Alive, DFS
TCP et UDP	53	AWS Microsoft AD VPC CIDR IPv4 géré	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	88	AWS Microsoft AD VPC CIDR IPv4 géré	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	AWS Microsoft AD VPC CIDR IPv4 géré	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	445	AWS Microsoft AD VPC CIDR IPv4 géré	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP et UDP	464	AWS Microsoft AD VPC CIDR IPv4 géré	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	135	AWS Microsoft AD VPC CIDR IPv4 géré	Réplication	RPC, EPM

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	636	AWS Microsoft AD VPC CIDR IPv4 géré	LDAP SSL	Directory , répliquon, stratégie d'authentification d'utilisateur et d'ordinateur, approbations
TCP	1024-65535	AWS Microsoft AD VPC CIDR IPv4 géré	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP	3268 - 3269	AWS Microsoft AD VPC CIDR IPv4 géré	LDAP GC et LDAP GC SSL	Directory , répliquon, stratégie d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	AWS Microsoft AD VPC CIDR IPv4 géré	Heure Windows	Heure Windows, approbations
UDP	138	AWS Microsoft AD VPC CIDR IPv4 géré	DFSN et NetLogon	DFS, stratégie de groupe

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
Tous	Tous	AWS groupe de sécurité créé pour les contrôleurs de domaine (<i>sg-1234567890abcde f0</i>)	Tout le trafic	

Règles sortantes

Protocole	Plage de ports	Destination	Type de trafic	Utilisation d'Active Directory
Tous	Tous	0.0.0.0/0	Tout le trafic	

- Pour plus d'informations sur les ports et protocoles utilisés par Active Directory, consultez la section [Présentation des services et exigences relatives aux ports réseau pour Windows](#) dans Microsoft la documentation.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Admin et le mot de passe spécifié. Ce compte se trouve sous le Users OU (Par exemple, Corp > Users). Vous utilisez ce compte pour gérer votre répertoire dans le AWS Cloud. Pour de plus amples informations, veuillez consulter [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#).

Important

N'oubliez pas d'enregistrer ce mot de passe. Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous pouvez toutefois réinitialiser un mot de passe depuis la Directory Service console ou à l'aide de l'[ResetUserPasswordAPI](#).

- Crée les trois unités organisationnelles suivantes (OUs) sous la racine du domaine :

Nom de l'unité d'organisation	Description
AWS Delegated Groups	Stocke tous les groupes que vous pouvez utiliser pour déléguer AWS des autorisations spécifiques à vos utilisateurs.
AWS Reserved	Stocke tous les comptes spécifiques à la AWS gestion.
<votrenomdedomaine>	Le nom de cette unité d'organisation est basé sur le nom NetBIOS que vous avez saisi lors de la création de votre annuaire. Si vous n'avez pas spécifié de nom NetBIOS, il comprendra par défaut la première partie du nom DNS de votre annuaire (par exemple, dans le cas de soc.exemple.com, le nom NetBIOS serait soc). Cette unité d'organisation est détenue par AWS et contient tous vos AWS objets de répertoire associés, sur lesquels vous avez le contrôle total. Cette unité d' OUs organisation comporte deux enfants par défaut : les ordinateurs et les utilisateurs. Par exemple : • Corp • Computers (Ordinateurs) • Users

- Crée les groupes suivants dans AWS Delegated Groups OU :

Nom du groupe	Description
AWS Delegated Account Operators	Les membres de ce groupe de sécurité ont peu de capacités de gestion de compte comme les réinitialisations de mots de passe

Nom du groupe	Description
AWS Delegated Active Directory Based Activation Administrators	Les membres de ce groupe de sécurité peuvent créer des objets d'activation de licences en volume Active Directory, ce qui permet aux entreprises d'activer des ordinateurs via une connexion à leur domaine.
AWS Delegated Add Workstations To Domain Users	Les membres de ce groupe de sécurité peuvent joindre 10 ordinateurs à un domaine.
AWS Delegated Administrators	Les membres de ce groupe de sécurité peuvent gérer AWS Managed Microsoft AD, avoir le contrôle total de tous les objets de votre unité d'organisation et gérer les groupes contenus dans leAWS Delegated Groups OU.
AWS Delegated Allowed to Authenticate Objects	Les membres de ce groupe de sécurité ont la possibilité de s'authentifier auprès des ressources informatiques dans le AWS Reserved OU (uniquement nécessaire pour les objets locaux avec des approbations activées par l'authentification sélective).
AWS Delegated Allowed to Authenticate to Domain Controllers	Les membres de ce groupe de sécurité ont la possibilité de s'authentifier auprès des ressources informatiques dans le Domain Controllers OU (uniquement nécessaire pour les objets locaux avec des approbations activées par l'authentification sélective).
AWS Delegated Deleted Object Lifetime Administrators	Les membres de ce groupe de sécurité peuvent modifier l'msDS-DeletedObjectLifetimeobjet, ce qui définit la durée pendant laquelle un objet supprimé pourra être récupéré depuis la corbeille AD.

Nom du groupe	Description
AWS Delegated Distributed File System Administrators	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des espaces de noms FRS, DFS-R et DFS.
AWS Delegated Domain Name System Administrators	Les membres de ce groupe de sécurité peuvent gérer les DNS intégré à Active Directory.
AWS Delegated Dynamic Host Configuration Protocol Administrators	Les membres de ce groupe de sécurité peuvent autoriser des serveurs DHCP Windows dans l'entreprise.
AWS Delegated Enterprise Certificate Authority Administrators	Les membres de ce groupe de sécurité peuvent déployer et gérer une autorité de certification d'entreprise Microsoft.
AWS Delegated Fine Grained Password Policy Administrators	Les membres de ce groupe de sécurité peuvent modifier les stratégies de gestion de mots de passe granulaires prédéfinies.
AWS Delegated FSx Administrators	Les membres de ce groupe de sécurité ont la possibilité de gérer les FSx ressources Amazon.
AWS Delegated Group Policy Administrators	Les membres de ce groupe de sécurité peuvent effectuer des tâches de gestion de stratégies de groupe (créer, modifier, supprimer un lien).
AWS Delegated Kerberos Delegation Administrators	Les membres de ce groupe de sécurité peuvent activer une délégation sur les ordinateurs et les comptes utilisateur.
AWS Delegated Managed Service Account Administrators	Les membres de ce groupe de sécurité peuvent créer et supprimer des comptes de services gérés.

Nom du groupe	Description
AWS Delegated MS-NPRC Non-Compliant Devices	Les membres de ce groupe de sécurité seront exemptés de l'obligation d'exiger des communications par canal sécurisé avec les contrôleurs de domaine. Ce groupe est destiné aux comptes d'ordinateur.
AWS Delegated Remote Access Service Administrators	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des serveurs RAS du groupe de serveurs RAS et IAS.
AWS Delegated Replicate Directory Changes Administrators	Les membres de ce groupe de sécurité peuvent synchroniser les informations de profil dans Active Directory avec le SharePoint serveur.
AWS Delegated Server Administrators	Les membres de ce groupe de sécurité sont inclus dans le groupe d'administrateurs locaux sur tous les ordinateurs liés au domaine.
AWS Delegated Sites and Services Administrators	Les membres de ce groupe de sécurité peuvent renommer l' Default-First-Site-Nameobjet dans Active Directory Sites and Services.
AWS Delegated System Management Administrators	Les membres de ce groupe de sécurité peuvent créer et gérer des objets dans le conteneur System Management.
AWS Delegated Terminal Server Licensing Administrators	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des serveurs de licences Terminal Server dans le groupe de serveurs de licences Terminal Server.
AWS Delegated User Principal Name Suffix Administrators	Les membres de ce groupe de sécurité peuvent ajouter et supprimer des suffixes de noms principaux d'utilisateurs.

 Note

Vous pouvez en ajouter AWS Delegated Groups.

- Crée et applique les objets de stratégie de groupe suivants (GPOs) :

 Note

Vous n'êtes pas autorisé à les supprimer, les modifier ou les GPOs dissocier. Ceci est intentionnel car ils sont réservés à AWS l'usage. Vous pouvez les lier à OUs celui que vous contrôlez si nécessaire.

Nom de la stratégie de groupe	S'applique à	Description
Default Domain Policy	Domaine	Inclut les stratégies de mot de passe de domaine et Kerberos.
ServerAdmins	Tous les comptes d'ordinateurs autres que contrôleurs de domaine	Ajoute le 'AWS Delegated Server Administrators' en tant que membre du BUILTIN Administrators Group.
AWS Reserved Policy\User	AWS Reserved user accounts	Définit les paramètres de sécurité recommandés pour tous les comptes utilisateur du AWS Reserved OU.
AWS Managed Active Directory Policy	Tous les contrôleurs de domaine	Définit les paramètres de sécurité recommandés sur tous les contrôleurs de domaine.

Nom de la stratégie de groupe	S'applique à	Description
TimePolicyNT5DS	Tous les contrôleurs autres que les contrôleurs PDCE de domaine	Définit la politique horaire de tous les contrôleurs autres que les contrôleurs de PDCE domaine afin qu'ils utilisent Windows Time (NT5DS).
TimePolicyPDC	Le contrôleur PDCE de domaine	Définit la politique horaire du contrôleur de PDCE domaine pour utiliser le protocole NTP (Network Time Protocol).
Default Domain Controllers Policy	Non utilisé	Provisionnée lors de la création du domaine, la politique AWS Managed Active Directory est utilisée à sa place.

Si vous souhaitez voir les paramètres de chaque GPO, vous pouvez les afficher à partir d'une instance Windows jointe au domaine avec la [console de gestion des stratégies de groupe \(GPMC\)](#) activée.

- Crée les éléments suivants default local accounts pour AWS la gestion de Microsoft AD :

Important

N'oubliez pas de sauvegarder le mot de passe administrateur. Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous [pouvez toutefois réinitialiser un mot de passe depuis la Directory Service console](#) ou à l'aide de l'[ResetUserPasswordAPI](#).

Admin

AdminII est directory administrator account créé lorsque le AWS Managed Microsoft AD est créé pour la première fois. Vous fournissez un mot de passe pour ce compte lorsque vous créez un AWS Managed Microsoft AD. Ce compte se trouve sous le Users OU (Par exemple,

Corp > Users). Vous utilisez ce compte pour gérer votre Active Directory dans le AWS. Pour de plus amples informations, veuillez consulter [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#).

AWS_111111111111

Tout nom de compte commençant par un AWS trait de soulignement et situé dans AWS Reserved OU est un compte géré par un service. Ce compte géré par le service est utilisé AWS pour interagir avec Active Directory. Ces comptes sont créés lorsque les données de service d' AWS annuaire sont activées et chaque nouvelle AWS application est autorisée sur Active Directory. Ces comptes ne sont accessibles que par les AWS services.

krbtgt account

Il krbtgt account joue un rôle important dans les échanges de tickets Kerberos utilisés par votre Managed AWS Microsoft AD. krbtgt account Il s'agit d'un compte spécial utilisé pour le chiffrement des tickets d'octroi de tickets (TGT) Kerberos, et il joue un rôle crucial dans la sécurité du protocole d'authentification Kerberos. Pour plus d'informations, consultez [la documentation Microsoft](#).

AWS fait automatiquement pivoter le krbtgt account mot de passe de votre Microsoft AD AWS géré deux fois tous les 90 jours. Il y a une période d'attente de 24 heures entre les deux rotations consécutives tous les 90 jours.

Pour plus d'informations sur le compte administrateur et les autres comptes créés par Active Directory, consultez [Microsoft la documentation](#).

AWS Compte administrateur Microsoft AD géré et autorisations de groupe

Lorsque vous créez un AWS annuaire Directory Service pour Microsoft Active Directory, vous AWS créez une unité organisationnelle (UO) pour stocker tous les groupes et comptes AWS associés. Pour plus d'informations sur cette unité d'organisation, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#). Cela inclut le compte Admin. Le compte Admin dispose des autorisations pour effectuer les activités administratives courantes suivantes pour votre unité d'organisation :

- Ajouter, mettre à jour ou supprimer des utilisateurs, des groupes et des ordinateurs. Pour de plus amples informations, veuillez consulter [Gestion des utilisateurs et des groupes dans AWS Managed Microsoft AD](#).

- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs et groupes dans votre unité d'organisation.
- Créez OUs des conteneurs supplémentaires.
- Déléguez le pouvoir des conteneurs supplémentaires OUs et des conteneurs. Pour de plus amples informations, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).
- Créer et associer des stratégies de groupes.
- Restaurer des objets supprimés de la corbeille Active Directory.
- Exécutez les PowerShell modules Active Directory et DNS sur le service Web Active Directory.
- Créer et configurer des comptes de services gérés de groupe. Pour de plus amples informations, veuillez consulter [Comptes de service administrés de groupe](#).
- Configurer la délégation Kerberos contrainte. Pour de plus amples informations, veuillez consulter [Délégation Kerberos contrainte](#).

Le compte Admin dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'évènements DNS
- Afficher les journaux d'évènements de sécurité

Seules les actions répertoriées ici sont autorisées pour le compte Admin. De même, le compte Admin ne détient pas les autorisations liées à toutes les actions sur l'annuaire en dehors de votre unité d'organisation spécifique, comme sur l'unité d'organisation parent.

Considérations

- AWS Les administrateurs de domaine ont un accès administratif complet à tous les domaines hébergés sur AWS. Consultez votre accord AWS et la [FAQ sur la protection AWS des données](#) pour plus d'informations sur la manière dont vous AWS gérez le contenu, y compris les informations d'annuaire, que vous stockez sur AWS les systèmes.

- Nous vous recommandons de ne pas supprimer ou renommer ce compte. Si vous ne souhaitez plus utiliser le compte, nous vous recommandons de définir un mot de passe long (64 caractères aléatoires maximum), puis de désactiver le compte.

Note

AWS a le contrôle exclusif des utilisateurs et groupes privilégiés de l'administrateur du domaine et de l'administrateur d'entreprise. Cela permet AWS d'effectuer la gestion opérationnelle de votre annuaire.

Comptes disposant de droits d'administrateur d'entreprise et de domaine

AWS remplace automatiquement le mot de passe administrateur intégré par un mot de passe aléatoire tous les 90 jours. Chaque fois que le mot de passe administrateur intégré est demandé pour un usage humain, un AWS ticket est créé et enregistré auprès de l'équipe Directory Service. Les informations d'identification du compte sont chiffrées et traitées via des canaux sécurisés. De plus, les informations d'identification du compte administrateur ne peuvent être demandées que par l'équipe Directory Service de direction.

Pour effectuer la gestion opérationnelle de votre annuaire, AWS vous avez le contrôle exclusif des comptes dotés des privilèges d'administrateur d'entreprise et d'administrateur de domaine. Cela inclut le contrôle exclusif du compte administrateur Active Directory. AWS protège ce compte en automatisant la gestion des mots de passe grâce à l'utilisation d'un coffre-fort de mots de passe. Lors de la rotation automatique du mot de passe administrateur, AWS crée un compte utilisateur temporaire et lui accorde les privilèges d'administrateur de domaine. Ce compte temporaire est utilisé en tant que sauvegarde en cas de défaillance de la rotation du mot de passe du compte administrateur. Après avoir réussi à faire pivoter le mot de passe administrateur, AWS supprime le compte administrateur temporaire.

Normalement AWS, le répertoire est entièrement géré par automatisation. Si un processus d'automatisation ne parvient pas à résoudre un problème opérationnel, vous devrez peut-être demander à un ingénieur de support de se connecter à votre contrôleur de domaine (DC) pour effectuer un diagnostic. Dans ces rares cas, AWS implémente un request/notification système pour accorder l'accès. Au cours de ce processus, AWS l'automatisation crée un compte utilisateur à durée limitée dans votre annuaire doté d'autorisations d'administrateur de domaine. AWS associe le compte utilisateur à l'ingénieur chargé de travailler sur votre annuaire. AWS enregistre cette association

dans notre système de journalisation et fournit à l'ingénieur les informations d'identification à utiliser. Toutes les actions réalisées par l'ingénieur sont consignées dans les journaux d'événements Windows. Au terme du temps alloué, l'automatisation supprime le compte utilisateur.

Vous pouvez surveiller les actions du compte administrateur à l'aide de la fonction de transfert de journaux de votre annuaire. Cette fonctionnalité vous permet de transférer les événements de sécurité AD à votre CloudWatch système où vous pouvez mettre en œuvre des solutions de surveillance. Pour de plus amples informations, veuillez consulter [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#).

Les événements de sécurité IDs 4624, 4672 et 4648 sont tous enregistrés lorsqu'une personne se connecte à un DC de manière interactive. Vous pouvez consulter le journal des événements de sécurité Windows de chaque DC à l'aide de l'Observateur d'événements Microsoft Management Console (MMC) à partir d'un ordinateur Windows joint au domaine. Vous pouvez également [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#) envoyer tous les journaux des événements de sécurité aux CloudWatch journaux de votre compte.

Il est possible que des utilisateurs soient parfois créés et supprimés au sein de l'unité d'organisation AWS réservée. AWS est responsable de la gestion et de la sécurité de tous les objets de cette unité d'organisation et de toute autre unité d'organisation ou conteneur pour lesquels nous ne vous avons pas délégué les autorisations d'accès et de gestion. Vous pouvez voir des créations et des suppressions dans cette UO. Cela est dû au fait qu'il Directory Service utilise l'automatisation pour alterner régulièrement le mot de passe de l'administrateur de domaine. Lorsque le mot de passe a effectué une rotation, une sauvegarde est créée en cas d'échec de la rotation. Une fois la rotation réussie, le compte de sauvegarde est automatiquement supprimé. De même, dans les rares cas où un accès interactif est nécessaire à des DCs fins de dépannage, un compte utilisateur temporaire est créé pour qu'un Directory Service ingénieur puisse l'utiliser. Une fois qu'un ingénieur aura terminé son travail, le compte utilisateur temporaire sera supprimé. Notez que chaque fois que des informations d'identification interactives sont demandées pour un annuaire, l'équipe Directory Service de direction en est informée.

Concepts clés et meilleures pratiques pour AWS Managed Microsoft AD

Vous pouvez tirer le meilleur parti de votre AWS Managed Microsoft AD en vous familiarisant avec les concepts clés et les meilleures pratiques. Les concepts clés vous aident à comprendre le fonctionnement de AWS Managed Microsoft AD. Les concepts clés incluent l'apprentissage

d'informations supplémentaires sur le schéma Active Directory, le calendrier d'application des correctifs et les comptes de services gérés par des groupes. Le schéma Active Directory inclut des éléments tels que des attributs, des classes et des objets qui constituent AWS Managed Microsoft AD. AWS applique des mises à jour Microsoft à vos contrôleurs de domaine Microsoft AD gérés en votre nom. Vous pouvez également en savoir plus sur les comptes de services gérés de groupe (gMSAs) et les utiliser avec votre Microsoft AD AWS géré.

Vous pouvez éviter les problèmes liés à votre AWS Managed Microsoft AD en appliquant les meilleures pratiques. Certaines de ces meilleures pratiques incluent :

- Lorsque vous configurez votre AWS Managed Microsoft AD, configurez les groupes de sécurité en fonction de vos besoins, mémorisez l'identifiant et le mot de passe de votre compte administrateur et activez le paramètre du redirecteur conditionnel.
- Lorsque vous utilisez votre AWS Managed Microsoft AD, ne modifiez pas l'unité organisationnelle AWS créée lors de la création de l'annuaire, surveillez les performances à l'aide d'outils tels qu'Amazon CloudWatch et Amazon SNS et utilisez des clients SMB 2.x.
- Lorsque vous programmez des applications pour qu'elles fonctionnent avec AWS Managed Microsoft AD, utilisez le service Windows DC Locator, testez les modifications avant de les déployer dans des environnements de production et utilisez des requêtes LDAP efficaces pour éviter des cycles CPU importants dans un contrôleur de domaine.

Rubriques

- [AWS Concepts clés de Microsoft AD gérés](#)
- [AWS Meilleures pratiques en matière de gestion de Microsoft AD](#)

AWS Concepts clés de Microsoft AD gérés

Vous tirerez le meilleur parti de AWS Managed Microsoft AD si vous vous familiarisez avec les concepts clés suivants.

Rubriques

- [Schéma Active Directory](#)
- [Application de correctifs et maintenance pour AWS Managed Microsoft AD](#)
- [Comptes de service administrés de groupe](#)
- [Délégation Kerberos contrainte](#)

Schéma Active Directory

Un schéma est la définition des attributs et classes qui font partie d'un annuaire distribué et sont similaires aux champs et tables d'une base de données. Les schémas incluent un ensemble de règles qui déterminent le type et le format des données qui peuvent être ajoutées ou incluses dans la base de données. La classe Utilisateur est l'exemple d'une classe qui est stockée dans la base de données. Certains exemples d'attributs de classe utilisateur peuvent inclure le prénom, le nom de famille, le numéro de téléphone de l'utilisateur, etc.

Éléments du schéma

Les attributs, les classes et les objets sont les éléments de base qui sont utilisés pour créer des définitions d'objets dans le schéma. Vous trouverez ci-dessous des détails sur les éléments de schéma qu'il est important de connaître avant de commencer le processus d'extension de votre schéma AWS Managed Microsoft AD.

Attributs

Chaque attribut de schéma, qui est similaire au champ d'une base de données, possède plusieurs propriétés qui définissent les caractéristiques de l'attribut. Par exemple, la propriété utilisée par les clients LDAP pour lire et écrire l'attribut est `LDAPDisplayName`. La propriété `LDAPDisplayName` doit être unique sur tous les attributs et classes. Pour obtenir une liste complète des caractéristiques de l'attribut, veuillez consulter [Characteristics of Attributes](#) (français non garanti) sur le site web MSDN. Pour plus d'informations sur la création d'un nouvel attribut, veuillez consulter [Defining a New Attribute](#) (français non garanti) sur le site web MSDN.

Classes

Les classes sont analogues aux tables dans une base de données et disposent également de plusieurs propriétés à définir. Par exemple, le code `objectClassCategory` définit la catégorie de la classe. Pour obtenir une liste complète des caractéristiques de la classe, veuillez consulter [Characteristics of Object Classes](#) (français non garanti) sur le site web MSDN. Pour plus d'informations sur la création d'une nouvelle classe, veuillez consulter [Defining a New Class](#) (français non garanti) sur le site web MSDN.

Identificateur d'objet (OID)

Chaque classe et attribut doit posséder un OID unique pour tous vos objets. Les fournisseurs de logiciel doivent obtenir leurs propres OID pour garantir l'unicité. L'unicité permet d'éviter les conflits lorsque le même attribut est utilisé par plus d'une application à différentes fins. Pour garantir l'unicité, vous pouvez obtenir un OID racine auprès d'une autorité d'enregistrement

de nom ISO. Sinon, vous pouvez obtenir un OID de base auprès de Microsoft. Pour plus d'informations à leur sujet OIDs et pour savoir comment les obtenir, consultez la section [Identifiants d'objets](#) sur le site Web de MSDN.

Attributs liés à un schéma

Certains attributs sont liés entre deux classes par des liens suivants et précédents. Le meilleur exemple est les groupes. Lorsque vous observez un groupe, il vous montre les membres qui le composent ; si vous observez un utilisateur, vous pouvez voir les groupes auxquels il appartient. Lorsque vous ajoutez un utilisateur à un groupe, Active Directory crée un lien suivant vers le groupe. Ensuite, Active Directory ajoute un lien précédent à partir du groupe de l'utilisateur. Un ID de lien unique doit être généré lors de la création d'un attribut qui sera lié. Pour plus d'informations, veuillez consulter [Linked Attributes](#) (français non garanti) sur le site web MSDN.

Rubriques en relation

- [Quand étendre votre schéma AWS Managed Microsoft AD](#)
- [Tutoriel : extension de votre schéma Microsoft AD AWS géré](#)

Application de correctifs et maintenance pour AWS Managed Microsoft AD

AWS Le service d'annuaire pour Microsoft Active Directory, également connu sous le nom de AWS DS pour AWS Managed Microsoft AD, est en fait les services de domaine Microsoft Active Directory (AD DS), fournis sous forme de service géré. Le système utilise Microsoft Windows Server 2019 pour les contrôleurs de domaine (DCs) et y AWS ajoute un logiciel à des DCs fins de gestion des services. AWS mises à jour (correctifs) DCs pour ajouter de nouvelles fonctionnalités et maintenir le logiciel Microsoft Windows Server à jour. Pendant le processus d'application des correctifs, votre annuaire reste disponible pour utilisation.

Garantie de la disponibilité

Par défaut, chaque répertoire est composé de deux DCs, chacun étant installé dans une zone de disponibilité différente. À votre convenance, vous pouvez en ajouter DCs pour augmenter encore la disponibilité. Pour les environnements critiques nécessitant une haute disponibilité et une tolérance aux pannes, nous recommandons d'en déployer d'autres. DCs AWS applique des correctifs DCs séquentiels, période pendant laquelle le contrôleur de domaine qui applique activement le correctif AWS n'est pas disponible. Si l'un ou plusieurs de vos répertoires DCs sont temporairement hors service, AWS reportez l'application des correctifs jusqu'à ce qu'au moins deux de vos annuaires

soient opérationnels. DCs Cela vous permet d'utiliser l'autre DCs pendant le processus de correction, qui prend généralement 30 à 45 minutes par DC, bien que cette durée puisse varier. Pour garantir que vos applications puissent atteindre un contrôleur de domaine en fonctionnement en cas d'indisponibilité d'un ou de plusieurs d' DCs entre eux pour une raison quelconque, y compris pour l'application de correctifs, vos applications doivent utiliser le service de localisation de contrôleurs de domaine Windows et ne pas utiliser d'adresses de domaine statiques.

Présentation de la planification d'application des correctifs

Pour maintenir le logiciel Microsoft Windows Server à jour sur votre ordinateur DCs, AWS utilise les mises à jour Microsoft. Comme Microsoft met à disposition des correctifs cumulatifs mensuels pour Windows Server, elle AWS fait de son mieux pour tester et appliquer le correctif cumulatif à tous les clients DCs dans un délai de trois semaines calendaires. En outre, il AWS passe en revue les mises à jour publiées par Microsoft en dehors du récapitulatif mensuel en fonction de leur applicabilité et de leur urgence. DCs Pour les correctifs de sécurité considérés comme critiques ou importants par Microsoft et pour lesquels ils sont pertinents DCs, elle AWS met tout en œuvre pour tester et déployer le correctif dans un délai de cinq jours.

Comptes de service administrés de groupe

Avec Windows Server 2012, Microsoft a introduit une nouvelle méthode que les administrateurs pouvaient utiliser pour gérer les comptes de service appelée comptes de service gérés de groupe (gMSAs). Grâce à gMSAs, les administrateurs de service n'ont plus besoin de gérer manuellement la synchronisation des mots de passe entre les instances de service. Un administrateur peut simplement créer un gMSA dans Active Directory, puis configurer plusieurs instances de service pour utiliser ce compte gMSA spécifique.

Pour accorder des autorisations permettant aux utilisateurs de AWS Managed Microsoft AD de créer un GMSA, vous devez ajouter leurs comptes en tant que membre du groupe de sécurité AWS Delegated Managed Service Account Administrators. Par défaut, le compte administrateur est membre de ce groupe. Pour plus d'informations sur gMSAs, consultez la section [Présentation des comptes de services gérés par le groupe](#) sur le TechNet site Web de Microsoft.

Article AWS de blog sur la sécurité connexe

- [Comment AWS Managed Microsoft AD contribue à simplifier le déploiement et à améliorer la sécurité des applications .NET intégrées à Active Directory](#)

Délégation Kerberos contrainte

La délégation Kerberos contrainte est une fonctionnalité de Windows Server. Cette fonctionnalité permet aux administrateurs de services de spécifier et d'appliquer les limites de confiance des applications en limitant la portée dans laquelle les services d'application peuvent agir au nom d'un utilisateur. Cela peut être utile lorsque vous avez besoin de spécifier les comptes de service frontaux qui sont autorisés à déléguer des tâches à leurs services dorsaux. La délégation Kerberos contrainte empêche également votre gMSA de se connecter à n'importe quel service pour le compte de vos utilisateurs Active Directory, ce qui évite le risque d'abus par un développeur malveillant.

Par exemple, supposons que l'utilisateur jsmith se connecte à une application RH. Vous souhaitez que le serveur SQL applique les autorisations de base de données de jsmith. Cependant, par défaut, SQL Server ouvre la connexion à la base de données en utilisant les informations d'identification du compte hr-app-service de service qui s'applique, au lieu des autorisations configurées par jsmith. Vous devez permettre à l'application de paie RH d'accéder à la base de données SQL Server à l'aide des informations d'identification du jsmith. Pour ce faire, vous activez la délégation contrainte Kerberos pour le compte de hr-app-service service dans votre répertoire Managed AWS Microsoft AD dans AWS. Lorsque jdupont se connecte, Active Directory émet un ticket Kerberos que Windows utilise automatiquement lorsque jdupont tente d'accéder à d'autres services sur le réseau. La délégation Kerberos permet au hr-app-service compte de réutiliser le ticket Kerberos jsmith lors de l'accès à la base de données, appliquant ainsi des autorisations spécifiques à jsmith lors de l'ouverture de la connexion à la base de données.

Pour accorder des autorisations permettant aux utilisateurs de AWS Managed Microsoft AD de configurer la délégation contrainte Kerberos, vous devez ajouter leurs comptes en tant que membre du groupe de sécurité AWS Delegated Kerberos Delegation Administrators. Par défaut, le compte administrateur est membre de ce groupe. Pour plus d'informations sur la délégation contrainte de Kerberos, consultez la section [Présentation de la délégation contrainte de Kerberos sur le site Web de Microsoft](#). TechNet

La [délégation contrainte basée sur les ressources](#) a été introduite avec Windows Server 2012. Elle fournit à l'administrateur de service principal la possibilité de configurer la délégation contrainte pour le service.

AWS Meilleures pratiques en matière de gestion de Microsoft AD

Voici quelques suggestions et directives à prendre en compte pour éviter les problèmes et tirer le meilleur parti de AWS Managed Microsoft AD.

Rubriques

- [Bonnes pratiques pour configurer un Microsoft AD AWS géré](#)
- [Bonnes pratiques lors de l'utilisation d'un annuaire Microsoft AD AWS géré](#)
- [Meilleures pratiques lors de la programmation de vos applications pour un Microsoft AD AWS géré](#)

Bonnes pratiques pour configurer un Microsoft AD AWS géré

Voici quelques suggestions et directives à suivre lors de la configuration de votre AWS Managed Microsoft AD :

Rubriques

- [Prérequis](#)
- [Création de votre Microsoft AD AWS géré](#)

Prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.
- AD Connector connecte simplement votre Active Directory local existant à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .
- Simple AD est un annuaire de base à moindres coûts qui offre une compatibilité de base avec Active Directory. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des Directory Service options, voir [Que choisir ?](#).

Assurez-vous que vos instances VPCs et instances sont correctement configurées

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPCs répertoires auxquels ils sont associés. Consultez [Conditions préalables à la création d'un Microsoft AWS AD géré](#), [Conditions préalables requises pour AD Connector](#) ou [Prérequis pour Simple AD](#) pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans [Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré](#).

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez [AWS Quotas Microsoft AD gérés](#), [Quotas AD Connector](#) ou [Quotas Simple AD](#) pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un [groupe de sécurité](#) et l'attache aux [interfaces réseau élastiques](#) du contrôleur de domaine de votre annuaire. Ce groupe de sécurité bloque le trafic inutile vers le contrôleur de domaine et autorise le trafic nécessaire aux communications Active Directory. AWS configure le groupe de sécurité pour ouvrir uniquement les ports requis pour les communications Active Directory. Dans la configuration par défaut, le groupe de sécurité accepte le trafic vers ces ports à partir de l'adresse IPv4 CIDR Microsoft AD VPC AWS gérée. AWS attache le groupe de sécurité aux interfaces de votre contrôleur de domaine accessibles depuis votre peered ou [VPCs](#) redimensionné. Ces interfaces n'étant pas accessibles depuis Internet, même si vous modifiez les tables de routage, changez les connexions réseau vers votre VPC et configurez le [service de passerelle NAT](#). Par conséquent, seules les instances et les ordinateurs qui disposent d'un chemin d'accès réseau dans le VPC peuvent accéder à l'annuaire. Cela simplifie la configuration et vous permet de ne plus avoir à configurer des plages d'adresses spécifiques. Au lieu de cela, vous configurez dans le VPC des routes et des groupes de sécurité qui autorisent uniquement le trafic provenant d'instances et d'ordinateurs approuvés.

Modification du groupe de sécurité de l'annuaire

Si vous souhaitez renforcer la sécurité des groupes de sécurité de votre annuaire, vous pouvez les modifier pour accepter le trafic provenant d'une liste d'adresses IP plus restrictive. Par exemple,

vous pouvez remplacer les adresses acceptées de votre plage d'adresses IPv4 CIDR VPC par une plage d'adresses CIDR spécifique à un sous-réseau ou à un seul ordinateur. De même, vous pouvez choisir de restreindre les adresses de destination vers lesquelles vos contrôleurs de domaine peuvent communiquer. Effectuez ces modifications uniquement si vous avez entièrement compris le fonctionnement du filtrage des groupes de sécurité. Pour plus d'informations, consultez les [groupes EC2 de sécurité Amazon pour les instances Linux](#) dans le guide de EC2 l'utilisateur Amazon. Des modifications inappropriées peuvent entraîner une perte de communication avec les ordinateurs et les instances concernés. AWS recommande de ne pas essayer d'ouvrir des ports supplémentaires vers le contrôleur de domaine car cela réduit la sécurité de votre répertoire. Veuillez lire attentivement le [modèle de responsabilité partagée AWS](#).

 Warning

Il est techniquement possible d'associer les groupes de sécurité utilisés par votre annuaire à d'autres EC2 instances que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances avec lesquelles vous associez le groupe de sécurité de l'annuaire. En outre, l'association du groupe de sécurité de l'annuaire à vos EC2 instances crée un risque de sécurité potentiel pour vos EC2 instances. Le groupe de sécurité de l'annuaire accepte le trafic sur les ports Active Directory requis à partir de l'adresse IPv4 CIDR Microsoft AD VPC AWS gérée. Si vous associez ce groupe de sécurité à une EC2 instance dont l'adresse IP publique est connectée à Internet, n'importe quel ordinateur connecté à Internet peut communiquer avec votre EC2 instance sur les ports ouverts.

Création de votre Microsoft AD AWS géré

Voici quelques suggestions à prendre en compte lors de la création de votre AWS Managed Microsoft AD.

Rubriques

- [Rétention de vos ID et mot de passe d'administrateur](#)
- [Créer un jeu d'options DHCP](#)
- [Activer le paramètre du redirecteur conditionnel](#)
- [Déploiement de contrôleurs de domaine supplémentaires](#)
- [Comprendre les restrictions sur le nom d'utilisateur pour les applications AWS](#)

Rétention de vos ID et mot de passe d'administrateur

Lorsque vous configurez votre annuaire, vous fournissez un mot de passe pour le compte d'administrateur. Cet identifiant de compte est Admin for AWS Managed Microsoft AD. Retenez le mot de passe créé pour ce compte, sinon vous ne serez pas en mesure d'ajouter des objets à votre annuaire.

Créer un jeu d'options DHCP

Nous vous recommandons de créer un ensemble d'options DHCP pour votre Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. De cette façon, toutes les instances de ce VPC peuvent pointer vers le domaine spécifié, et les serveurs DNS peuvent résoudre leurs noms de domaine.

Pour plus d'informations sur les jeux d'options DHCP, veuillez consulter [Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD](#).

Activer le paramètre du redirecteur conditionnel

Les paramètres de transfert conditionnel suivants Stockez ce redirecteur conditionnel dans Active Directory, répliquez-le comme suit : doit être activé. L'activation de ces paramètres garantit que le paramètre du redirecteur conditionnel est persistant lorsqu'un nœud est remplacé en raison d'une défaillance de l'infrastructure ou d'une panne de surcharge.

Les redirecteurs conditionnels doivent être créés sur un contrôleur de domaine avec le paramètre précédent activé. Cela permettra la réplication vers d'autres contrôleurs de domaine.

Déploiement de contrôleurs de domaine supplémentaires

Par défaut, AWS crée deux contrôleurs de domaine qui existent dans des zones de disponibilité distinctes. Cela fournit une résilience aux pannes lors de l'application des correctifs logiciels et d'autres événements qui peuvent rendre un contrôleur de domaine inaccessible ou indisponible. Nous vous recommandons de [déployer des contrôleurs de domaine supplémentaires](#) pour augmenter encore plus la résilience et garantir des performances d'augmentation en cas d'événement à long terme affectant l'accès à un contrôleur de domaine ou à une zone de disponibilité.

Pour de plus amples informations, veuillez consulter [Utiliser le service Windows DC Locator](#).

Comprendre les restrictions sur le nom d'utilisateur pour les applications AWS

Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées

aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications WorkSpaces WorkDocs, telles qu'Amazon WorkMail ou Quick Suite. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces
- Caractères multioctets
- !"#\$%&'()*+,-./:;<=>?@[\\]^`{|}~

 Note

Le symbole @ est autorisé s'il précède un suffixe UPN.

Bonnes pratiques lors de l'utilisation d'un annuaire Microsoft AD AWS géré

Voici quelques suggestions à prendre en compte lorsque vous utilisez votre Microsoft AD AWS géré.

Rubriques

- [Ne pas modifier les utilisateurs, groupes et unités d'organisation prédéfinis](#)
- [Jonction automatique des domaines](#)
- [Configuration appropriée des relations d'approbation](#)
- [Suivez les performances de votre contrôleur de domaine](#)
- [Planifiez soigneusement les extensions de schéma](#)
- [À propos des équilibres de charge](#)
- [Réalisation d'une sauvegarde de votre instance](#)
- [Configuration de la messagerie SNS](#)
- [Appliquer les paramètres du service d'annuaire](#)
- [Supprimez les applications d'entreprise Amazon avant de supprimer un annuaire](#)
- [Utiliser les clients SMB 2.x lors de l'accès aux partages SYSVOL et NETLOGON](#)

Ne pas modifier les utilisateurs, groupes et unités d'organisation prédéfinis

Lorsque vous lancez un annuaire, il AWS crée une unité organisationnelle (Directory Service UO) contenant tous les objets de votre répertoire. Cette unité d'organisation, qui porte le nom NetBIOS

que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine est détenue et gérée par AWS. Plusieurs groupes et un utilisateur administratif sont créés.

Ne déplacez pas, ne supprimez pas ou ne modifiez pas ces objets prédéfinis. Cela peut rendre votre répertoire inaccessible à la fois par vous-même et AWS. Pour de plus amples informations, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Jonction automatique des domaines

Lors du lancement d'une instance Windows destinée à faire partie d'un Directory Service domaine, il est souvent plus facile de rejoindre le domaine dans le cadre du processus de création de l'instance plutôt que de l'ajouter manuellement ultérieurement. Pour joindre automatiquement un domaine, il suffit de sélectionner l'annuaire approprié pour le paramètre Domain join directory lors du lancement d'une nouvelle instance. Pour plus de détails, veuillez consulter [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).

Configuration appropriée des relations d'approbation

Lorsque vous configurez une relation de confiance entre votre annuaire Microsoft AD AWS géré et un autre annuaire, tenez compte des consignes suivantes :

- Le type d'approbation doit correspondre des deux côtés (forêt ou externe)
- Assurez-vous que la direction d'approbation est correctement configurée si vous utilisez une approbation unidirectionnelle (sortante sur le domaine d'approbation, entrante sur le domaine approuvé)
- Les noms de domaine complets (FQDNs) et les noms NetBIOS doivent être uniques entre les forêts et les domaines

Pour plus de détails et des instructions spécifiques sur la configuration d'une relation d'approbation, veuillez consulter [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#).

Suivez les performances de votre contrôleur de domaine

Pour optimiser les décisions de dimensionnement et améliorer la résilience et les performances des annuaires, nous vous recommandons d'utiliser CloudWatch des métriques. Pour de plus amples informations, veuillez consulter [Utilisation CloudWatch pour surveiller les performances de vos contrôleurs de domaine Microsoft AD AWS gérés](#).

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez [Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation](#) dans le blog sur la AWS sécurité.

Planifiez soigneusement les extensions de schéma

Appliquez soigneusement les extensions de schéma de manière à indexer votre annuaire pour les requêtes importantes et fréquentes. Veillez à ne pas trop indexer l'annuaire, car les index consomment de l'espace d'annuaire, et la modification rapide des valeurs indexées risque d'entraîner des problèmes de performance. Pour ajouter des index, vous devez créer un fichier LDIF (Directory Interchange Format) de LDAP (Lightweight Directory Access Protocol) et étendre la modification de votre schéma. Pour de plus amples informations, veuillez consulter [Étendez votre schéma AWS Managed Microsoft AD](#).

À propos des équilibres de charge

N'utilisez pas d'équilibreur de charge devant les points de terminaison Microsoft AD AWS gérés. Microsoft Active Directory (AD) a été conçu pour être utilisé avec un algorithme de découverte du contrôleur de domaine (DC) qui trouve le contrôleur de domaine opérationnel le plus réactif sans équilibrage de charge externe. Les équilibreurs de charge réseau externes ne détectent pas correctement l'activité DCs et peuvent entraîner l'envoi de votre application vers un contrôleur de domaine qui arrive mais qui n'est pas prêt à être utilisé. Pour plus d'informations, voir [Équilibreurs de charge et Active Directory](#) sur Microsoft, TechNet qui recommande de corriger les applications pour qu'elles utilisent correctement Active Directory plutôt que d'implémenter des équilibreurs de charge externes.

Réalisation d'une sauvegarde de votre instance

Si vous décidez d'ajouter manuellement une instance à un Directory Service domaine existant, effectuez d'abord une sauvegarde ou prenez un instantané de cette instance. Cela est particulièrement important lors de la jonction d'une instance Linux. Certaines des procédures utilisées pour ajouter une instance, si elles ne sont pas effectuées correctement, peuvent rendre votre instance inaccessible ou non utilisable. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#).

Configuration de la messagerie SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre

annuaire passe du statut Active au statut Impaired ou Inoperable. Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

N'oubliez pas non plus que si vous avez une rubrique SNS qui reçoit des messages Directory Service, avant de supprimer cette rubrique de la console Amazon SNS, vous devez associer votre annuaire à une autre rubrique SNS. Sinon, vous risquez de manquer des messages importants sur le statut de l'annuaire. Pour savoir comment configurer Amazon SNS, veuillez consulter [Activation des notifications d'état de l'annuaire Microsoft AD AWS géré avec Amazon Simple Notification Service](#).

Appliquer les paramètres du service d'annuaire

AWS Managed Microsoft AD vous permet d'adapter votre configuration de sécurité pour répondre à vos exigences de conformité et de sécurité. AWS Managed Microsoft AD déploie et gère la configuration sur tous les contrôleurs de domaine de votre annuaire, y compris lors de l'ajout de nouvelles régions ou de contrôleurs de domaine supplémentaires. Vous pouvez configurer et appliquer ces paramètres de sécurité à tous vos annuaires nouveaux et existants. Vous pouvez le faire dans la console en suivant les étapes indiquées dans [Modifier les paramètres de sécurité de l'annuaire](#) ou via l'[UpdateSettingsAPI](#).

Pour de plus amples informations, veuillez consulter [Modification des paramètres de sécurité de l'annuaire Microsoft AD AWS géré](#).

Supprimez les applications d'entreprise Amazon avant de supprimer un annuaire

Avant de supprimer un répertoire associé à une ou plusieurs applications Amazon Enterprise telles qu'Amazon WorkSpaces Application Manager WorkSpaces WorkDocs, Amazon ou Amazon WorkMail Relational Database Service (Amazon RDS), vous devez d'abord supprimer chaque application. AWS Management Console Pour en savoir plus sur la suppression de ces applications, veuillez consulter [Suppression de votre Microsoft AD AWS géré](#).

Utiliser les clients SMB 2.x lors de l'accès aux partages SYSVOL et NETLOGON

Les ordinateurs clients utilisent le module SMB (Server Message Block) pour accéder aux partages SYSVOL et NETLOGON sur les contrôleurs de domaine AWS Microsoft AD gérés pour la stratégie de groupe, les scripts de connexion et d'autres fichiers. AWS Managed Microsoft AD prend uniquement en charge les versions SMB 2.0 (SMBv2) et ultérieures.

Les protocoles SMBv2 et les versions plus récentes ajoutent un certain nombre de fonctionnalités qui améliorent les performances des clients et renforcent la sécurité de vos contrôleurs de domaine et de vos clients. Cette modification fait suite aux recommandations de l'équipe de [préparation](#)

[aux situations d'urgence informatique des États-Unis d'Amérique](#) et de [Microsoft](#) concernant la désactivation. SMBv1

 Important

Si vous utilisez actuellement des SMBv1 clients pour accéder aux partages SYSVOL et NETLOGON de votre contrôleur de domaine, vous devez mettre à jour ces clients pour qu'ils soient utilisés ou plus récents. SMBv2 Votre annuaire fonctionnera correctement, mais vos SMBv1 clients ne parviendront pas à se connecter aux partages SYSVOL et NETLOGON de vos contrôleurs de domaine AWS Microsoft AD gérés et ne pourront pas non plus traiter la politique de groupe.

SMBv1 les clients fonctionneront avec tous les autres serveurs de fichiers SMBv1 compatibles dont vous disposez. Il vous AWS recommande toutefois de mettre à jour tous vos serveurs et clients SMB vers une version plus récente. SMBv2 [Pour en savoir plus sur sa désactivation SMBv1 et sa mise à jour vers des versions SMB plus récentes sur vos systèmes, consultez ces articles publiés sur Microsoft TechNet et dans la documentation. Microsoft](#)

Suivi des connexions SMBv1 à distance

Vous pouvez consulter le journal des événements Microsoft-Windows- SMBServer /Audit Windows en vous connectant à distance au contrôleur de domaine AWS Microsoft AD géré. Tous les événements de ce journal indiquent des connexions. SMBv1 Voici un exemple des informations que vous pouvez voir dans l'un de ces journaux :

SMB1 accès

Adresse du client : ###.###.###.###

Conseils :

Cet événement indique qu'un client a tenté d'accéder au serveur en utilisant SMB1. Pour arrêter d'auditer SMB1 l'accès, utilisez l'PowerShellapplet de commande Set-. SmbServerConfiguration

Meilleures pratiques lors de la programmation de vos applications pour un Microsoft AD AWS géré

Avant de programmer vos applications pour qu'elles fonctionnent avec AWS Managed Microsoft AD, tenez compte des points suivants :

Rubriques

- [Utiliser le service Windows DC Locator](#)
- [Testez la charge avant de lancer la production](#)
- [Utilisez des requêtes LDAP efficaces](#)

Utiliser le service Windows DC Locator

Lorsque vous développez des applications, utilisez le service Windows DC Locator ou le service DNS dynamique (DDNS) de votre Managed AWS Microsoft AD pour localiser les contrôleurs de domaine (DCs). Ne codez pas en dur les applications avec l'adresse d'un contrôleur de domaine. Le service de localisation des contrôleurs de domaine permet de garantir que l'annuaire est distribué et vous permet de tirer parti de la mise à l'échelle horizontale en ajoutant des contrôleurs de domaine à votre déploiement. Si vous liez votre application à un contrôleur de domaine fixe et que le contrôleur de domaine est soumis à des correctifs ou à une restauration, votre application perdra l'accès au contrôleur de domaine au lieu d'utiliser l'un des autres contrôleurs. DCs En outre, le codage en dur du contrôleur de domaine peut entraîner la création d'un point chaud sur un seul contrôleur de domaine. Dans des cas extrêmes, la création de ce point chaud peut entraîner une absence de réponse de votre contrôleur de domaine. Dans de tels cas, l'automatisation de l' AWS annuaire peut également signaler le répertoire comme étant altéré et peut déclencher des processus de restauration qui remplacent le contrôleur de domaine qui ne répond pas.

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des objets et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, testez avec des capacités supplémentaires DCs tout en répartissant les demandes entre les DCs. Pour de plus amples informations, veuillez consulter [Déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré](#).

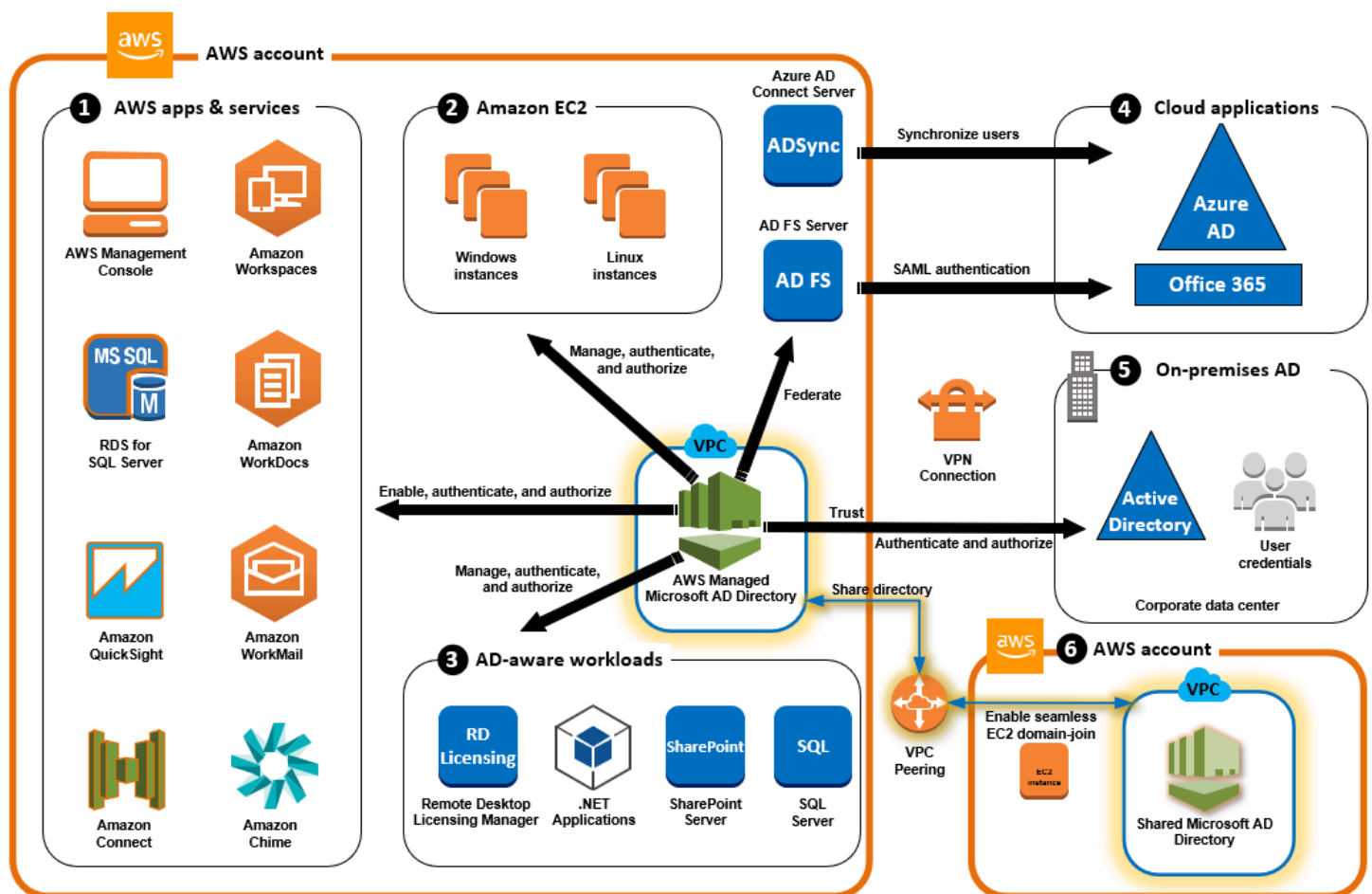
Utilisez des requêtes LDAP efficaces

De vastes requêtes LDAP effectuées dans un contrôleur de domaine sur des dizaines de milliers d'objets peuvent consommer des cycles de processeur considérables sur un seul contrôleur de domaine, ce qui se traduit par la création de points chauds. Ces points chauds peuvent affecter les applications qui partagent le même contrôleur de domaine lors de la requête.

Cas d'utilisation de AWS Managed Microsoft AD

Avec AWS Managed Microsoft AD, vous pouvez partager un répertoire unique pour plusieurs cas d'utilisation. Par exemple, vous pouvez partager un annuaire pour authentifier et autoriser l'accès aux applications .NET, [Amazon RDS for SQL Server](#) avec l'[authentification Windows](#) activée, et [Amazon Chime](#) pour la messagerie et la vidéoconférence.

Le schéma suivant montre certains des cas d'utilisation de votre annuaire Microsoft AD AWS géré. Il s'agit notamment de la possibilité d'accorder à vos utilisateurs l'accès à des applications cloud externes et de permettre à vos utilisateurs Active Directory locaux de gérer les ressources du AWS cloud et d'y avoir accès.



Utilisez AWS Managed Microsoft AD pour l'un des cas d'utilisation professionnels suivants.

Rubriques

- [Cas d'utilisation 1 : connectez-vous aux AWS applications et aux services avec des informations d'identification Active Directory](#)

- [Cas d'utilisation 2 : gestion EC2 des instances Amazon](#)
- [Cas d'utilisation 3 : fournir des services d'annuaire à vos charges de travail compatibles avec Active Directory](#)
- [Cas d'utilisation 4 : AWS IAM Identity Center vers Office 365 et d'autres applications cloud](#)
- [Cas d'utilisation 5 : étendez votre Active Directory local au AWS Cloud](#)
- [Cas d'utilisation 6 : partagez votre annuaire pour associer facilement EC2 des instances Amazon à un domaine sur plusieurs AWS comptes](#)

Cas d'utilisation 1 : connectez-vous aux AWS applications et aux services avec des informations d'identification Active Directory

[Vous pouvez activer plusieurs AWS applications et services tels que Amazon Chime AWS Client VPN AWS Management Console AWS IAM Identity Center, Amazon Connect, Amazon, Quick Suite FSx, Amazon RDS for SQL Server, WorkMail Amazon WorkDocs, WorkSpaces](#) et utiliser votre [annuaire Microsoft AD AWS géré](#). Lorsque vous activez une AWS application ou un service dans votre annuaire, vos utilisateurs peuvent accéder à l'application ou au service avec leurs informations d'identification Active Directory.

Par exemple, vous pouvez permettre à vos utilisateurs de se [connecter à l' AWS Management Console](#) aide de leurs informations d'identification Active Directory. Pour ce faire, vous l'activez en AWS Management Console tant qu'application dans votre annuaire, puis vous assignez vos utilisateurs et groupes Active Directory à des rôles IAM. Lorsque vos utilisateurs se connectent au AWS Management Console, ils assument un rôle IAM pour gérer les AWS ressources. Cela vous permet d'accorder plus facilement à vos utilisateurs un accès à AWS Management Console sans qu'il soit nécessaire de configurer et de gérer une infrastructure SAML distincte.

Pour améliorer encore l'expérience de l'utilisateur final, vous pouvez activer les fonctionnalités d'[authentification unique](#) pour WorkDocs, qui permettent à vos utilisateurs d'accéder à l'annuaire WorkDocs depuis un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Vous pouvez accorder l'accès aux comptes utilisateurs de votre annuaire ou de votre Active Directory local, afin qu'ils puissent se connecter AWS Management Console ou AWS CLI utiliser leurs informations d'identification et autorisations existantes pour gérer les AWS ressources en attribuant des rôles IAM directement aux comptes utilisateurs existants.

FSx pour l'intégration du serveur de fichiers Windows avec AWS Managed Microsoft AD

L'intégration FSx de Windows File Server à AWS Managed Microsoft AD fournit un système de fichiers de protocole SMB (Server Message Block) natif entièrement géré basé sur Microsoft Windows qui vous permet de déplacer facilement vos applications et clients Windows (qui utilisent le stockage de fichiers partagé) vers. AWS Bien que le serveur FSx de fichiers Windows puisse être intégré à un Microsoft Active Directory autogéré, nous n'aborderons pas ce scénario ici.

Cas d' FSx utilisation courants et ressources d'Amazon

Cette section fournit une référence aux ressources communes relatives aux intégrations FSx de serveurs de fichiers Windows avec les cas d'utilisation de AWS Managed Microsoft AD. Chacun des cas d'utilisation présentés dans cette section commence par une configuration Microsoft AD AWS de base et FSx pour une configuration de serveur de fichiers Windows. Pour plus d'informations sur la création de ces configurations, veuillez consulter :

- [Commencer à utiliser AWS Managed Microsoft AD](#)
- [Commencer à utiliser Amazon FSx](#)

FSx pour le serveur de fichiers Windows en tant que stockage persistant sur des conteneurs Windows

[Amazon Elastic Container Service \(ECS\)](#) prend désormais en charge les conteneurs Windows sur les instances de conteneur qui sont lancées avec l'AMI Windows optimisée pour Amazon ECS. Les instances de conteneur Windows utilisent leur propre version de l'agent de conteneur Amazon ECS. Sur l'AMI Windows optimisée pour Amazon ECS, l'agent de conteneur Amazon ECS s'exécute comme un service sur l'hôte.

Amazon ECS prend en charge l'authentification Active Directory pour les conteneurs Windows par l'intermédiaire d'un type de compte de service spécial appelé gMSA (group Managed Service Account). Étant donné que les conteneurs Windows ne peuvent pas être joints à un domaine, vous devez configurer un conteneur Windows pour qu'il s'exécute avec un compte gMSA.

Éléments connexes

- [Utilisation FSx du serveur de fichiers Windows comme stockage persistant sur des conteneurs Windows](#)
- [Comptes de service administrés de groupe](#)

Support Amazon AppStream 2.0

[Amazon AppStream 2.0](#) est un service de streaming d'applications entièrement géré. Il fournit une gamme de solutions permettant aux utilisateurs de sauvegarder et d'accéder aux données par le biais de leurs applications. Amazon FSx with WorkSpaces Applications fournit un disque de stockage persistant personnel à l'aide d'Amazon FSx et peut être configuré pour fournir un dossier partagé permettant d'accéder aux fichiers courants.

Éléments connexes

- [Procédure pas à pas 4 : Utilisation d'Amazon FSx avec Amazon 2.0 AppStream](#)
- [Utilisation d'Amazon FSx avec Amazon AppStream 2.0](#)
- [Utilisation d'Active Directory avec des WorkSpaces applications](#)

Prise en charge de Microsoft SQL Server

FSx pour Windows File Server peut être utilisé comme option de stockage pour Microsoft SQL Server 2012 (à partir de 2012 version 11.x) et les bases de données système plus récentes (y compris Master, Model, MSDB et TempDB), ainsi que pour les bases de données utilisateur du moteur de base de données.

Éléments connexes

- [Installez SQL Server avec un stockage en partage de fichiers SMB](#)
- [Simplifiez vos déploiements de haute disponibilité de Microsoft SQL Server à l'aide FSx de Windows File Server](#)
- [Comptes de service administrés de groupe](#)

Prise en charge des dossiers personnels et des profils d'utilisateurs itinérants

FSx pour Windows File Server peut être utilisé pour stocker les données des dossiers personnels des utilisateurs Active Directory et de Mes documents dans un emplacement central. FSx pour Windows File Server peut également être utilisé pour stocker des données provenant de profils utilisateur itinérants.

Éléments connexes

- [Les annuaires personnels de Windows simplifiés avec Amazon FSx](#)
- [Déploiement de profils d'utilisateurs itinérants](#)

- [Utilisation FSx d'un serveur de fichiers pour Windows avec WorkSpaces](#)

Prise en charge du partage de fichiers en réseau

Les partages de fichiers en réseau sur un serveur de fichiers FSx pour Windows constituent une solution de partage de fichiers gérée et évolutive. L'un des cas d'utilisation est celui des lecteurs mappés pour les clients qui peuvent être créés manuellement ou via une politique de groupe.

Éléments connexes

- [Démonstration 6 : mettre à l'échelle les performances avec Shards](#)
- [Mappage des lecteurs](#)
- [Utilisation FSx d'un serveur de fichiers pour Windows avec WorkSpaces](#)

Prise en charge de l'installation du logiciel de politique de groupe

La taille et les performances du dossier SYSVOL étant limitées, il est recommandé d'éviter de stocker des données telles que des fichiers d'installation de logiciels dans ce dossier. Pour résoudre ce problème, le serveur de fichiers Windows peut être configuré FSx pour stocker tous les fichiers logiciels installés à l'aide de la stratégie de groupe.

Éléments connexes

- [Utiliser la stratégie de groupe pour installer des logiciels à distance](#)

Prise en charge des cibles Windows Server Backup

FSx pour Windows File Server peut être configuré en tant que lecteur cible dans Windows Server Backup à l'aide du partage de fichiers UNC. Dans ce cas, vous devez spécifier le chemin UNC vers votre serveur de fichiers FSx pour Windows plutôt que vers le volume EBS attaché.

Éléments connexes

- [Effectuez une récupération de l'état du système de votre serveur](#)

Amazon prend FSx également en charge le partage d'annuaires Microsoft AD AWS géré. Pour en savoir plus, consultez :

- [Partagez votre Microsoft AD AWS géré](#)

- [Utilisation d'Amazon FSx avec AWS Managed Microsoft AD dans un autre VPC ou un autre compte](#)

Intégration d'Amazon RDS à AWS Managed Microsoft AD

Amazon RDS prend en charge l'authentification externe des utilisateurs de bases de données à l'aide de Kerberos avec Microsoft Active Directory. Kerberos est un protocole d'authentification réseau qui utilise les tickets et la cryptographie de clé symétrique pour vous éviter d'acheminer vos mots de passe via le réseau. La prise en charge de Kerberos et Active Directory par Amazon RDS procure les avantages d'une authentification unique et centralisée des utilisateurs de bases de données, afin que vous puissiez conserver vos informations d'identification dans Active Directory.

Pour commencer à utiliser ce cas d'utilisation, vous devez d'abord configurer une configuration de base de AWS Managed Microsoft AD et Amazon RDS.

- [Commencer à utiliser AWS Managed Microsoft AD](#)
- [Mise en route avec Amazon RDS](#)

Tous les cas d'utilisation mentionnés ci-dessous débiteront par une base AWS Managed Microsoft AD et Amazon RDS et expliqueront comment intégrer Amazon RDS à Managed AWS Microsoft AD.

- [Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS for SQL Server](#)
- [Utilisation de l'authentification Kerberos pour MySQL](#)
- [Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle](#)
- [Utilisation de l'authentification Kerberos avec Amazon RDS for PostgreSQL](#)

Amazon RDS prend également en charge le partage d'annuaires Microsoft AD AWS géré. Pour en savoir plus, consultez :

- [Partagez votre Microsoft AD AWS géré](#)
- [Regrouper vos instances Amazon RDS DB des différents comptes dans un seul domaine partagé](#)

Pour plus d'informations sur la jonction d'un Amazon RDS for SQL Server à votre Active Directory, veuillez consulter [Join Amazon RDS for SQL Server to your self-managed Active Directory](#) (français non garanti).

Application .NET utilisant Amazon RDS for SQL Server avec des comptes de service administrés de groupe

Vous pouvez intégrer Amazon RDS for SQL Server à une application .NET de base et regrouper des comptes de services gérés (MSAs). Pour plus d'informations, consultez [Comment AWS Managed Microsoft AD contribue à simplifier le déploiement et à améliorer la sécurité des applications .NET intégrées à Active Directory](#)

Cas d'utilisation 2 : gestion EC2 des instances Amazon

À l'aide des outils d'administration Active Directory habituels, vous pouvez appliquer des objets de politique de groupe Active Directory (GPOs) pour gérer de manière centralisée vos instances Amazon EC2 pour Windows ou Linux en [joignant vos instances à votre domaine Microsoft AD AWS géré](#).

En outre, vos utilisateurs peuvent se connecter à vos instances à l'aide de leurs informations d'identification Active Directory. Ainsi, vous n'avez plus besoin d'utiliser d'informations d'identification d'instance individuelle ou distribuer de fichiers de clé privée (PEM). Cela vous permet d'accorder ou de révoquer instantanément l'accès aux utilisateurs à l'aide des outils d'administration des utilisateurs Active Directory que vous utilisez déjà.

Cas d'utilisation 3 : fournir des services d'annuaire à vos charges de travail compatibles avec Active Directory

AWS Managed Microsoft AD est un véritable Microsoft Active Directory qui vous permet d'exécuter des charges de travail compatibles avec Active Directory traditionnelles, telles que [Remote Desktop Licensing Manager Microsoft](#), [SharePoint](#) et [Microsoft SQL Server Always On in the Cloud](#). AWS Managed Microsoft AD vous aide également à simplifier et à améliorer la sécurité des applications .NET intégrées à Active Directory en utilisant des [comptes de service gérés de groupe \(gMSAs\) et la délégation contrainte Kerberos](#) (KCD).

Cas d'utilisation 4 : AWS IAM Identity Center vers Office 365 et d'autres applications cloud

Vous pouvez utiliser AWS Managed Microsoft AD pour fournir des AWS IAM Identity Center services pour les applications cloud. Vous pouvez utiliser Microsoft Entra Connect (anciennement connu sous le nom Azure Active Directory Connect) pour synchroniser vos utilisateurs dans Microsoft Entra (anciennement connu sous le nom de Azure Active Directory (AzureAD)), puis utiliser Active Directory Federation Services (AD FS) afin que vos utilisateurs puissent accéder à [Microsoft Office 365](#) et à d'autres applications cloud SAML 2.0 en utilisant leurs informations d'identification Active Directory.

[L'intégration de AWS Managed Microsoft AD à IAM Identity Center](#) ajoute des fonctionnalités SAML à votre AWS Microsoft AD géré et/ou à vos domaines fiables sur site. Une fois intégré, vos utilisateurs peuvent utiliser IAM Identity Center avec des services compatibles avec le AWS Management Console protocole SAML, notamment des applications cloud tierces telles qu'Office 365, Concur et Salesforce, sans avoir à configurer une infrastructure SAML. Pour une démonstration du processus permettant à vos utilisateurs locaux d'utiliser IAM Identity Center, visionnez la vidéo suivante YouTube .

 Note

AWS Single Sign-On a été renommé IAM Identity Center.

Cas d'utilisation 5 : étendez votre Active Directory local au AWS Cloud

Si vous possédez déjà une infrastructure Active Directory et que vous souhaitez l'utiliser lors de la migration de charges de travail compatibles avec Active Directory vers le, AWS Cloud Managed AWS Microsoft AD peut vous aider. Vous pouvez utiliser les [approbations Active Directory](#) pour connecter AWS Managed Microsoft AD à votre Active Directory existant. Cela signifie que vos utilisateurs peuvent accéder aux AWS applications compatibles avec Active Directory avec leurs informations d'identification Active Directory locales, sans que vous ayez à synchroniser les utilisateurs, les groupes ou les mots de passe.

Par exemple, vos utilisateurs peuvent se connecter à Amazon AWS Management Console et à l'aide WorkSpaces de leurs noms d'utilisateur et mots de passe Active Directory existants. En outre, lorsque vous utilisez des applications compatibles SharePoint avec Active Directory, telles que Managed AWS Microsoft AD, les Windows utilisateurs connectés peuvent accéder à ces applications sans avoir à saisir à nouveau leurs informations d'identification.

Vous pouvez également migrer votre domaine Active Directory sur site AWS afin de vous libérer de la charge opérationnelle de votre infrastructure Active Directory à l'aide du [kit de migration Active Directory \(ADMT\)](#) et du service d'exportation de mots de passe (PES) pour effectuer la migration.

Cas d'utilisation 6 : partagez votre annuaire pour associer facilement EC2 des instances Amazon à un domaine sur plusieurs AWS comptes

Le partage de votre répertoire entre plusieurs AWS comptes vous permet de gérer EC2 facilement AWS des services tels qu'[Amazon](#) sans avoir à gérer un annuaire pour chaque compte et chaque

VPC. Vous pouvez utiliser votre annuaire depuis n'importe quel compte AWS et n'importe quel [VPC Amazon](#) à l'intérieur d'une région AWS. Cette fonctionnalité permet de gérer plus facilement et de manière plus rentable les charges de travail basées sur les annuaires avec un seul répertoire pour tous les comptes et VPCs. Par exemple, vous pouvez désormais gérer vos [charges de travail Windows](#) déployées dans des EC2 instances sur plusieurs comptes et VPCs facilement à l'aide d'un seul répertoire Microsoft AD AWS géré.

Lorsque vous partagez votre annuaire Microsoft AD AWS géré avec un autre AWS compte, vous pouvez utiliser la EC2 console Amazon ou [AWS Systems Manager](#) rejoindre facilement vos instances depuis n'importe quel Amazon VPC au sein du compte et AWS de la région. Vous pouvez rapidement déployer vos charges de travail basées sur les annuaires sur des EC2 instances en éliminant le besoin de joindre manuellement vos instances à un domaine ou de déployer des annuaires dans chaque compte et VPC. Pour de plus amples informations, veuillez consulter [Partagez votre Microsoft AD AWS géré](#).

Gérez votre Microsoft AD AWS géré

Vous pouvez utiliser le AWS Management Console pour gérer votre Microsoft AD AWS géré et effectuer des tâches day-to-day administratives. Vous pouvez gérer votre répertoire de différentes manières, notamment :

- [Consultez les détails de votre annuaire Microsoft AD AWS géré](#) pour connaître le type d'annuaire Microsoft AD AWS géré, l'ID du répertoire, le statut du répertoire et les détails du réseau tels que son Amazon VPC, ses sous-réseaux et ses zones de disponibilité.
- [Restaurez votre compte Microsoft AD AWS géré à l'aide de snapshots](#). Vous pouvez également créer et supprimer des instantanés.
- [Déployez des contrôleurs de domaine supplémentaires](#) pour améliorer les performances et la disponibilité de votre solution Microsoft AD AWS gérée.
- [Mettez à niveau votre AWS Managed Microsoft AD](#) de l'édition Standard à l'édition Enterprise, qui prend en charge un plus grand nombre d'objets d'annuaire.
- [Ajoutez un autre nom d'utilisateur principal \(UPN\)](#) pour améliorer l'expérience de connexion de l'utilisateur.
- [Renommez le nom de votre site Microsoft AD AWS géré](#) pour améliorer la capacité de AWS Managed Microsoft AD à rechercher et à authentifier les utilisateurs Active Directory existants dans votre annuaire local.
- [Supprimez votre Microsoft AD AWS géré](#) lorsque vous n'en avez plus besoin.

Affichage des informations de l'annuaire Microsoft AD AWS géré

Vous pouvez utiliser le AWS Management Console pour afficher les détails de votre annuaire Microsoft AD AWS géré, tels que :

- Type de répertoire
- ID de l'annuaire
- État du répertoire
- Détails du réseau pour votre Microsoft AD AWS géré, tels que :
 - Amazon VPC
 - Sous-réseaux
 - Zones de disponibilité
 - Adresses DNS

Vous trouverez les informations suivantes concernant votre Microsoft AD AWS géré :

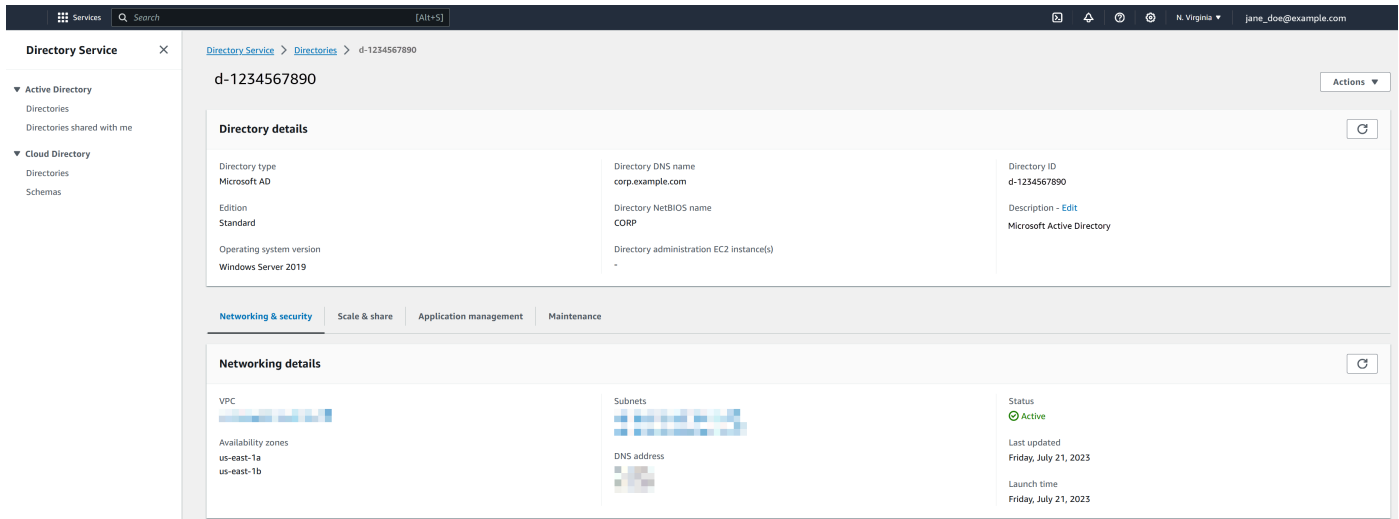
- Dans l'onglet Partager et partager, vous pouvez partager votre Microsoft AD AWS géré avec d'autres personnes Comptes AWS et connaître les détails du réseau de vos contrôleurs de domaine.
- Dans l'onglet Gestion des applications, vous pouvez activer une URL d'accès aux applications pour votre Microsoft AD AWS géré et activer AWS des applications et des services pour votre Microsoft AD AWS géré.
- Dans l'onglet Maintenance, vous pouvez activer Amazon Simple Notification Service pour recevoir des notifications concernant l'état de votre AWS Managed Microsoft AD et consulter des instantanés de votre AWS Managed Microsoft AD.
- Pour de plus amples informations sur le champ Status (Statut), veuillez consulter [Comprendre le statut de votre annuaire Microsoft AD AWS géré](#).

Vous pouvez consulter les informations de l'annuaire Microsoft AD AWS géré à l'aide du AWS Management Console AWS CLI, ou PowerShell :

AWS Management Console

Pour afficher les informations détaillées de l'annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaire.
2. Choisissez le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.



AWS CLI

Pour consulter les informations détaillées de l'annuaire à l'aide du AWS CLI

- Ouvrez le AWS CLI. Pour consulter les informations de votre annuaire Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID du répertoire par votre identifiant de répertoire Microsoft AD AWS géré :

```
aws ds describe-directories --directory-id d-1234567890 --output table
```

Pour de plus amples informations, veuillez consulter [describe-directories](#).

PowerShell

Pour afficher les informations détaillées de l'annuaire avec PowerShell

- Ouvrir PowerShell. Pour consulter les informations de votre annuaire Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID du répertoire par votre identifiant de répertoire Microsoft AD AWS géré :

```
(Get-DSDirectory -DirectoryId d-1234567890 |  
    ForEach-Object {$_, $_.RegionsInfo, $_.VpcSettings}) |  
Format-List *
```

Pour de plus amples informations, veuillez consulter [Get-DSDirectory](#).

Restauration de votre Microsoft AD AWS géré à l'aide de snapshots

AWS Directory Service fournit des instantanés quotidiens automatisés et la possibilité de prendre des instantanés manuels des données pour votre répertoire AWS Microsoft AD Active Directory géré. Ces instantanés peuvent être utilisés pour effectuer une point-in-time restauration de votre Active Directory. Vous êtes limité à cinq instantanés manuels pour chaque répertoire Microsoft AD Active Directory AWS géré. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre. Il est impossible de prendre des instantanés des annuaires AD Connector.

Note

Snapshot est une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez [Configuration de la réplique multirégionale pour AWS Managed Microsoft AD](#), les procédures suivantes doivent être effectuées dans [Région principale](#). Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Rubriques

- [Création d'un instantané de votre annuaire.](#)
- [Restauration de l'annuaire à partir d'un instantané.](#)
- [Suppression d'un instantané](#)

Création d'un instantané de votre annuaire.

Un instantané vous permet de restaurer votre répertoire tel qu'il était au moment où il a été pris. Pour créer un instantané manuel de votre annuaire, exécutez les étapes suivantes.

Note

Vous êtes limité à 5 instantanés manuels par annuaire. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre.

Utilisez la procédure suivante pour créer un instantané manuel de votre AWS Managed Microsoft AD avec le AWS Management Console AWS CLI, ou PowerShell :

AWS Management Console

Pour créer un instantané manuel dans AWS Management Console

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis sélectionnez Créer un instantané.
5. Dans la boîte de dialogue Créer un instantané d'annuaire, entrez une description de l'instantané, si vous le souhaitez. Lorsque vous êtes prêt, choisissez Créer.

AWS CLI

Pour créer un instantané manuel avec AWS CLI

- Ouvrez le AWS CLI. Pour créer un instantané de votre compte Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds create-snapshot --directory-id d-1234567890 --name ManualSnapshot
```

Pour de plus amples informations, veuillez consulter [create-snapshot](#).

PowerShell

Pour créer un instantané manuel avec PowerShell

- Ouvrir PowerShell. Pour créer un instantané de votre compte Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
New-DSSnapshot -DirectoryId d-1234567890 -Name ManualSnapshot
```

Pour de plus amples informations, veuillez consulter [New-DSSnapshot](#).

Selon la taille de votre répertoire, la création de l'instantané peut prendre plusieurs minutes. Lorsque l'instantané est prêt, la valeur Statut devient Completed.

Restauration de l'annuaire à partir d'un instantané.

Restaurer un annuaire à partir d'un instantané revient à le déplacer dans le temps. Les instantanés d'annuaire sont propres à l'annuaire à partir duquel ils ont été créés. Un instantané ne peut être restauré que dans l'annuaire à partir duquel il a été créé. En outre, la durée maximale de prise en charge pour un instantané manuel est de 180 jours. Pour plus d'informations, consultez la section [Durée de conservation utile d'une sauvegarde de l'état du système d'Active Directory](#) sur le Microsoft site Web.

Warning

Nous vous recommandons de contacter le [Centre AWS Support](#) avant toute restauration à partir d'un instantané ; nous pourrions peut-être vous aider à éviter d'avoir à effectuer une restauration à partir d'un instantané. Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné. Il est important que vous sachiez que tous les serveurs DNS DCs et les serveurs DNS associés à l'annuaire seront hors ligne jusqu'à ce que l'opération de restauration soit terminée.

Utilisez la procédure suivante pour restaurer votre répertoire à partir d'un instantané à l'aide du AWS Management Console AWS CLI, ou PowerShell :

AWS Management Console

Pour restaurer un répertoire à partir d'un instantané dans le AWS Management Console

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, sélectionnez un instantané dans la liste, choisissez Actions, puis sélectionnez Restaurer l'instantané.
5. Passez en revue les informations contenues dans la boîte de dialogue Restaurer un instantané d'annuaire, puis sélectionnez Restaurer.

AWS CLI

Pour restaurer un répertoire à partir d'un instantané avec AWS CLI

1. Ouvrez le AWS CLI. Pour répertorier les instantanés de votre Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*].
  {ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. Pour restaurer votre Microsoft AD AWS géré à partir d'un instantané, vous pouvez utiliser la [restore-from-snapshot](#) commande. Assurez-vous de remplacer le snapshot-id paramètre par l'ID de capture que vous souhaitez utiliser pour restaurer votre AWS Managed Microsoft AD :

```
aws ds restore-from-snapshot --snapshot-id s-1234567890
```


PowerShell

Pour restaurer un répertoire à partir d'un instantané avec PowerShell

1. Ouvrir PowerShell. Pour répertorier les instantanés de votre Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Pour restaurer votre Microsoft AD AWS géré à partir d'un instantané, vous pouvez utiliser la [Restore-DSFromSnapshot](#) commande. Assurez-vous de remplacer le snapshot-id paramètre par l'ID de capture que vous souhaitez utiliser pour restaurer votre AWS Managed Microsoft AD :

```
Restore-DSFromSnapshot -SnapshotId s-1234567890
```

Pour un annuaire Microsoft AD AWS géré, la restauration du répertoire peut prendre de deux à trois heures. Une fois la restauration réussie, la valeur Statut du répertoire devient Active. Toutes les modifications apportées à l'annuaire après la date de l'instantané sont remplacées.

Suppression d'un instantané

Utilisez la procédure suivante pour supprimer un instantané de votre AWS Managed Microsoft AD avec AWS Management Console AWS CLI, ou PowerShell :

AWS Management Console

Pour supprimer un instantané dans AWS Management Console

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis Supprimer l'instantané.
5. Vérifiez que vous souhaitez supprimer l'instantané, puis sélectionnez Supprimer.

AWS CLI

Pour supprimer un instantané avec AWS CLI

1. Ouvrez le AWS CLI. Pour répertorier les instantanés de votre Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds describe-snapshots --directory-id d-1234567890 \  
  --query '(sort_by(Snapshots[*].  
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \  
  --output table
```

2. Pour supprimer un instantané de votre Microsoft AD AWS géré, vous pouvez utiliser la [delete-snapshot](#) commande. Assurez-vous de remplacer le snapshot-id paramètre par l'ID du cliché que vous souhaitez supprimer :

```
aws ds delete-snapshot --snapshot-id s-1234567890
```

PowerShell

Pour supprimer un instantané avec PowerShell

1. Ouvrir PowerShell. Pour répertorier les instantanés de votre Microsoft AD AWS géré, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Pour restaurer votre Microsoft AD AWS géré à partir d'un instantané, vous pouvez utiliser la [Remove-DSSnapshot](#) commande. Assurez-vous de remplacer le snapshot-id paramètre par l'ID du cliché que vous souhaitez supprimer :

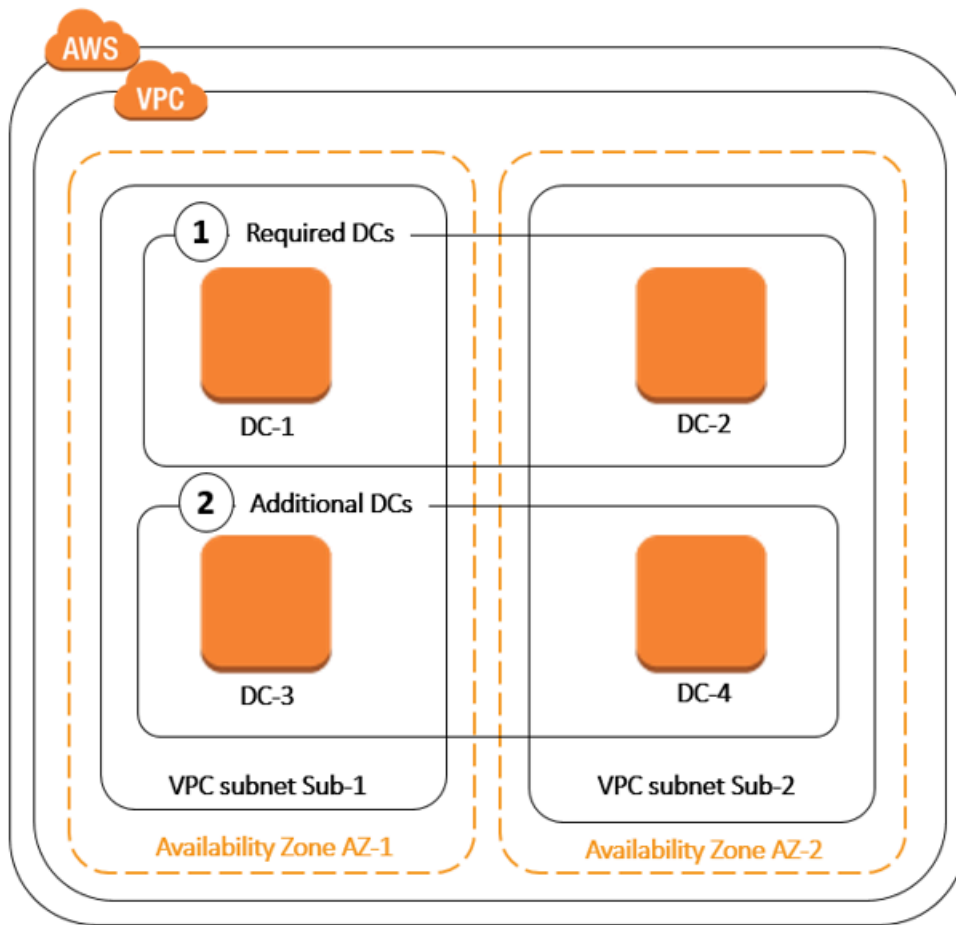
```
Remove-DSSnapshot -SnapshotId s-1234567890
```

Déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré

Le déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré augmente la redondance, ce qui se traduit par une résilience et une disponibilité accrues. Ceci améliore également les performances de votre annuaire, grâce à la prise en charge d'un plus grand nombre de demandes Active Directory. Par exemple, vous pouvez désormais utiliser AWS Managed Microsoft AD pour prendre en charge plusieurs applications .NET déployées sur de vastes flottes d'instances Amazon EC2 et Amazon RDS for SQL Server.

Lorsque vous créez votre annuaire pour la première fois, AWS Managed Microsoft AD déploie deux contrôleurs de domaine dans plusieurs zones de disponibilité, ce qui est nécessaire à des fins de haute disponibilité. Plus tard, vous pouvez facilement déployer des contrôleurs de domaine supplémentaires via la Directory Service console en spécifiant simplement le nombre total de contrôleurs de domaine que vous souhaitez. AWS Managed Microsoft AD distribue les contrôleurs de domaine supplémentaires aux zones de disponibilité et aux sous-réseaux Amazon VPC sur lesquels votre annuaire est exécuté.

Par exemple, dans l'illustration ci-dessous, DC-1 et DC-2 représentent les deux contrôleurs de domaine qui ont été initialement créés avec votre annuaire. La Directory Service console désigne ces contrôleurs de domaine par défaut par le terme « Obligatoire ». AWS Managed Microsoft AD localise intentionnellement chacun de ces contrôleurs de domaine dans des zones de disponibilité distinctes lors du processus de création de l'annuaire. Vous pouvez ensuite décider d'ajouter deux contrôleurs de domaine supplémentaires pour mieux répartir la charge d'authentification sur les pics de connexion. DC-3 et DC-4 représentent les nouveaux contrôleurs de domaine, que la console désigne comme des contrôleurs Supplémentaires. Comme auparavant, AWS Managed Microsoft AD place à nouveau automatiquement les nouveaux contrôleurs de domaine dans différentes zones de disponibilité afin de garantir la haute disponibilité de votre domaine.



Grâce à ce processus, vous n'avez plus besoin de configurer manuellement la réplication des données d'annuaire, la génération automatique des instantanés quotidiens ou la surveillance des contrôleurs de domaine supplémentaires. Il est également plus facile pour vous de migrer et d'exécuter des charges de travail Active Directory essentielles, en intégrant des charges de travail AWS Cloud sans avoir à déployer et à gérer votre propre infrastructure Active Directory.

Vous pouvez utiliser l'un des outils suivants pour déployer ou supprimer des contrôleurs de domaine supplémentaires sur votre Microsoft AD AWS géré :

- [update-number-of-domain-controllers](#) AWS CLI commande
- API [UpdateNumberOfDomainControllers](#)
- [Ajouter ou supprimer des contrôleurs de domaine supplémentaires à l'aide du AWS Management Console](#)

 Note

Les contrôleurs de domaine supplémentaires constituent une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Ajouter ou supprimer des contrôleurs de domaine supplémentaires à l'aide du AWS Management Console

Vous pouvez utiliser le AWS Management Console pour ajouter ou supprimer des contrôleurs de domaine supplémentaires à votre AWS Managed Microsoft AD.

Prérequis

Avant d'ajouter ou de supprimer des contrôleurs de domaine supplémentaires à votre Microsoft AD AWS géré, voici plus d'informations sur les exigences relatives aux contrôleurs de domaine :

- Après le déploiement de contrôleurs de domaine supplémentaires, vous pouvez ramener à deux le nombre de contrôleurs de domaine, ce qui correspond au minimum requis pour garantir la tolérance aux pannes et la haute disponibilité.
- Les contrôleurs de domaine supprimés seront supprimés de la liste des contrôleurs de domaine supplémentaires. Les contrôleurs de domaine principal et secondaire sont obligatoires et ne peuvent pas être supprimés.
- Si vous avez configuré votre AWS Managed Microsoft AD pour activer LDAPS, LDAPS sera également activé automatiquement sur tous les contrôleurs de domaine supplémentaires que vous ajouterez. Pour de plus amples informations, veuillez consulter [Activer le protocole LDAP ou LDAPS sécurisé](#).

Procédure

Utilisez la procédure suivante pour déployer ou supprimer des contrôleurs de domaine supplémentaires dans votre AWS Managed Microsoft AD avec le AWS Management Console AWS CLI, ou PowerShell.

AWS Management Console

Pour ajouter ou supprimer des contrôleurs de domaine supplémentaires à l'aide du AWS Management Console

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez ajouter ou supprimer des contrôleurs de domaine, puis cliquez sur l'onglet Scale & share (Mettre à l'échelle et partager). Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Mettre à l'échelle et partager.
4. Dans la section Domain controllers (Contrôleurs de domaine), choisissez Edit (Modifier).
5. Spécifiez le nombre de contrôleurs de domaine à ajouter ou supprimer de votre annuaire, puis choisissez Modify (Modifier).
6. Lorsque AWS Managed Microsoft AD termine le processus de déploiement, tous les contrôleurs de domaine affichent le statut Actif, et la zone de disponibilité et les sous-réseaux Amazon VPC attribués apparaissent. Les nouveaux contrôleurs de domaine sont également répartis sur les zones de disponibilité et sur les sous-réseaux sur lesquels votre annuaire est déjà déployé.

AWS CLI

Pour ajouter ou supprimer des contrôleurs de domaine supplémentaires avec AWS CLI

1. Ouvrez le AWS CLI. Pour vérifier le nombre actuel de contrôleurs de domaine, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds describe-directories --directory-id d-1234567890 | grep  
DesiredNumberOfDomainControllers
```

2. Pour ajouter ou supprimer des contrôleurs de domaine, vous pouvez utiliser la [update-number-of-domain-controllers](#) commande. Par exemple, vous pouvez utiliser la commande suivante pour définir le nombre total de contrôleurs de domaine sur 4. Assurez-vous de remplacer l'ID de répertoire par votre ID d'annuaire Microsoft AD AWS géré et le `desired-number` paramètre par le nombre de contrôleurs de domaine que vous souhaitez déployer.

```
aws ds update-number-of-domain-controllers --directory-id d-1234567890 --desired-number 4
```

PowerShell

Pour ajouter ou supprimer des contrôleurs de domaine supplémentaires avec PowerShell

1. Ouvrir PowerShell. Pour vérifier le nombre actuel de contrôleurs de domaine, exécutez la commande suivante en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
Get-DSDirectory -DirectoryId d-1234567890 | Select-Object  
DesiredNumberOfDomainControllers
```

2. Pour ajouter ou supprimer des contrôleurs de domaine, vous pouvez utiliser la [Set-DSDomainControllerCount](#) commande. Par exemple, vous pouvez utiliser la commande suivante pour définir le nombre total de contrôleurs de domaine sur 4. Assurez-vous de remplacer l'ID de répertoire par votre ID d'annuaire Microsoft AD AWS géré et le `DesiredNumber` paramètre par le nombre de contrôleurs de domaine que vous souhaitez déployer.

```
Set-DSDomainControllerCount -DirectoryId d-1234567890 -DesiredNumber 4
```

Article AWS de blog sur la sécurité connexe

- [Comment augmenter la redondance et les performances de AWS Microsoft AD Directory Service pour Managed en ajoutant des contrôleurs de domaine](#)

Mise à niveau de votre Microsoft AD AWS géré

Vous pouvez mettre à niveau votre édition Standard AWS Managed Microsoft AD vers l'édition Enterprise. Ce qui suit décrit les différences entre les éditions Standard et Enterprise :

- **Standard Edition** : AWS Managed Microsoft AD (Standard Edition) est optimisé pour être utilisé comme annuaire principal dans les petites et moyennes entreprises comptant jusqu'à 5 000 employés. Il offre suffisamment de capacité de stockage pour prendre en charge jusqu'à 30 000* objets d'annuaire (par exemple, des utilisateurs, des groupes et des ordinateurs).
- **Enterprise Edition** : AWS Managed Microsoft AD (Enterprise Edition) s'adresse aux grandes entreprises qui ont à gérer jusqu'à 500 000* objets d'annuaire.

* Les plafonds indiqués sont fournis à titre indicatif. Votre annuaire peut prendre en charge plus ou moins d'objets d'annuaire, selon la taille de vos objets et le comportement et les besoins de performances de vos applications.

Pour mettre à niveau votre édition Standard AWS Managed Microsoft AD vers l'édition Enterprise, utilisez-la [UpdateDirectorySetup](#) à partir de l'API AWS CLI, ou [update-directory-setup](#) à partir de la [mise à jour et de la DSDirectory configuration](#) Outils AWS pour PowerShell.

API

Pour mettre à niveau votre édition Standard AWS Managed Microsoft AD vers l'édition Enterprise, procédez comme suit :

```
{
  "DirectoryId": "d-1234567890",
  "UpdateType": "SIZE",
  "DirectorySizeUpdateSettings": {
    "DirectorySize": "Large"
  }
}
```

AWS CLI

Pour mettre à niveau votre édition Standard AWS Managed Microsoft AD vers l'édition Enterprise, procédez comme suit :

```
aws ds update-directory-setup \
```



```
--directory-id d-1234567890 \  
--update-type SIZE \  
--directory-size-update-settings DirectorySize=Large
```

PowerShell

Pour mettre à niveau votre édition Standard AWS Managed Microsoft AD vers l'édition Enterprise, procédez comme suit :

```
Update-DSDirectorySetup `   
-DirectoryId d-9a676e4148 `   
-UpdateType SIZE `   
-DirectorySizeUpdateSettings_DirectorySize Large
```

Note

La réplication multirégionale est uniquement disponible dans l'édition AWS Managed Microsoft AD Enterprise pour les régions suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Osaka)
- Asia Pacific (Seoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Thaïlande)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Chine (Beijing)
- Chine (Ningxia)
- Mexique (centre)
- Europe (Francfort)

- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)
- AWS GovCloud (US-Ouest)
- AWS GovCloud (USA Est)

Il existe quelques limites à prendre en compte lors de la mise à niveau de votre Microsoft AD AWS géré. Il s'agit des options suivantes :

- La mise à niveau entraînera un coût supplémentaire. Consultez [Tarification Directory Service](#) pour plus d'informations.
- Une fois votre Active Directory mis à niveau, il est impossible de revenir à son édition précédente.
- Les snapshots précédents ne peuvent pas être utilisés pour restaurer Active Directory après sa mise à niveau.
- Les mises à niveau ont lieu à une date et à une heure planifiées convenues avec vous Support. Les mises à niveau ont lieu du lundi au vendredi, de 9 h à 17 h, heure normale du Pacifique.
- Le processus de mise à niveau prend de quatre à cinq heures.
- Au cours du processus de mise à niveau, les contrôleurs de domaine de votre AWS Managed Microsoft AD sont mis à niveau un par un. Cela peut avoir un impact négatif sur vos performances et provoquer des temps d'arrêt pendant votre période de maintenance.
- Le processus de mise à niveau modifiera le nom d'hôte de chaque instance de contrôleur de domaine, mais leurs adresses IP resteront les mêmes.
- Si vous utilisez le protocole LDAPS (Lightweight Directory Access Protocol over SSL), les contrôleurs de domaine auront besoin de nouveaux certificats.

Mise à jour du type de réseau d'annuaire

Vous pouvez mettre à jour le type de réseau de votre Directory Service annuaire en le faisant IPv4 passer à Dual-stack (IPv4 et IPv6). La mise à jour du type de réseau pour inclure les adresses IPv6 IP fournit un espace d'adressage plus important que IPv4. IPv4 et les IPv6 communications sont indépendantes l'une de l'autre.

Pour plus de détails, consultez la section [Comparer IPv4 et IPv6](#) le guide de l'utilisateur d'Amazon Virtual Private Cloud.

 Important

Il s'agit d'une opération unidirectionnelle qui ne peut pas être inversée. Testez d'abord dans un environnement hors production.

Prérequis

Avant de mettre à jour le type de réseau de votre annuaire, assurez-vous que les conditions suivantes sont remplies :

- Votre VPC et les sous-réseaux associés dans lesquels votre répertoire existe actuellement doivent être configurés avec IPv6 des plages d'adresses CIDR. Pour plus de détails, consultez la section relative [à la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.
- Vous avez un accès administratif au AWS Management Console.
- Votre répertoire doit être à l'état actif.
- Vous disposez des autorisations IAM appropriées pour modifier les Directory Service paramètres.

Pour mettre à jour le type de réseau d'annuaire

Pour mettre à jour votre répertoire vers un réseau à double pile

 Note

Si votre répertoire est répliqué dans plusieurs régions, effectuez cette mise à jour dans chaque région.

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sélectionnez le répertoire cible.
3. Accédez à l'onglet Réseau et sécurité.
4. Choisissez Ajouter un IPv6 support. Cette option n'est disponible que pour les répertoires IPv4 uniquement.

5. Consultez les informations de mise à jour et les détails des prix.
6. Choisissez Ajouter pour confirmer la mise à jour.

Une fois la mise à jour lancée, le statut du répertoire passe à Mise à jour pendant le processus de mise à jour. La mise à jour prend généralement 15 à 30 minutes. Une fois terminée, le statut du répertoire redevient Actif.

Ajouter d'autres suffixes UPN à votre compte Microsoft AD géré AWS

Vous pouvez simplifier la gestion des noms de connexion Active Directory (AD) et améliorer l'expérience de connexion des utilisateurs en ajoutant des suffixes de nom d'utilisateur principal (UPN) alternatifs à votre répertoire AWS Microsoft AD géré. Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe Administrateurs délégués des suffixes de noms principaux d'utilisateurs AWS . Pour en savoir plus sur ce groupe, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Pour ajouter des suffixes UPN alternatifs

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Localisez une EC2 instance Amazon jointe à votre répertoire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
3. Dans la fenêtre Gestionnaire de serveur, choisissez Outils. Puis choisissez Domaines et approbations Active Directory.
4. Dans le volet de gauche, effectuez un clic droit sur Domaines et approbations Active Directory, puis choisissez Propriétés .
5. Dans l'onglet Suffixes UPN, tapez un suffixe UPN alternatif (par exemple, **sales.example.com**). Sélectionnez Ajouter, puis Appliquer.
6. Si vous devez ajouter d'autres suffixes UPN alternatifs, répétez l'étape 5 jusqu'à ce que vous ayez les suffixes UPN dont vous avez besoin.

Renommer le nom du site de votre annuaire Microsoft AD AWS géré

Vous pouvez renommer le nom de site par défaut de votre annuaire Microsoft AD AWS géré afin qu'il corresponde aux noms de sites Microsoft Active Directory (AD) existants. Cela permet à AWS Managed Microsoft AD de trouver et d'authentifier plus rapidement vos utilisateurs AD existants dans votre annuaire local. Il en résulte une meilleure expérience lorsque les utilisateurs se connectent à

AWS des ressources telles que les instances [Amazon EC2](#) et [Amazon RDS for SQL](#) Server que vous avez jointes à AWS votre répertoire Managed Microsoft AD.

Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe Administrateurs AWS délégués des sites et services. Pour en savoir plus sur ce groupe, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Pour prendre connaissance des avantages supplémentaires à renommer votre site en fonction des approbations, veuillez consulter [Domain Locator Across a Forest Trust](#) (français non garanti) sur le site web de Microsoft.

Pour renommer le nom du site AWS Managed Microsoft AD

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Localisez une EC2 instance Amazon jointe à votre répertoire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
3. Dans la fenêtre Gestionnaire de serveur, choisissez Outils. Choisissez ensuite Sites et services Active Directory.
4. Dans le volet de gauche, développez le dossier Sites, effectuez un clic droit sur le nom de site (par défaut, c'est Default-Site-Name), puis choisissez Renommer.
5. Tapez le nouveau nom de site, puis sélectionnez Entrée.

Suppression de votre Microsoft AD AWS géré

Lorsqu'un annuaire Microsoft AD AWS géré, Simple AD ou hybride est supprimé, toutes les données de l'annuaire et les instantanés sont supprimés et ne peuvent pas être restaurés. Une fois que l'annuaire est supprimé, toutes les instances qui sont jointes à l'annuaire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous y connecter avec un compte utilisateur qui est local à l'instance.

Lorsqu'un connecteur AD Connector est supprimé, votre annuaire sur site reste intact. Toutes les instances qui sont jointes à l'annuaire restent également intactes et jointes à votre annuaire sur site. Vous pouvez toutefois utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances.

Pour supprimer un annuaire

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire). Assurez-vous que vous vous trouvez à l' Région AWS endroit où votre Active Directory est déployé. Pour plus d'informations, voir [Choisir une région](#).
2. Assurez-vous qu'aucune AWS application n'est activée pour le répertoire que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AWS Managed Microsoft AD ou Simple AD.
 - a. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
 - b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre annuaire.
 - Désactivez AWS Management Console l'accès. Pour de plus amples informations, veuillez consulter [Désactivation AWS Management Console de l'accès](#).
 - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez [Supprimer un répertoire](#) dans le guide d' WorkSpaces administration Amazon.
 - Pour le désactiver WorkDocs, vous devez supprimer le WorkDocs site dans la WorkDocs console. Pour plus d'informations, consultez [Supprimer un site](#) dans le guide d' WorkDocs administration Amazon.
 - Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez [Supprimer une organisation](#) dans le manuel Amazon WorkMail Administrator Guide.
 - Pour désactiver le serveur de fichiers Amazon FSx pour Windows, vous devez supprimer le système de FSx fichiers Amazon du domaine. Pour plus d'informations, consultez la section [Travailler avec Active Directory dans FSx un serveur de fichiers Windows](#) dans le guide de l'utilisateur d'Amazon FSx pour Windows File Server.
 - Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section [Managing a DB instance in a domain](#) (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
 - Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la [section Utilisation du Client VPN](#) dans le Guide de AWS Client VPN l'administrateur.

- Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, consultez [Supprimer votre instance Amazon Connect](#) dans le guide d'administration Amazon Connect.
- Pour désactiver Amazon Quick Suite, vous devez vous désabonner d'Amazon Quick Suite. Pour plus d'informations, consultez la section [Fermeture de votre Amazon Quick Suite compte](#) dans le guide de l'utilisateur d'Amazon Quick Suite.

 Note

Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous souhaitez supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section [Change your identity source](#) (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaire).
4. Sélectionnez uniquement l'annuaire à supprimer, puis cliquez sur Supprimer. La suppression de l'annuaire prend plusieurs minutes. Lorsque l'annuaire a été supprimé, il est retiré de votre liste d'annuaires.

Sécurisez votre Microsoft AD AWS géré

Vous pouvez utiliser des politiques de mot de passe, des fonctionnalités telles que l'authentification multifactorielle (MFA) et des paramètres pour sécuriser votre AWS Managed Microsoft AD. Vous pouvez notamment sécuriser votre répertoire :

- [Découvrez comment fonctionnent les politiques de mot de passe d'Active Directory](#) afin qu'elles puissent être appliquées aux utilisateurs de AWS Managed Microsoft AD. Vous pouvez également déléguer les utilisateurs autorisés à gérer vos politiques de mot de passe Microsoft AD AWS gérées.
- [Activez le MFA](#) pour renforcer la sécurité de votre AWS Managed Microsoft AD.
- [>Activez le protocole Lightweight Directory Access Protocol via Secure Socket Layer \(SSL\) / Transport Layer Security \(TLS\) \(LDAPS\)](#) afin que les communications via LDAP soient cryptées et améliorent la sécurité.

- [Gérez votre conformité AWS à Microsoft AD géré](#) avec des normes telles que le Federal Risk and Authorization Management Program (FedRAMP) et la norme de sécurité des données (DSS) du secteur des cartes de paiement (PCI).
- [Améliorez la configuration de sécurité de votre réseau Microsoft AD AWS géré](#) > en modifiant le groupe AWS de sécurité pour répondre aux besoins de votre environnement.
- [Modifiez les paramètres de sécurité de votre annuaire Microsoft AD AWS géré](#), tels que l'authentification par certificat, le chiffrement par canal sécurisé et le protocole, pour répondre à vos besoins.
- [Configurez AWS Autorité de certification privée Connector for AD](#) afin de pouvoir émettre et gérer des certificats pour votre Microsoft AD AWS géré avec AWS CA privée.

Comprendre les politiques de AWS gestion des mots de passe Microsoft AD

AWS Managed Microsoft AD vous permet de définir et d'attribuer différentes politiques de verrouillage des mots de passe et des comptes (également appelées politiques de [mot de passe détaillées](#)) pour les groupes d'utilisateurs que vous gérez dans votre domaine AWS Microsoft AD géré. Lorsque vous créez un annuaire Microsoft AD AWS géré, une politique de domaine par défaut est créée et appliquée à Active Directory. Cette stratégie contient les paramètres suivants :

Politique	Paramètre
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Durée de vie maximale du mot de passe	42 jours *
Durée de vie minimale du mot de passe	1 jour
Longueur minimum du mot de passe	7 caractères
Le mot de passe doit respecter des exigences de complexité	Activées
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivées

Note

* L'âge maximum du mot de passe de 42 jours inclut le mot de passe administrateur.

Par exemple, vous pouvez attribuer un paramètre de stratégie moins strict pour les employés qui n'ont accès qu'à des informations de faible importance. Pour les cadres supérieurs qui accèdent régulièrement à des informations confidentielles, vous pouvez appliquer des paramètres plus stricts.

Les ressources suivantes fournissent des informations supplémentaires sur les politiques de mot de passe et les politiques de sécurité affinées d'Microsoft Active Directory :

- [Configuration des paramètres de politique de sécurité](#)
- [Exigences de complexité des mots de passe](#)
- [Complexité des mots de passe et considérations](#)

AWS fournit un ensemble de politiques de mot de passe détaillées dans AWS Managed Microsoft AD que vous pouvez configurer et attribuer à vos groupes. Pour configurer les politiques, vous pouvez utiliser des outils de Microsoft stratégie standard tels que le [centre d'administration Active Directory](#). Pour commencer à utiliser les outils Microsoft de politique, voir [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

Comment les politiques relatives aux mots de passe sont appliquées

Il existe des différences dans la façon dont les politiques de mot de passe affinées sont appliquées selon que le mot de passe a été réinitialisé ou modifié. Les utilisateurs du domaine peuvent modifier leur propre mot de passe. Un administrateur ou un utilisateur Active Directory disposant des autorisations nécessaires peut [réinitialiser les mots de passe des utilisateurs](#). Consultez le tableau suivant pour plus d'informations.

Politique	Réinitialisation du mot	Changement de mot de passe
Appliquer l'historique des mots de passe	 Non	 Oui

Politique	Réinitialisation du mot	Changement de mot de passe
Durée de vie maximale du mot de passe	 Oui	 Oui
Durée de vie minimale du mot de passe	 Non	 Oui
Longueur minimum du mot de passe	 Oui	 Oui
Le mot de passe doit respecter des exigences de complexité	 Oui	 Oui

Ces différences ont des conséquences sur le plan de la sécurité. Par exemple, chaque fois que le mot de passe d'un utilisateur est réinitialisé, les politiques relatives à l'historique des mots de passe et à l'âge minimum des mots de passe ne sont pas appliquées. Pour plus d'informations, consultez la documentation Microsoft sur les considérations de sécurité liées à l'application de l'[historique des mots de passe](#) et des politiques relatives à l'[âge minimum des mots de passe](#).

Paramètres de stratégie pris en charge

AWS Managed Microsoft AD inclut cinq politiques détaillées avec une valeur de priorité non modifiable. Les stratégies possèdent un certain nombre de propriétés que vous pouvez configurer pour mettre en œuvre vos mots de passe et actions de verrouillage de compte en cas d'échecs de connexion. Vous pouvez attribuer des stratégies à zéro ou plusieurs groupes Active Directory. Si un utilisateur final est membre de plusieurs groupes et reçoit plus d'une stratégie de mot de passe, Active Directory applique la stratégie avec la valeur de priorité la plus faible.

AWS politiques de mots de passe prédéfinies

Le tableau suivant répertorie les cinq politiques incluses dans votre répertoire Microsoft AD AWS géré et la valeur de priorité qui leur est attribuée. Pour de plus amples informations, veuillez consulter [Priorité](#).

Nom de la politique	Priorité
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Propriétés de stratégie de mot de passe

Vous pouvez modifier les propriétés suivantes dans vos stratégies de mot de passe pour respecter les normes de conformité qui répondent à vos besoins métier.

- Nom de la politique
- [Appliquer l'historique des mots de passe](#)
- [Longueur minimum du mot de passe](#)
- [Durée de vie minimale du mot de passe](#)
- [Durée de vie maximale du mot de passe](#)
- [Enregistrer les mots de passe en utilisant un chiffrement réversible](#)
- [Le mot de passe doit respecter des exigences de complexité](#)

Vous ne pouvez pas modifier les valeurs de priorité pour ces stratégies. Pour plus de détails sur la manière dont ces paramètres affectent l'application des mots de passe, voir [AD DS : politiques de mot de passe précises sur le site](#) Web de Microsoft TechNet. Pour obtenir des informations générales sur ces politiques, consultez la section [Politique en matière de mots de passe](#) sur le TechNet site Web de Microsoft.

Stratégies de verrouillage de compte

Vous pouvez également modifier les propriétés suivantes de vos stratégies de mot de passe pour indiquer si et comment Active Directory doit verrouiller un compte en cas d'échecs de connexion :

- Nombre d'échecs de connexion autorisés
- Durée de verrouillage du compte
- Réinitialiser les tentatives de connexion échouées après une période donnée

Pour obtenir des informations générales sur ces politiques, consultez la section [Politique de verrouillage des comptes](#) sur le TechNet site Web de Microsoft.

Priorité

Les stratégies avec une valeur de priorité inférieure ont une priorité plus élevée. Vous pouvez attribuer des stratégies de mot de passe à des groupes de sécurité Active Directory. Même si vous devez appliquer une seule stratégie à un groupe de sécurité, un même utilisateur peut recevoir plus d'une stratégie de mot de passe. Par exemple, si jsmith est membre du groupe RESSOURCES HUMAINES et également membre du groupe RESPONSABLES. Si vous attribuez CustomerPSO-05 (avec une priorité de 50) au groupe RESSOURCES HUMAINES, et CustomerPSO-04 (avec une priorité de 40) au groupe RESPONSABLES, CustomerPSO-04 a la priorité la plus élevée et Active Directory applique cette stratégie à jsmith.

Si vous attribuez plusieurs stratégies à un utilisateur ou un groupe, Active Directory détermine la stratégie résultante comme suit :

1. Une stratégie que vous attribuez directement à l'objet utilisateur s'applique.
2. Si aucune stratégie n'est attribuée directement à l'objet utilisateur, la stratégie avec la valeur de priorité la plus faible reçue par l'utilisateur suite à son adhésion à un groupe s'applique.

Pour plus de détails, voir [AD DS : politiques de mot de passe détaillées sur le site](#) Web de Microsoft TechNet.

Rubriques

- [Affectation de politiques de mot de passe à vos AWS utilisateurs Microsoft AD gérés](#)
- [Délégation des personnes habilitées à gérer vos politiques de mot de passe Microsoft AD AWS gérées](#)

Article AWS de blog sur la sécurité connexe

- [Comment configurer des politiques de mot de passe encore plus strictes pour répondre à vos normes de sécurité à l'aide Directory Service de AWS Managed Microsoft AD](#)

Affectation de politiques de mot de passe à vos AWS utilisateurs Microsoft AD gérés

Les comptes utilisateurs membres du groupe de sécurité AWS Delegated Fine Grained Password Policy Administrators (Administrateurs délégués de stratégies de mot de passe affinées) peuvent recourir à la procédure suivante pour attribuer des stratégies à des utilisateurs et des groupes de sécurité.

Pour attribuer des stratégies de mot de passe à vos utilisateurs

1. Lancez le [centre d'administration Active Directory \(ADAC\)](#) à partir de n'importe quelle EC2 instance gérée que vous avez jointe à votre domaine Microsoft AD AWS géré.
2. Passez à l'arborescence et accédez à System>Password Settings Container.
3. Double-cliquez sur la stratégie affinée que vous souhaitez modifier. Cliquez sur Ajouter pour modifier les propriétés de la stratégie et ajouter des utilisateurs ou des groupes de sécurité à la stratégie. Pour plus d'informations sur les stratégies affinées fournies par défaut avec AWS Managed Microsoft AD, veuillez consulter [AWS politiques de mots de passe prédéfinies](#).
4. Pour vérifier que la politique de mot de passe a été appliquée, exécutez la PowerShell commande suivante :

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

Note

Évitez d'utiliser la commande `net user`, car ses résultats peuvent être inexacts.

Si vous ne configurez aucune des cinq politiques de mot de passe de votre annuaire Microsoft AD AWS géré, Active Directory utilise la stratégie de groupe de domaines par défaut. Pour plus d'informations sur l'utilisation du Conteneur de paramètres de mots de passe, veuillez consulter ce [billet de blog Microsoft](#).

Délégation des personnes habilitées à gérer vos politiques de mot de passe Microsoft AD AWS gérées

Vous pouvez déléguer les autorisations de gestion des politiques de mot de passe à des comptes utilisateur spécifiques que vous avez créés dans votre AWS Managed Microsoft AD en ajoutant les comptes au groupe de sécurité AWS Delegated Fine Grained Password Policy Administrators. Lorsqu'un compte devient membre de ce groupe, il dispose des autorisations nécessaires pour modifier et configurer les stratégies de mot de passe [précédemment](#) mentionnées.

Pour déléguer des autorisations de gestion de vos stratégies de mot de passe

1. Lancez le [centre d'administration Active Directory \(ADAC\)](#) à partir de n'importe quelle EC2 instance gérée que vous avez jointe à votre domaine Microsoft AD AWS géré.
2. Basculez vers l'arborescence et accédez à l'unité d'organisation AWS Delegated Groups (Groupes délégués). Pour plus d'informations sur cette unité d'organisation, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).
3. Recherchez le groupe d'utilisateurs AWS Delegated Fine Grained Password Policy Administrators (Administrateurs délégués de stratégies de mot de passe affinées). Ajoutez des utilisateurs ou des groupes de votre domaine à ce groupe.

Activation de l'authentification multifactorielle pour AWS Managed Microsoft AD

Vous pouvez activer l'authentification multifactorielle (MFA) pour votre annuaire Microsoft AD AWS géré afin de renforcer la sécurité lorsque vos utilisateurs spécifient leurs informations d'identification AD pour accéder aux applications Amazon Enterprise prises en charge. Lorsque vous activez la MFA, vos utilisateurs saisissent leur nom d'utilisateur et leur mot de passe (premier facteur), comme ils en ont l'habitude, mais ils doivent également saisir un code d'authentification (deuxième facteur) qui leur est fourni par votre solution MFA matérielle ou virtuelle. Ensemble, ces facteurs offrent une sécurité supplémentaire en empêchant l'accès à vos applications d'entreprise Amazon si les utilisateurs ne sont pas en mesure d'indiquer des informations d'identification utilisateur valides et un code MFA valide.

Pour activer l'authentification MFA, vous devez posséder une solution MFA qui est un serveur [Remote authentication dial-in user service](#) (RADIUS), ou disposer d'un plugin sur un serveur RADIUS déjà installé dans votre infrastructure sur site. Votre solution d'authentification MFA doit utiliser des

codes secrets uniques que les utilisateurs obtiennent à partir d'un périphérique physique ou d'un logiciel exécuté sur un périphérique, par exemple un téléphone portable.

RADIUS est un client/server protocole standard qui assure l'authentification, l'autorisation et la gestion de la comptabilité afin de permettre aux utilisateurs de se connecter aux services réseau. AWS Managed Microsoft AD inclut un client RADIUS qui se connecte au serveur RADIUS sur lequel vous avez implémenté votre solution MFA. Votre serveur RADIUS valide le nom d'utilisateur et le code secret unique. Si votre serveur RADIUS valide correctement l'utilisateur, AWS Managed Microsoft AD authentifie ensuite l'utilisateur auprès d'Active Directory. Une fois l'authentification Active Directory réussie, les utilisateurs peuvent accéder à l'AWS application. La communication entre le client Microsoft AD RADIUS AWS géré et votre serveur RADIUS nécessite que vous configuriez des groupes AWS de sécurité qui permettent la communication via le port 1812.

Vous pouvez activer l'authentification multifactorielle pour votre annuaire Microsoft AD AWS géré en suivant la procédure suivante. Pour plus d'informations sur la configuration de votre serveur RADIUS pour être utilisé avec Directory Service et MFA, veuillez consulter [Prérequis pour l'authentification multifactorielle](#).

Considérations

Voici quelques considérations relatives à l'authentification multifactorielle pour votre Microsoft AD AWS géré :

- L'authentification multifactorielle n'est pas disponible pour Simple AD. Toutefois, l'authentification MFA peut être activée pour votre annuaire AD Connector. Pour de plus amples informations, veuillez consulter [Enabling multi-factor authentication for AD Connector](#).
- Le MFA est une fonctionnalité régionale de Managed AWS Microsoft AD. Si vous utilisez [la réplification multirégionale](#), vous ne pourrez utiliser le MFA que dans la région principale de votre Microsoft AD AWS géré.
- Si vous avez l'intention d'utiliser AWS Managed Microsoft AD pour les communications externes, nous vous recommandons de configurer une passerelle Internet ou une passerelle Internet de traduction d'adresses réseau (NAT) en dehors du AWS réseau pour ces communications.
 - Si vous souhaitez prendre en charge les communications externes entre votre Microsoft AD AWS géré et votre serveur RADIUS hébergé sur le AWS réseau, veuillez contacter [Support](#).
- Toutes les applications informatiques Amazon Enterprise WorkSpaces, y compris Amazon WorkDocs, Amazon Quick Suite WorkMail, ainsi que l'accès à AWS IAM Identity Center Managed Microsoft AD et AD Connector avec MFA, AWS Management Console sont prises en charge lors

de l'utilisation de AWS Managed Microsoft AD et AD Connector. Ces AWS applications utilisant le MFA ne sont pas prises en charge dans plusieurs régions.

Pour plus d'informations, consultez [Comment activer l'authentification multifactorielle pour les AWS services à l'aide de AWS Managed Microsoft AD et des informations d'identification locales](#).

- Pour plus d'informations sur la configuration de l'accès utilisateur de base aux applications Amazon Enterprise, l'authentification AWS unique et l' AWS Management Console utilisation Directory Service, consultez [Accès aux AWS applications et aux services depuis votre Microsoft AD AWS géré](#) et [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#).
- Consultez ce billet de blog sur la AWS sécurité suivant pour savoir comment activer l'authentification MFA pour les WorkSpaces utilisateurs d'Amazon sur votre compte AWS Microsoft AD géré, [comment activer l'authentification multifactorielle pour les AWS services à l'aide de Managed AWS Microsoft AD et d'informations d'identification sur site](#)

Activation de l'authentification multifactorielle (MFA) pour AWS Managed Microsoft AD

La procédure suivante explique comment activer l'authentification multifactorielle pour AWS Managed Microsoft AD.

1. Identifiez l'adresse IP de votre serveur MFA RADIUS et de votre répertoire AWS Managed Microsoft AD.
2. Modifiez vos groupes de sécurité Virtual Private Cloud (VPC) pour permettre les communications via le port 1812 entre vos points de terminaison IP AWS Microsoft AD gérés et votre serveur MFA RADIUS.
3. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
4. Choisissez le lien d'ID de répertoire pour votre annuaire Microsoft AD AWS géré.
5. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez activer l'authentification MFA, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Mise en réseau et sécurité.

6. Dans la section Authentification multifactorielle, choisissez Actions, puis sélectionnez Activer.
7. Dans la page Activer l'authentification multifactorielle (MFA), indiquez les valeurs suivantes :

Afficher l'étiquette

Indiquez un nom d'étiquette.

Nom DNS ou adresses IP du serveur RADIUS

Adresses IP des points de terminaison de votre serveur RADIUS ou adresse IP de l'équilibreur de charge de votre serveur RADIUS. Vous pouvez entrer plusieurs adresses IP en les séparant par une virgule (par exemple, 192.0.0.0,192.0.0.12).

 Note

RADIUS MFA s'applique uniquement pour authentifier l' AWS Management Console accès aux applications et services Amazon Enterprise tels qu'Amazon Quick Suite ou WorkSpaces Amazon Chime. Les applications et services Amazon Enterprise ne sont pris en charge dans la région principale que si la réplication multirégionale est configurée pour votre Microsoft AD AWS géré. Il ne fournit pas de MFA aux charges de travail Windows exécutées sur des EC2 instances ou pour la connexion à une instance. EC2 Directory Service ne prend pas en charge l'authentification RADIUS Challenge/Response.

Les utilisateurs doivent disposer de leur code MFA au moment d'entrer leurs noms d'utilisateur et leurs mots de passe. Vous devez également utiliser une solution qui exécute l'authentification multifacteur, out-of-band telle que les notifications push ou les mots de passe à usage unique (OTP) d'authentification pour l'utilisateur. Dans les solutions out-of-band MFA, vous devez vous assurer de définir la valeur du délai d'expiration RADIUS de manière appropriée pour votre solution. Lorsque vous utilisez une solution out-of-band MFA, la page de connexion invite l'utilisateur à saisir un code MFA. Dans ce cas, les utilisateurs doivent entrer leurs mots de passe dans la zone de mot de passe et dans la zone MFA.

Port

Port que votre serveur RADIUS utilise pour les communications. Votre réseau local doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (UDP:1812) en provenance des serveurs. Directory Service

Shared secret code

Code secret partagé qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Confirmer le code secret partagé

Confirmez le code secret partagé pour vos points de terminaison RADIUS.

Protocole

Sélectionnez le protocole qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Délai d'attente du serveur (en secondes)

Durée, en secondes, d'attente de la réponse du serveur RADIUS. La valeur doit être comprise entre 1 et 50.

Note

Nous vous recommandons de configurer le délai d'attente de votre serveur RADIUS à 20 secondes ou moins. Si le délai d'attente est supérieur à 20 secondes, le système ne peut pas réessayer avec un autre serveur RADIUS, ce qui peut entraîner un échec lié au délai d'attente.

Nombre maximal de tentatives RADIUS

Nombre de tentatives de communication avec le serveur RADIUS. La valeur doit être comprise entre 0 et 10.

L'authentification multifactorielle est disponible lorsque le paramètre RADIUS Status passe à l'état Enabled.

8. Sélectionnez Activer.

Activer le protocole LDAP ou LDAPS sécurisé

LDAP (Lightweight Directory Access Protocol) est un protocole de communication standard utilisé pour lire et écrire des données vers et depuis Active Directory. Certaines applications utilisent LDAP

pour ajouter, supprimer ou rechercher des utilisateurs et des groupes dans Active Directory ou pour transférer des informations d'identification afin d'authentifier des utilisateurs dans Active Directory. Chaque communication LDAP comprend un client (par exemple une application) et un serveur (comme Active Directory).

Par défaut, les communications via LDAP ne sont pas chiffrées. Cela permet à un utilisateur malveillant d'utiliser un logiciel de surveillance réseau pour afficher les paquets de données sur le réseau. C'est pourquoi de nombreuses stratégies de sécurité d'entreprise imposent généralement aux organisations de chiffrer toutes les communications LDAP.

Pour atténuer cette forme d'exposition des données, AWS Managed Microsoft AD propose une option : vous pouvez activer LDAP via Secure Sockets Layer (SSL) /Transport Layer Security (TLS), également connu sous le nom de LDAPS. Avec LDAPS, vous pouvez renforcer la sécurité de votre réseau. Vous pouvez également répondre aux exigences de conformité en chiffrant toutes les communications entre vos applications compatibles LDAP et Managed AWS Microsoft AD.

AWS Managed Microsoft AD prend en charge le protocole LDAPS dans les scénarios de déploiement suivants :

- LDAPS côté serveur chiffre les communications LDAP entre vos applications LDAP commerciales ou locales et votre annuaire AWS Managed Microsoft AD (tenant lieu de serveur LDAP). Pour de plus amples informations, veuillez consulter [Activation du protocole LDAPS côté serveur à l'aide de Managed Microsoft AD AWS](#).
- Le protocole LDAPS côté client chiffre les communications LDAP entre des AWS applications telles que WorkSpaces (agissant en tant que clients LDAP) et votre Active Directory autogéré (sur site) (agissant en tant que serveur LDAP). Pour de plus amples informations, veuillez consulter [Activation du protocole LDAPS côté client à l'aide de Managed Microsoft AD AWS](#).

Pour plus d'informations sur les meilleures pratiques relatives à la sécurisation de votre implémentation d'MicrosoftActive DirectoryCertificate Services, consultez [Microsoftla documentation](#).

Rubriques

- [Activation du protocole LDAPS côté serveur à l'aide de Managed Microsoft AD AWS](#)
- [Activation du protocole LDAPS côté client à l'aide de Managed Microsoft AD AWS](#)

Activation du protocole LDAPS côté serveur à l'aide de Managed Microsoft AD AWS

Le Lightweight Directory Access Protocol Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) support côté serveur chiffre les LDAP communications entre vos applications commerciales ou locales et votre LDAP annuaire Microsoft AD géré AWS . Cela permet d'améliorer la sécurité sur le réseau et de répondre aux exigences de conformité à l'aide du protocole Secure Sockets Layer (SSL) cryptographique.

Activez LDAPS côté serveur à l'aide de AWS Autorité de certification privée

Pour obtenir des instructions détaillées sur la façon de configurer et de configurer le protocole LDAPS côté serveur et votre serveur d'autorité de certification (CA) à l'aide AWS CA privée de. [Configurer le AWS CA privée connecteur pour AD pour Microsoft AD AWS géré](#)

Activer le protocole LDAPS côté serveur à l'aide de CA Microsoft

Pour obtenir des instructions détaillées sur la façon de configurer et de configurer le protocole LDAPS côté serveur et votre serveur d'autorité de certification (CA), consultez la section [Comment activer le protocole LDAPS côté serveur pour votre annuaire Microsoft AD AWS géré](#) sur le blog de sécurité. AWS

Vous devez effectuer la majeure partie de la configuration à partir de l' EC2 instance Amazon que vous utilisez pour gérer vos contrôleurs de domaine Microsoft AD AWS gérés. Les étapes suivantes vous indiquent comment activer LDAPS pour votre domaine dans le AWS Cloud.

Si vous souhaitez utiliser l'automatisation pour configurer votre PKI infrastructure, vous pouvez utiliser l'[infrastructure à clé Microsoft publique sur AWS QuickStart Guide](#). Plus précisément, vous devez suivre les instructions du guide pour charger le modèle de [déploiement MicrosoftPKI dans un système existant VPCAWS](#). Une fois que vous avez chargé le modèle, assurez-vous de choisir **AWSManaged** quand vous accédez à l'option Type de services de domaine Active Directory. Si vous avez utilisé le QuickStart guide, vous pouvez accéder directement à [Étape 3 : créer un modèle de certificat](#).

Rubriques

- [Étape 1 : déléguer les rôles autorisés à activer LDAPS](#)
- [Étape 2 : configurer votre autorité de certification](#)
- [Étape 3 : créer un modèle de certificat](#)
- [Étape 4 : Ajouter des règles de groupe de sécurité](#)

Étape 1 : déléguer les rôles autorisés à activer LDAPS

Pour activer le protocole LDAPS côté serveur, vous devez être membre du groupe Admins ou AWS Delegated Enterprise Certificate Authority Administrators de votre annuaire AWS Microsoft AD géré. Vous pouvez également être l'utilisateur administratif par défaut (compte Admin). Si vous préférez, vous pouvez faire en sorte qu'un autre utilisateur que le compte Admin configure LDAPS. Dans ce cas, ajoutez cet utilisateur au groupe Admins ou AWS Delegated Enterprise Certificate Authority Administrators dans votre répertoire AWS Managed Microsoft AD.

Étape 2 : configurer votre autorité de certification

Avant de pouvoir activer LDAPS côté serveur, vous devez créer un certificat. Ce certificat doit être émis par un Microsoft Enterprise CA serveur joint à votre domaine Microsoft AD AWS géré. Une fois créé, le certificat doit être installé sur chacun des contrôleurs de domaine qui se trouvent dans ce domaine. Ce certificat permet au LDAP service des contrôleurs de domaine d'écouter et d'accepter automatiquement les SSL connexions des LDAP clients.

Note

Le protocole LDAPS côté serveur avec AWS Microsoft AD géré ne prend pas en charge les certificats émis par une autorité de certification autonome. Il ne prend pas non plus en charge les certificats émis par une autorité de certification tierce.

Selon vos besoins spécifiques, vous disposez de différentes options pour configurer une autorité de certification ou pour vous connecter à une autorité de certification dans votre domaine :

- Créer un serveur subordonné Microsoft Enterprise CA — (recommandé) Avec cette option, vous pouvez déployer un Microsoft Enterprise CA serveur subordonné dans le AWS cloud. Le serveur peut utiliser Amazon EC2 afin de fonctionner avec votre autorité de Microsoft certification racine existante. Pour plus d'informations sur la configuration d'un subordonné Microsoft Enterprise CA, voir [Étape 4 : Ajouter un Microsoft Enterprise CA à votre AWS Microsoft AD répertoire dans Comment activer le protocole LDAPS côté serveur pour votre annuaire AWS Microsoft AD géré.](#)
- Créer une racine Microsoft Enterprise CA : avec cette option, vous pouvez créer une racine Microsoft Enterprise CA dans le AWS cloud à l'aide d'Amazon EC2 et la joindre à votre domaine Microsoft AD AWS géré. Cette autorité de certification racine peut émettre le certificat sur vos contrôleurs de domaine. Pour plus d'informations sur la configuration d'une nouvelle autorité de certification racine, voir [Étape 3 : Installation et configuration d'une autorité de certification hors](#)

ligne dans [Comment activer le protocole LDAPS côté serveur pour votre annuaire AWS Microsoft AD géré](#).

Pour plus d'informations sur la façon de joindre votre EC2 instance au domaine, consultez [Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré](#).

Étape 3 : créer un modèle de certificat

Une fois votre Enterprise CA configuration terminée, vous pouvez configurer le modèle de certificat Kerberos d'authentification.

Pour créer un modèle de certificat

1. Lancez Microsoft Windows Server Manager. Sélectionnez Outils > Autorité de certification.
2. Dans la fenêtre Autorité de certification, développez l'arborescence Autorité de certification dans le volet de gauche. Cliquez avec le bouton droit sur Modèles de certificats, puis sélectionnez Gérer.
3. Dans la fenêtre Console de modèles de certificats, cliquez avec le bouton droit sur Authentification Kerberos, puis sélectionnez Dupliquer le modèle.
4. La fenêtre Propriétés du nouveau modèle s'ouvre.
5. Dans la fenêtre Propriétés du nouveau modèle, accédez à l'onglet Compatibilité, puis procédez comme suit :
 - a. Remplacez l'autorité de certification par celle OS qui correspond à votre autorité de certification.
 - b. Si une fenêtre Modifications résultantes s'affiche, sélectionnez OK.
 - c. Changez le destinataire de la certification en Windows 10/Windows Server 2016.

Note

AWS Managed Microsoft AD est alimenté par Windows Server 2019.

- d. Si la fenêtre Modifications résultantes s'affiche, sélectionnez OK.
6. Cliquez sur l'onglet Général et remplacez le nom d'affichage du modèle LDAP Over par SSL ou par tout autre nom que vous préférez.

7. Cliquez sur l'onglet Sécurité et sélectionnez Contrôleurs de domaine dans la section Noms de groupes ou d'utilisateurs. Dans la section Autorisations pour les contrôleurs de domaine, vérifiez que les cases Autoriser pour la lecture, l'inscription et l'inscription automatique sont cochées.
8. Cliquez sur OK pour créer le modèle de certificat LDAPOverSSL (ou le nom que vous avez spécifié ci-dessus). Fermez la fenêtre de la Console des modèles de certificats.
9. Dans la fenêtre Autorité de certificats, cliquez avec le bouton droit sur Modèles de certificats, puis sélectionnez Nouveau > Modèle de certificat à émettre.
10. Dans la fenêtre Activer les modèles de certificats, choisissez LDAPOverSSL (ou le nom que vous avez spécifié ci-dessus), puis cliquez sur OK.

Étape 4 : Ajouter des règles de groupe de sécurité

Dans la dernière étape, vous devez ouvrir la EC2 console Amazon et ajouter des règles de groupe de sécurité. Ces règles permettent à vos contrôleurs de domaine de se connecter Enterprise CA à votre pour demander un certificat. Pour ce faire, vous ajoutez des règles entrantes afin de Enterprise CA pouvoir accepter le trafic entrant en provenance de vos contrôleurs de domaine. Vous ajoutez ensuite des règles de sortie pour autoriser le trafic de vos contrôleurs de domaine vers le Enterprise CA.

Une fois les deux règles configurées, vos contrôleurs de domaine vous demandent Enterprise CA automatiquement un certificat et activent LDAPS pour votre annuaire. Le LDAP service de vos contrôleurs de domaine est désormais prêt à accepter les connexions LDAPS.

Pour configurer des règles de groupe de sécurité

1. Accédez à votre EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2> et connectez-vous à l'aide des informations d'identification d'administrateur.
2. Dans le volet de gauche, sélectionnez Security Groups sous l'onglet Network & Security.
3. Dans le volet principal, choisissez le groupe AWS de sécurité pour votre autorité de certification.
4. Sélectionnez l'onglet Inbound (Entrant), puis Edit (Modifier).
5. Dans la boîte de dialogue Edit inbound rules, exécutez l'une des actions suivantes :
 - Choisissez Add Rule (Ajouter une règle).
 - Choisissez l'option All traffic pour le champ Type et l'option Custom pour le champ Source.
 - Entrez le groupe AWS de sécurité (par exemple, sg-123456789) pour votre répertoire dans la zone à côté de Source.
 - Choisissez Enregistrer.

6. Choisissez maintenant le groupe de AWS sécurité de votre annuaire Microsoft AD AWS géré. Sélectionnez l'onglet Outbound, puis Edit.
7. Dans la boîte de dialogue Edit outbound rules, exécutez l'une des actions suivantes :
 - Choisissez Add Rule (Ajouter une règle).
 - Choisissez l'option All traffic pour le champ Type et l'option Custom pour le champ Destination.
 - Entrez le groupe AWS de sécurité de votre autorité de certification dans la case à côté de Destination.
 - Choisissez Enregistrer.

Vous pouvez tester la connexion LDAPS au répertoire AWS Managed Microsoft AD à l'aide de l'LDPoutil. L'LDPoutil est livré avec leActive Directory Administrative Tools. Pour de plus amples informations, veuillez consulter [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

 Note

Avant de tester la connexion LDAPS, vous devez attendre jusqu'à 30 minutes pour que l'autorité de certification secondaire transmette un certificat à vos contrôleurs de domaine.

Pour plus de détails sur le protocole LDAPS côté serveur et pour voir un exemple de cas d'utilisation expliquant comment le configurer, consultez la section [Comment activer le protocole LDAPS côté serveur pour votre annuaire Microsoft AD AWS géré](#) sur le blog de sécurité. AWS

Activation du protocole LDAPS côté client à l'aide de Managed Microsoft AD AWS

La prise en charge du protocole SSL (Lightweight Directory Access Protocol) /Transport Layer Security (TLS) (LDAPS) côté client dans Managed AWS Microsoft AD chiffre les communications entre Microsoft Active Directory (AD) autogéré (sur site) et les applications. AWS Des exemples de telles applications incluent WorkSpaces, AWS IAM Identity Center, Quick Suite et Amazon Chime. Ce chiffrement vous aide à mieux protéger les données d'identité de votre entreprise et à répondre à vos exigences en matière de sécurité.

Prérequis

Avant d'activer LDAPS côté client, vous devez satisfaire les exigences suivantes.

Rubriques

- [Créez une relation de confiance entre votre Microsoft AD AWS géré et votre Microsoft Active Directory autogéré](#)
- [Déployer des certificats de serveur dans Active Directory](#)
- [Exigences relatives aux certificats de l'autorité de certification](#)
- [Exigences liées à la mise en réseau](#)

Créez une relation de confiance entre votre Microsoft AD AWS géré et votre Microsoft Active Directory autogéré

Tout d'abord, vous devez établir une relation de confiance entre votre Microsoft AD AWS géré et votre Microsoft Active Directory autogéré pour activer le protocole LDAPS côté client. Pour de plus amples informations, veuillez consulter [the section called "Création d'une relation d'approbation"](#).

Déployer des certificats de serveur dans Active Directory

Afin d'activer LDAPS côté client, vous devez obtenir et installer des certificats de serveur pour chaque contrôleur de domaine dans Active Directory. Ces certificats seront utilisés par le service LDAP pour écouter et accepter automatiquement les connexions SSL provenant de clients LDAP. Vous pouvez utiliser des certificats SSL émis par un déploiement AD CS (services de certificat Active Directory) interne ou achetés auprès d'un émetteur commercial. Pour plus d'informations sur les exigences relatives aux certificats de serveur Active Directory, veuillez consulter [LDAP over SSL \(LDAPS\) Certificate](#) (français non garanti) sur le site web de Microsoft.

Exigences relatives aux certificats de l'autorité de certification

Un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats de serveur, est requis pour le fonctionnement de LDAPS côté client. Les certificats d'une autorité de certification sont mis en correspondance avec les certificats de serveur présentés par vos contrôleurs de domaine Active Directory pour chiffrer les communications LDAP. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- L'autorité de certification d'entreprise (CA) est requise pour activer le protocole LDAPS côté client. Vous pouvez utiliser le service de certificats Active Directory, une autorité de certification commerciale tierce ou [AWS Certificate Manager](#). Pour plus d'informations sur Microsoft l'autorité de certification d'entreprise, consultez [Microsoftla documentation](#).
- Pour que vous puissiez enregistrer un certificat, celui-ci doit expirer dans plus de 90 jours.

- Les certificats doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats d'autorité de certification à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Un maximum de cinq (5) certificats CA peuvent être stockés par répertoire Microsoft AD AWS géré.
- Les certificats utilisant l'algorithme de signature RSASSA-PSS ne sont pas pris en charge.
- Les certificats d'autorité de certification qui sont chaînés à chaque certificat de serveur dans chaque domaine approuvé doivent être enregistrés.

Exigences liées à la mise en réseau

AWS le trafic LDAP de l'application s'exécutera exclusivement sur le port TCP 636, sans retour sur le port LDAP 389. Toutefois, les communications LDAP Windows prenant en charge la réplication, les approbations, etc. continueront d'utiliser le port LDAP 389 avec une sécurité native Windows. Configurez les groupes de AWS sécurité et les pare-feux réseau pour autoriser les communications TCP sur le port 636 dans Managed AWS Microsoft AD (sortie) et Active Directory autogéré (entrée). Laissez le port LDAP 389 ouvert entre AWS Managed Microsoft AD et Active Directory autogéré.

Activer LDAPS côté client

Pour activer LDAPS côté client, vous importez votre certificat d'une autorité de certification (CA) dans AWS Managed Microsoft AD, puis vous activez LDAPS sur votre annuaire. Lors de l'activation, tout le trafic LDAP entre les applications AWS et votre Active Directory autogéré est transmis avec le chiffrement de canal Secure Sockets Layer (SSL).

Vous pouvez utiliser deux méthodes différentes pour activer LDAPS côté client pour votre annuaire. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Note

Le LDAPS côté client est une fonctionnalité régionale de Managed AWS Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Rubriques

- [Étape 1 : enregistrer un certificat dans Directory Service](#)
- [Étape 2 : Vérifier l'état d'enregistrement](#)

- [Étape 3 : Activer LDAPS côté client](#)
- [Étape 4 : Vérifier l'état LDAPS](#)

Étape 1 : enregistrer un certificat dans Directory Service

Utilisez l'une des méthodes suivantes pour enregistrer un certificat dans Directory Service.

Méthode 1 : Pour enregistrer votre certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, effectuez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez enregistrer votre certificat, puis cliquez sur l'onglet Réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.
4. Dans la section LDAPS côté client sélectionnez le menu Actions, puis Enregistrer le certificat.
5. Dans la boîte de dialogue Enregistrer un certificat d'une autorité de certification, sélectionnez Parcourir, puis le certificat et choisissez Ouvrir.
6. Choisissez Register certificate (Enregistrer le certificat).

Méthode 2 : Pour enregistrer votre certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Un ID de certificat sera fourni dans la réponse.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

Étape 2 : Vérifier l'état d'enregistrement

Pour afficher l'état d'un enregistrement de certificat ou d'une liste de certificats enregistrés, utilisez l'une des méthodes suivantes.

Méthode 1 : pour vérifier le statut d'enregistrement du certificat dans Directory Service (AWS Management Console)

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Vérifiez l'état de l'enregistrement de certificat actuel qui s'affiche sous la colonne État de l'enregistrement. Lorsque la valeur de l'état de l'enregistrement passe à Enregistré, cela signifie que votre certificat a été enregistré avec succès.

Méthode 2 : pour vérifier le statut d'enregistrement du certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Si la valeur de l'état renvoie Registered, cela signifie que votre certificat a été enregistré avec succès.

```
aws ds list-certificates --directory-id your_directory_id
```

Étape 3 : Activer LDAPS côté client

Utilisez l'une des méthodes suivantes pour activer le protocole LDAPS côté client dans Directory Service

 Note

Avant de pouvoir activer LDAPS côté client, vous devez avoir enregistré avec succès au moins un certificat.

Méthode 1 : pour activer le protocole LDAPS côté client dans () Directory ServiceAWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Sélectionnez Activer. Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
3. Dans la boîte de dialogue Activer LDAPS côté client choisissez Activer.

Méthode 2 : pour activer le protocole LDAPS côté client dans () Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Étape 4 : Vérifier l'état LDAPS

Utilisez l'une des méthodes suivantes pour vérifier l'état du LDAPS dans Directory Service.

Méthode 1 : pour vérifier l'état du LDAPS dans Directory Service ()AWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Si la valeur d'état est affichée en tant que Activé, cela signifie que LDAPS a été configuré avec succès.

Méthode 2 : pour vérifier l'état du LDAPS dans Directory Service ()AWS CLI

- Exécutez la commande suivante. Si la valeur d'état renvoie Enabled, cela signifie que LDAPS a été configuré avec succès.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Gérer LDAPS côté client

Utilisez ces commandes pour gérer votre configuration LDAPS.

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres LDAPS côté client. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : pour afficher les détails du certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez afficher le certificat, puis cliquez sur l'onglet Réseau et

sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.
4. Les informations relatives au certificat sont affichées dans la section LDAPS côté client sous Certificats d'une autorité de certification.

Méthode 2 : pour afficher les détails du certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

 Note

Si un seul certificat est enregistré, vous devez d'abord désactiver LDAPS avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : pour annuler l'enregistrement d'un certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez annuler l'enregistrement d'un certificat, puis cliquez sur l'onglet Réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Actions, puis Annuler l'enregistrement du certificat.
 5. Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : pour annuler l'enregistrement d'un certificat dans Directory Service ()AWS CLI

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Désactiver LDAPS côté client

Utilisez l'une des méthodes suivantes pour désactiver LDAPS côté client.

Méthode 1 : pour désactiver le protocole LDAPS côté client dans () Directory ServiceAWS Management Console

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez désactiver LDAPS côté client, puis cliquez sur l'onglet Réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication multirégionale, cliquez sur l'onglet Réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Désactiver.
5. Dans la boîte de dialogue Désactiver LDAPS côté client, choisissez Désactiver.

Méthode 2 : pour désactiver le protocole LDAPS côté client dans () Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Problèmes liés à l'inscription aux certificats

Le processus d'inscription de vos contrôleurs de domaine Microsoft AD AWS gérés avec les certificats CA peut prendre jusqu'à 30 minutes. Si vous rencontrez des problèmes lors de l'inscription des certificats et que vous souhaitez redémarrer vos contrôleurs de domaine Microsoft AD AWS gérés, vous pouvez contacter Support. Pour créer un dossier d'assistance, consultez les sections [Création de dossiers d'assistance et gestion des dossiers](#).

Gérez la conformité pour AWS Managed Microsoft AD

Vous pouvez utiliser AWS Managed Microsoft AD pour prendre en charge vos applications compatibles Active Directory, dans le AWS cloud, qui sont soumises aux exigences de conformité suivantes. Sachez toutefois que vos applications ne respecteront pas ces exigences de conformité si vous utilisez Simple AD.

Normes de conformité prises en charge

AWS Managed Microsoft AD a fait l'objet d'un audit selon les normes suivantes et peut être utilisé dans le cadre de solutions pour lesquelles vous devez obtenir une certification de conformité.



AWS Managed Microsoft AD répond aux exigences de sécurité du Federal Risk and Authorization Management Program (FedRAMP) et a reçu l'autorisation provisoire d'exploitation (P-ATO) du FedRAMP Joint Authorization Board (JAB) sur la base de référence modérée et élevée du FedRAMP. Pour de plus amples informations sur FedRAMP, veuillez consulter [FedRAMP compliance](#) (français non garanti).



AWS Managed Microsoft AD possède une attestation de conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) version 3.2 au niveau 1 du fournisseur de services. Les clients qui utilisent AWS des produits et services pour stocker, traiter ou transmettre les données des titulaires de cartes peuvent utiliser AWS Managed Microsoft AD pour gérer leur propre certification de conformité à la norme PCI DSS.

Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section [PCI DSS niveau 1](#). Il est important de noter que vous devez configurer des politiques de mot de passe précises dans AWS Managed Microsoft AD afin qu'elles soient conformes aux normes PCI DSS version 3.2. Pour plus de détails sur les politiques qui doivent être appliquées, consultez la section ci-dessous intitulée Activer la conformité PCI pour votre annuaire Microsoft AD AWS géré.



AWS a étendu son programme de conformité à la loi HIPAA (Health Insurance Portability and Accountability Act) pour inclure Managed AWS Microsoft AD en tant que service éligible à la loi [HIPAA](#). Si vous avez signé un accord de partenariat commercial (BAA) avec AWS, vous pouvez utiliser AWS Managed Microsoft AD pour créer vos applications conformes à la loi HIPAA.

AWS propose un [livre blanc axé sur la loi HIPAA](#) aux clients qui souhaitent en savoir plus sur la manière dont ils peuvent tirer parti AWS pour le traitement et le stockage des informations de santé. Pour de plus amples informations, veuillez consulter [HIPAA compliance](#) (français non garanti).

Responsabilité partagée

La sécurité, et notamment la conformité aux réglementations FedRAMP, HIPAA et PCI, est une [responsabilité partagée](#). Il est important de comprendre que le statut de conformité de AWS Managed Microsoft AD ne s'applique pas automatiquement aux applications que vous exécutez dans le AWS cloud. Vous devez vous assurer que votre utilisation des AWS services est conforme aux normes.

Pour obtenir la liste complète des différents programmes de AWS conformité pris en charge par AWS Managed Microsoft AD, consultez la section [AWS Services concernés par programme de conformité](#).

Assurez la conformité à la norme PCI pour votre AWS annuaire Microsoft AD géré

Pour activer la conformité PCI pour votre annuaire Microsoft AD AWS géré, vous devez configurer des politiques de mot de passe détaillées, comme indiqué dans le document d'attestation de conformité (AOC) et de résumé des responsabilités PCI DSS fourni par AWS Artifact

Pour plus d'informations sur l'utilisation de politiques de mots de passe détaillées, veuillez consulter [Comprendre les politiques de AWS gestion des mots de passe Microsoft AD](#).

Amélioration de la configuration de sécurité de votre réseau AWS Managed Microsoft AD

Le groupe AWS de sécurité configuré pour le répertoire Microsoft AD AWS géré est configuré avec le minimum de ports réseau entrants requis pour prendre en charge tous les cas d'utilisation connus de votre répertoire AWS Microsoft AD géré. Pour plus d'informations sur le groupe de AWS sécurité provisionné, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Pour améliorer encore la sécurité réseau de votre annuaire Microsoft AD AWS géré, vous pouvez modifier le groupe AWS de sécurité en fonction des scénarios courants suivants.

Contrôleurs de domaine clients CIDR : ce bloc CIDR est l'endroit où résident les contrôleurs de domaine locaux de votre domaine.

CIDR du client : ce bloc CIDR permet à vos clients, tels que les ordinateurs ou les utilisateurs, de s'authentifier auprès de votre AWS Microsoft AD géré. Vos contrôleurs de domaine Microsoft AD AWS gérés résident également dans ce bloc CIDR.

Scénarios

- [AWS prise en charge des applications uniquement](#)
- [AWS applications uniquement avec support de confiance](#)

- [AWS support natif des applications et de la charge de travail Active Directory](#)
- [AWS prise en charge des applications et de la charge de travail Active Directory native avec prise en charge de la confiance](#)

AWS prise en charge des applications uniquement

Tous les comptes utilisateur sont configurés uniquement dans votre Microsoft AD AWS géré pour être utilisés avec les AWS applications prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- Suite rapide
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

Vous pouvez utiliser la configuration AWS de groupe de sécurité suivante pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine Microsoft AD AWS gérés.

Note

- Les éléments suivants ne sont pas compatibles avec cette configuration AWS de groupe de sécurité :
 - EC2 Instances Amazon
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Active Directory approuvé

- Clients ou serveurs joints au domaine

Règles entrantes

Aucune.

Règles sortantes

Aucune.

AWS applications uniquement avec support de confiance

Tous les comptes utilisateur sont configurés dans votre Microsoft AD AWS géré ou dans votre Active Directory approuvé pour être utilisés avec les AWS applications prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- Suite rapide
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe AWS de sécurité provisionné pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Microsoft AD gérés.

Note

- Les éléments suivants ne sont pas compatibles avec cette configuration AWS de groupe de sécurité :
 - EC2 Instances Amazon
 - Amazon FSx

- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- WorkSpaces
- Active Directory approuve
- Clients ou serveurs joints au domaine
- Cette configuration nécessite que vous vous assuriez que le réseau « Customer Domain Controllers CIDR » est sécurisé.
- TCP 445 est utilisé uniquement pour la création d'une approbation et peut être supprimé une fois que l'approbation a été établie.
- TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	Contrôleurs de domaine clients CIDR	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	Contrôleurs de domaine clients CIDR	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	Contrôleurs de domaine clients CIDR	LDAP	Directory, réplication, stratégie de

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
				groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	464	Contrôleurs de domaine clients CIDR	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	445	Contrôleurs de domaine clients CIDR	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP	135	Contrôleurs de domaine clients CIDR	Réplication	RPC, EPM
TCP	636	Contrôleurs de domaine clients CIDR	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	49152 - 65535	Contrôleurs de domaine clients CIDR	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP	3268 - 3269	Contrôleurs de domaine clients CIDR	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	Contrôleurs de domaine clients CIDR	Heure Windows	Heure Windows, approbations

Règles sortantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
Tous	Tous	Contrôleurs de domaine clients CIDR	Tout le trafic	

AWS support natif des applications et de la charge de travail Active Directory

Les comptes utilisateur sont fournis uniquement dans votre Microsoft AD AWS géré pour être utilisés avec les AWS applications prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- EC2 Instances Amazon
- Amazon FSx
- Suite rapide
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe AWS de sécurité provisionné pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Microsoft AD gérés.

Note

- Les approbations Active Directory ne peuvent pas être créées et AWS gérées entre votre annuaire Microsoft AD géré et le CIDR des contrôleurs de domaine clients.
- Cela vous oblige à vous assurer que le réseau « client-client CIDR » est sécurisé.
- TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.
- Si vous souhaitez utiliser une autorité de certification d'entreprise avec cette configuration, vous devez créer une règle sortante « TCP, 443, CA CIDR ».

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	Client CIDR	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	Client CIDR	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	Client CIDR	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	445	Client CIDR	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP et UDP	464	Client CIDR	Mot de passe Kerberos	Réplication, authentification d'utilisateur et

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
			(modification/définition)	d'ordinateur, approbations
TCP	135	Client CIDR	Réplication	RPC, EPM
TCP	636	Client CIDR	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	Client CIDR	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP	3268 - 3269	Client CIDR	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	9389	Client CIDR	SOAP	Services Web AD DS

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
UDP	123	Client CIDR	Heure Windows	Heure Windows, approbations
UDP	138	Client CIDR	DSN et NetLogon	DFS, stratégie de groupe

Règles sortantes

Aucune.

AWS prise en charge des applications et de la charge de travail Active Directory native avec prise en charge de la confiance

Tous les comptes utilisateur sont configurés dans votre Microsoft AD AWS géré ou dans votre Active Directory approuvé pour être utilisés avec les AWS applications prises en charge, telles que les suivantes :

- Amazon Chime
- Amazon Connect
- EC2 Instances Amazon
- Amazon FSx
- Suite rapide
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Vous pouvez modifier la configuration du groupe AWS de sécurité provisionné pour bloquer tout le trafic non essentiel vers vos contrôleurs de domaine AWS Microsoft AD gérés.

Note

- Cela vous oblige à vous assurer que les réseaux « contrôleurs de domaine client CIDR » et « CIDR client client » sont sécurisés.
- Le protocole TCP 445 avec le « CIDR des contrôleurs de domaine client » est utilisé uniquement pour la création de confiance et peut être supprimé une fois que la confiance a été établie.
- Le protocole TCP 445 avec le « CIDR client » doit être laissé ouvert car il est requis pour le traitement des politiques de groupe.
- TCP 636 est requis uniquement lorsque LDAP sur SSL est en cours d'utilisation.
- Si vous souhaitez utiliser une autorité de certification d'entreprise avec cette configuration, vous devez créer une règle sortante « TCP, 443, CA CIDR ».

Règles entrantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	Contrôleurs de domaine clients CIDR	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	Contrôleurs de domaine clients CIDR	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	389	Contrôleurs de domaine clients CIDR	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	464	Contrôleurs de domaine clients CIDR	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	445	Contrôleurs de domaine clients CIDR	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe
TCP	135	Contrôleurs de domaine clients CIDR	Réplication	RPC, EPM

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	636	Contrôleurs de domaine clients CIDR	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	Contrôleurs de domaine clients CIDR	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations
TCP	3268 - 3269	Contrôleurs de domaine clients CIDR	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
UDP	123	Contrôleurs de domaine clients CIDR	Heure Windows	Heure Windows, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	53	Contrôleurs de domaine clients CIDR	DNS	Authentification d'utilisateur et d'ordinateur, résolution de noms, approbations
TCP et UDP	88	Contrôleurs de domaine clients CIDR	Kerberos	Authentification d'utilisateur et d'ordinateur, approbations au niveau de la forêt
TCP et UDP	389	Contrôleurs de domaine clients CIDR	LDAP	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP et UDP	445	Contrôleurs de domaine clients CIDR	SMB / CIFS	Réplication, authentification d'utilisateur et d'ordinateur, approbations de stratégie de groupe

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP et UDP	464	Contrôleurs de domaine clients CIDR	Mot de passe Kerberos (modification/définition)	Réplication, authentification d'utilisateur et d'ordinateur, approbations
TCP	135	Contrôleurs de domaine clients CIDR	Réplication	RPC, EPM
TCP	636	Contrôleurs de domaine clients CIDR	LDAP SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	49152 - 65535	Contrôleurs de domaine clients CIDR	RPC	Réplication, authentification d'utilisateur et d'ordinateur, stratégie de groupe, approbations

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
TCP	3268 - 3269	Contrôleurs de domaine clients CIDR	LDAP GC et LDAP GC SSL	Directory, réplication, stratégie de groupe d'authentification d'utilisateur et d'ordinateur, approbations
TCP	9389	Contrôleurs de domaine clients CIDR	SOAP	Services Web AD DS
UDP	123	Contrôleurs de domaine clients CIDR	Heure Windows	Heure Windows, approbations
UDP	138	Contrôleurs de domaine clients CIDR	DSN et NetLogon	DFS, stratégie de groupe

Règles sortantes

Protocole	Plage de ports	Source	Type de trafic	Utilisation d'Active Directory
Tous	Tous	Contrôleurs de domaine clients CIDR	Tout le trafic	

Modification des paramètres de sécurité de l'annuaire Microsoft AD AWS géré

Vous pouvez configurer des paramètres d'annuaire précis pour votre AWS Microsoft AD géré afin de répondre à vos exigences de conformité et de sécurité sans augmenter la charge de travail opérationnelle. Dans les paramètres de l'annuaire, vous pouvez mettre à jour la configuration des canaux sécurisés pour les protocoles et les chiffrements utilisés dans votre annuaire. Par exemple, vous avez la possibilité de désactiver les anciens chiffrements individuels, tels que RC4 le DES, et les protocoles, tels que SSL 2.0/3.0 et TLS 1.0/1.1. AWS Managed Microsoft AD déploie ensuite la configuration sur tous les contrôleurs de domaine de votre annuaire, gère les redémarrages des contrôleurs de domaine et maintient cette configuration à mesure que vous augmentez ou que vous en déployez d'autres. Régions AWS Pour plus d'informations sur tous les paramètres disponibles, veuillez consulter [Liste des paramètres de sécurité de l'annuaire](#).

Modifier les paramètres de sécurité de l'annuaire

Vous pouvez configurer et modifier les paramètres de n'importe lequel de vos annuaires.

Pour modifier les paramètres de l'annuaire

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sous Networking & security (Réseau et sécurité), recherchez Directory settings (Paramètres de l'annuaire), puis choisissez Edit settings (Modifier les paramètres).
4. Dans Edit settings (Modifier les paramètres), modifiez la valeur des paramètres que vous souhaitez modifier. Lorsque vous modifiez un paramètre, son statut passe de Default (Par défaut) à Ready to Update (Prêt pour la mise à jour). Si vous avez déjà modifié le paramètre, son statut passe de Updated (Mis à jour) à Ready to Update (Prêt pour la mise à jour). Choisissez ensuite Review (Examiner).
5. Dans Review and update setting (Examen et mise à jour des paramètres), veuillez consulter Directory settings (Paramètres de l'annuaire) et assurez-vous que les nouvelles valeurs sont toutes correctes. Si vous souhaitez apporter d'autres modifications à vos paramètres, choisissez Edit settings (Modifier les paramètres). Lorsque vous êtes satisfait de vos modifications et que vous êtes prêt à implémenter les nouvelles valeurs, choisissez Mettre à jour les paramètres. Ensuite, vous êtes redirigé vers la page d'identification du répertoire.

 Note

Sous Directory settings (Paramètres de l'annuaire), vous pouvez consulter le statut de vos paramètres mis à jour. Lorsque les paramètres sont implémentés, le statut affiche Updating (Mise à jour). Vous ne pouvez pas modifier d'autres paramètres lorsqu'un paramètre affiche la mention Updating (Mise à jour) sous Status (Statut). Le statut affiche la mention Updated (Mis à jour) si le paramètre est correctement mis à jour avec votre modification. Le statut affiche la mention Failed (Échec) si le paramètre ne se met pas à jour avec votre modification.

Échec des paramètres de sécurité de l'annuaire

Si une erreur se produit lors d'une mise à jour des paramètres, le statut affiche la mention Failed (Échec). En cas d'échec, les paramètres ne sont pas mis à jour avec les nouvelles valeurs et les valeurs d'origine restent implémentées. Vous pouvez réessayer de mettre à jour ces paramètres ou rétablir leurs valeurs précédentes.

Pour résoudre l'échec de la mise à jour des paramètres

- Sous Directory settings (Paramètres de l'annuaire), choisissez Resolve failed settings (Résoudre l'échec de mise à jour des paramètres). Ensuite, effectuez l'une des actions suivantes :
 - Pour rétablir vos paramètres à leur valeur d'origine avant l'échec de mise à jour, choisissez Revert failed settings (Rétablir les paramètres qui n'ont pas pu être mis à jour). Choisissez ensuite Revert (Rétablir) dans la fenêtre contextuelle.
 - Pour réessayer de mettre à jour les paramètres de votre annuaire, choisissez Retry failed settings (Réessayer les paramètres qui n'ont pas pu être mis à jour). Si vous souhaitez apporter des modifications supplémentaires aux paramètres de votre annuaire avant de réessayer les mises à jour qui ont échoué, choisissez Continue editing (Continuer les modifications). Sous Review and retry failed updates (Examiner et réessayer les mises à jour qui ont échoué), choisissez Update settings (Mettre à jour les paramètres).

Liste des paramètres de sécurité de l'annuaire

La liste suivante indique le type, le nom du paramètre, le nom de l'API, les valeurs potentielles et la description du paramètre pour tous les paramètres de sécurité d'annuaire disponibles.

TLS 1.2 et AES 256/256 sont les paramètres de sécurité d'annuaire par défaut si tous les autres paramètres de sécurité sont désactivés. Ils ne peuvent pas être désactivés.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
Authentification basée sur des certificats	Competition de l'antidatage des certificats	CERTIFICATE_BACKDATING_COMPENSATION	Années : 0 à 50	Spécifiez une valeur indiquant la durée pendant laquelle un certificat peut être antérieur à un utilisateur dans Active Directory et continuer à être utilisé pour l'authentification dans Active Directory. La valeur par défaut est de 10 minutes. Vous pouvez définir cette valeur entre 1 seconde et 50 ans.
			Mois : 0 à 11	
			Jours : 0 à 30	
			Heures : 0 à 23	
			Minutes : 0 à 59	
			Secondes : 0 à 59	

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
				compatibilité pour Strong Certificate Binding Enforce. Pour plus d'informations, consultez la section KB5014754—Modifications de l'authentification basée sur les certificats sur les contrôleurs de domaine Windows dans la documentation Microsoft Support.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	Application stricte des certificats	CERTIFICATE_STRONG_ENFORCEMENT	Compatibilité, Application complète	Spécifiez l'un des types d'application suivants : Compatibilité : l'authentification est autorisée si un certificat ne peut pas être clairement mappé à un utilisateur. Si le certificat est antérieur au compte utilisateur dans Active Directory, vous devez également définir la compensation de l'antidatage des certificats, sinon l'authentification échouera.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
				• Application complète (par défaut) : l'authentification n'est pas autorisée si un certificat ne peut pas être clairement mappé à un utilisateur. Si vous choisissez ce type d'application, la compensation de l'antidatage des certificats ne peut pas être configurée. Pour plus d'informations, consultez la section KB5014754—Modifications

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
				de l'authentification basée sur les certificats sur les contrôleurs de domaine Windows dans la documentation Microsoft Support.
Canal sécurisé : chiffrement	AES 128	AES_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement AES 128/128 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.
	DE 56/56	DES_56_56	Activer, Désactiver	Activez ou désactivez le chiffrement DES 56/56 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	RC2 40/128	RC2_40_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 40/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.
	RC2 56/128	RC2_56_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 56/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	RC2 128/128	RC2_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC2 128/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.
	RC4 40/128	RC4_40_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 40/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	RC4 56/128	RC4_56_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 56/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.
	RC4 64/128	RC4_64_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 64/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	RC4 128/128	RC4_128_128	Activer, Désactiver	Activez ou désactivez le chiffrement RC4 128/128 pour les communications par canal sécurisé entre les contrôleurs de domaine de votre annuaire.
	Triple DES 168	3DES_168_168	Activer, Désactiver	Activez ou désactivez le chiffrement Triple DES 168/168 pour sécuriser les communications entre les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
Canal sécurisé : protocole	PCT 1.0	PCT_1_0	Activer, Désactiver	Activez ou désactivez le protocole PCT 1.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.
	SSL 2.0	SSL_2_0	Activer, Désactiver	Activez ou désactivez le protocole SSL 2.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	SSL 3.0	SSL_3_0	Activer, Désactiver	Activez ou désactivez le protocole SSL 3.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.
	TLS 1.0	TLS_1_0	Activer, Désactiver	Activez ou désactivez le protocole TLS 1.0 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Type	Nom du paramètre	Nom d'API	Valeurs potentielles	Description du paramètre
	TLS 1.1	TLS_1_1	Activer, Désactiver	Activez ou désactivez le protocole TLS 1.1 pour sécuriser les communications (serveur et client) sur les contrôleurs de domaine de votre annuaire.

Activez le chiffrement à clé publique pour l'authentification initiale (PKINIT) pour vos utilisateurs gérés de AWS Microsoft AD

AWS Les annuaires Microsoft AD gérés utilisent par défaut une liaison de certificats renforcée, ce qui nécessite un mappage explicite entre les certificats et les objets AD. Les mappages suivants sont considérés comme fiables pour AWS Managed Microsoft AD :

- altSecurityIdentitiesÉmetteur et numéro de série
- altSecurityIdentitiesIdentifiant clé du sujet
- altSecurityIdentities SHA1 Hachage de la clé publique

Ces attributs permettent un mappage renforcé des certificats, qui renforce la sécurité de l'authentification basée sur les certificats en exigeant certificate-to-user des relations explicites définies dans Active Directory. Cela permet de prévenir les attaques d'escalade de privilèges basées sur les certificats

Vous pouvez utiliser cette procédure pour configurer des liaisons de certificats renforcées afin de prévenir les attaques par augmentation de privilèges tout en préservant la fonctionnalité d'authentification des certificats.

Pour plus d'informations, voir [Microsoft KB5 014754 : Modifications de l'authentification basée sur des certificats sur les contrôleurs](#) de domaine Windows

Prérequis

- Un annuaire Microsoft AD AWS géré avec une autorité de certification configurée
- Accès administratif à votre environnement Active Directory
- PowerShell avec le module Active Directory installé
- Le certificat que vous souhaitez associer à l'objet AD

AltSecurityIdentityAttribut de carte

1. Choisissez l'une des méthodes de AltSecurityIdentity mappage suivantes en fonction des informations de votre certificat :

- SHA1 hash — Utilise le SHA1 hachage de la clé publique du certificat

Pour le mappage de SHA1 hachage, extrayez le hachage du certificat et appliquez-le à l'objet utilisateur :

```
$Username = 'YourUsername'
$cert = certutil -dump "YourCertificate.cer"
$certHash = ($cert | Select-String -Pattern "(sha1):*" |
    Select-String -Pattern "Cert").ToString().TrimStart('Cert Hash sha1:').Replace(' ', '')
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<SHA1-PUKEY>$CertHash"}
```

- Émetteur et numéro de série : utilise le nom et le numéro de série de l'émetteur du certificat

Pour le mappage de l'émetteur et du numéro de série, utilisez l'émetteur et le numéro de série du certificat :

```
$Username = 'YourUsername'
$IssuerName = 'YourCertificateIssuer'
$SerialNumber = 'YourCertificateSerialNumber'
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<I>$IssuerName<SR>$SerialNumber"}
```

- Identifiant de clé d'objet : utilise l'extension d'identifiant de clé d'objet du certificat

Pour le mappage de l'identifiant de clé d'objet, utilisez l'identifiant de clé d'objet du certificat :

```
$Username = 'YourUsername'
$SubjectKeyIdentifier = 'YourSubjectKeyIdentifier'
Set-ADUser -Identity $Username -Add @{altSecurityIdentities='"X509:<SKI>
$SubjectKeyIdentifier"}
```

2. Vérifiez que le mappage a été correctement appliqué :

```
Get-ADUser -Identity $Username -Properties altSecurityIdentities |
Select-Object -ExpandProperty altSecurityIdentities
```

3. Attendez que la réplication Active Directory soit terminée (généralement 15 à 30 secondes) avant de tester l'authentification par certificat.

Exemple : certificat groupé mappant l' AltSecurityIdentity attribut

L'exemple suivant montre comment mapper un AltSecurityIdentity attribut pour plusieurs certificats utilisateur à partir d'une autorité de certification :

```
$CertificateTemplateName = 'User'
$Now = (($Get-Date).ToString($(Get-culture).DateTimeFormat.ShortDatePattern))
$Restrict = "Disposition=20,NotAfter>=$Now,Certificate Template=
$CertificateTemplateName"
$Out = "SerialNumber,Certificate Hash,User Principal
Name,RequesterName,CommonName,CertificateTemplate,NotBefore,NotAfter"
$Certs = certutil -view -restrict $Restrict -out $Out csv | ConvertFrom-CSV
$UserSha1HashMapping = @{}

ForEach ($Cert in $Certs) {
    $UPN = $Cert.'User Principal Name'
    $Username, $Domain = $UPN.Split('@')
    $CertificateThumbprint = ($Cert.'Certificate Hash').Replace(' ','')
    $AdUserObject = Get-ADUser -Identity $Username
    If ($AdUserObject -And $AdUserObject.Count -gt 1) {
        Write-Output "Unable to map user: $Username, multiple user objects found"
        Continue
    }
    If ($AdUserObject) {
        If ($UserSha1HashMapping.Keys -Contains $Username) {
            $UserSha1HashMapping[$Username] += $CertificateThumbprint
        }
    }
}
```

```
        } Else {
            $UserSha1HashMapping[$Username] = @($CertificateThumbprint)
        }
    }
}

ForEach ($User in $UserSha1HashMapping.Keys) {
    Write-Output "Mapping altSecurityIdentity for $User"
    $UserObject = Get-ADUser -Identity $User | Get-ADObject -Properties
'altSecurityIdentities'
    $altSecurityIdentities = $UserObject.altSecurityIdentities
    ForEach ($thumbprint in $UserSha1HashMapping[$User]) {
        $SHA1PUKEY = "X509:<SHA1-PUKEY>$thumbprint"
        If ($altSecurityIdentities -Contains $SHA1PUKEY) {
            Write-Output "Skipping $thumbprint, already mapped."
            Continue
        }
        Write-Output "Adding $thumbprint to $User as altSecurityIdentity"
        Set-ADUser -Identity $User -Add @{'altSecurityIdentities'=$SHA1PUKEY}
    }
}
```

Étapes suivantes

- Testez l'authentification basée sur les certificats avec vos certificats mappés
- Configurez vos applications pour utiliser les certificats mappés pour l'authentification
- [Surveillez votre Microsoft AD AWS géré](#) pour les événements d'authentification

Configurer le AWS CA privée connecteur pour AD pour Microsoft AD AWS géré

Vous pouvez intégrer votre Microsoft AD AWS géré à [AWS Autorité de certification privée \(CA\)](#) pour émettre et gérer des certificats pour vos contrôleurs de domaine Active Directory, vos utilisateurs joints à un domaine, vos groupes et vos machines. AWS CA privée Connector for Active Directory vous permet d'utiliser une solution de remplacement entièrement gérée AWS CA privée pour votre entreprise autogérée CAs sans qu'il soit nécessaire de déployer, de patcher ou de mettre à jour des agents locaux ou des serveurs proxy.

Vous pouvez configurer AWS CA privée l'intégration à votre annuaire via la Directory Service console, la console AWS CA privée Connector for Active Directory ou en appelant

l'[CreateTemplate](#) API. Pour configurer l'intégration de Private CA via la console AWS CA privée Connector for Active Directory, reportez-vous à la section [Création d'un modèle de connecteur](#). Consultez les étapes suivantes pour configurer cette intégration depuis la Directory Service console.

Configuration AWS CA privée du connecteur pour AD

Pour créer un connecteur CA privé pour Active Directory

1. Connectez-vous à la Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Dans l'onglet Gestion des AWS applications et dans la section Applications et services, sélectionnez AWS CA privée Connector for AD.
4. Sur la page Créer un certificat d'autorité de certification privée pour Active Directory, suivez les étapes pour créer votre connecteur d'autorité de certification privée pour Active Directory.

Pour de plus amples informations, veuillez consulter [Creating a connector](#) (français non garanti).

AWS CA privée Connecteur de visualisation pour AD

Pour afficher les détails du connecteur Private CA

1. Connectez-vous à la Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Dans l'onglet Gestion des AWS applications et dans la section Applications et services, consultez vos connecteurs d'autorité de certification privée et l'autorité de certification privée associée. Les champs suivants s'affichent :
 - a. AWS CA privée ID du connecteur : identifiant unique d'un AWS CA privée connecteur. Sélectionnez-le pour afficher la page de détails.
 - b. AWS CA privée objet — Informations concernant le nom distinctif de l'autorité de certification. Sélectionnez-le pour afficher la page de détails.
 - c. État — Résultats de la vérification de l'état du AWS CA privée connecteur et AWS CA privée :
 - Actif — Les deux contrôles sont réussis

- Échec d'une demi-vérification — échec d'une vérification
- Échec : les deux vérifications échouent

Pour obtenir des informations sur le statut d'échec, passez le pointeur de la souris sur le lien hypertexte pour voir quelle vérification a échoué.

- d. État d'inscription des certificats DC — Vérification de l'état du certificat du contrôleur de domaine :
 - Activé — L'inscription aux certificats est activée
 - Désactivé — L'inscription au certificat est désactivée
- e. Date de création : date de création AWS CA privée du connecteur.

Pour plus d'informations, veuillez consulter [View connector details](#) (français non garanti).

Le tableau suivant présente les différents statuts d'inscription des certificats de contrôleur de domaine pour AWS Managed Microsoft AD with AWS CA privée.

État d'inscription au DC	Description	Action requise
Activées	Les certificats de contrôleur de domaine sont correctement inscrits dans votre annuaire.	Aucune action requise.
Échec	L'activation ou la désactivation de l'inscription des certificats de contrôleur de domaine a échoué pour votre annuaire.	Si votre action d'activation échoue, réessayez en désactivant les certificats de contrôleur de domaine, puis en les réactivant. Si votre action de désactivation échoue, réessayez en activant les certificats de contrôleur de domaine, puis en les désactivant à nouveau. Si la nouvelle tentative échoue, contactez le AWS Support.
Dégradé	Les contrôleurs de domaine rencontrent des problèmes de	Vérifiez les politiques relatives aux points de terminaison AWS

État d'inscription au DC	Description	Action requise
	connectivité réseau lorsqu'ils communiquent avec les AWS CA privée terminaux.	CA privée VPC et aux compartiments S3 pour autoriser la connectivité réseau avec votre annuaire. Pour plus d'informations, consultez Résoudre les messages d'exception des autorités de certification AWS privées et Résoudre les problèmes de révocation de AWS CA privée certificats .
Désactivées	L'inscription des certificats de contrôleur de domaine est correctement désactivée pour votre annuaire.	Aucune action requise.
Désactivation	La désactivation de l'inscription des certificats de contrôleur de domaine est en cours.	Aucune action requise.
Activation	L'activation de l'inscription des certificats de contrôleur de domaine est en cours.	Aucune action requise.

Configuration des politiques AD

AWS CA privée Le Connector for AD doit être configuré de manière AWS à ce que les contrôleurs de domaine et les objets Microsoft AD gérés puissent demander et recevoir des certificats. Configurez votre objet de stratégie de groupe ([GPO](#)) afin de AWS CA privée pouvoir délivrer des certificats aux objets Microsoft AD AWS gérés.

Configuration des politiques Active Directory pour les contrôleurs de domaine

Activer les politiques Active Directory pour les contrôleurs de domaine

1. Ouvrez l'onglet Réseau et sécurité.
2. Choisissez AWS CA privée Connectors.

3. Choisissez un connecteur lié au AWS CA privée sujet qui émet des certificats de contrôleur de domaine pour votre annuaire.
4. Choisissez Actions, puis Activer les certificats de contrôleur de domaine.

 Important

Configurez un modèle de contrôleur de domaine valide avant d'activer les certificats de contrôleur de domaine afin d'éviter les mises à jour différées.

Une fois que vous avez activé l'inscription des certificats de contrôleur de domaine, les contrôleurs de domaine de votre annuaire demandent et reçoivent des certificats de AWS CA privée Connector for AD.

Pour modifier votre émission AWS CA privée de certificats de contrôleur de domaine, connectez d'abord le nouveau AWS CA privée à votre annuaire à l'aide d'un nouveau AWS CA privée Connector for AD. Avant d'activer l'enregistrement des certificats sur le nouveau AWS CA privée, désactivez l'enregistrement des certificats sur le certificat existant :

Désactiver les certificats de contrôleur de domaine

1. Ouvrez l'onglet Réseau et sécurité.
2. Choisissez AWS CA privée Connectors.
3. Choisissez un connecteur lié au AWS CA privée sujet qui émet des certificats de contrôleur de domaine pour votre annuaire.
4. Choisissez Actions, Désactiver les certificats de contrôleur de domaine.

Configuration des politiques Active Directory pour les utilisateurs, ordinateurs et machines joints à un domaine

Configuration des objets de stratégie de groupe

1. Connectez-vous à l'instance d'administration Microsoft AD AWS gérée et ouvrez le [Gestionnaire de serveur](#) depuis le menu Démarrer.
2. Sous Outils, sélectionnez Gestion des politiques de groupe.
3. Sous Forêt et domaines, recherchez l'unité organisationnelle (UO) de votre sous-domaine (par exemple, corp il s'agit de votre unité organisationnelle de sous-domaine si vous avez suivi les

procédures décrites dans [Création de votre AWS compte Microsoft AD géré](#)) et cliquez avec le bouton droit sur l'unité organisationnelle de votre sous-domaine. Choisissez Créer un GPO dans ce domaine, liez-le ici et entrez PCA GPO pour le nom. Choisissez OK.

4. Le GPO nouvellement créé apparaît après le nom de votre sous-domaine. Cliquez avec le bouton droit sur PCA GPO et choisissez Modifier. Si une boîte de dialogue s'ouvre avec un message d'alerte indiquant qu'il s'agit d'un lien et que les modifications sont propagées dans le monde entier, confirmez le message en choisissant OK pour continuer. La fenêtre de l'éditeur de gestion des politiques de groupe s'ouvre.
5. Dans la fenêtre de l'éditeur de gestion des stratégies de groupe, accédez à Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Politiques de clé publique (choisissez le dossier).
6. Sous Type d'objet, choisissez Certificate Services Client - Certificate Enrollment Policy.
7. Dans la fenêtre Client des services de certificats - Politique d'inscription des certificats, remplacez le modèle de configuration par Activé.
8. Vérifiez que la politique d'inscription Active Directory est sélectionnée et activée. Choisissez Ajouter.
9. La boîte de dialogue du serveur de politiques d'inscription aux certificats s'ouvre. Entrez le point de terminaison du serveur de politique d'inscription des certificats que vous avez généré lorsque vous avez créé votre connecteur dans le champ Entrez l'URI de la politique du serveur d'inscription. Laissez le type d'authentification Windows intégré.
10. Choisissez Valider. Une fois la validation réussie, choisissez Ajouter.
11. Revenez à la boîte de dialogue Client des services de certificats - Politique d'inscription des certificats et cochez la case à côté du connecteur nouvellement créé pour vous assurer que le connecteur est la politique d'inscription par défaut.
12. Choisissez la politique d'inscription Active Directory, puis sélectionnez Supprimer.
13. Dans la boîte de dialogue de confirmation, choisissez Oui pour supprimer l'authentification basée sur LDAP.
14. Choisissez Appliquer puis OK dans la fenêtre Client des services de certificats - Politique d'inscription des certificats. Fermez ensuite la fenêtre.
15. Sous Type d'objet pour le dossier Public Key Policies, choisissez Certificate Services Client - Auto-Enrollment.
16. Modifiez l'option Modèle de configuration sur Activé.
17. Vérifiez que les options Renouveler les certificats expirés et Mettre à jour les certificats sont toutes deux sélectionnées. Laissez les autres paramètres tels quels.

18. Choisissez Appliquer, puis OK, puis fermez la boîte de dialogue.

Configurez ensuite les politiques de clé publique pour la configuration utilisateur en répétant les étapes 6 à 17 dans la section Configuration utilisateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Politiques de clé publique.

Une fois que vous avez terminé la configuration GPOs et les politiques de clé publique, les objets du domaine demandent des certificats à AWS CA privée Connector for AD et reçoivent des certificats émis par AWS CA privée.

Confirmation de la AWS CA privée délivrance d'un certificat

Le processus de mise AWS CA privée à jour pour émettre des certificats pour votre Microsoft AD AWS géré peut prendre jusqu'à 8 heures.

Vous pouvez effectuer l'une des actions suivantes :

- Vous pouvez attendre cette période.
- Vous pouvez redémarrer les machines jointes au domaine Microsoft AD AWS géré qui ont été configurées pour recevoir des certificats du AWS CA privée. Vous pouvez ensuite confirmer que les certificats ont AWS CA privée été émis aux membres de votre domaine Microsoft AD AWS géré en suivant la procédure décrite dans la [Microsoftdocumentation](#).
- Vous pouvez utiliser la PowerShell commande suivante pour mettre à jour les certificats de votre Microsoft AD AWS géré :

```
certutil -pulse
```

Surveillez votre Microsoft AD AWS géré

Vous pouvez tirer le meilleur parti de votre Microsoft AD AWS géré en découvrant les différents statuts de Microsoft AD AWS géré et ce qu'ils signifient pour votre Microsoft AD AWS géré. Vous pouvez également utiliser AWS des services tels qu'Amazon Simple Notification Service et Amazon CloudWatch pour surveiller votre Microsoft AD AWS géré. Amazon Simple Notification Service peut vous envoyer des notifications concernant le statut de votre annuaire Microsoft AD AWS géré. Amazon CloudWatch peut surveiller les performances de vos contrôleurs de domaine Microsoft AD AWS gérés.

Tâches pour surveiller votre Microsoft AD AWS géré

- [Comprendre le statut de votre annuaire Microsoft AD AWS géré](#)
- [Activation des notifications d'état de l'annuaire Microsoft AD AWS géré avec Amazon Simple Notification Service](#)
- [Comprendre les journaux de votre annuaire Microsoft AD AWS géré](#)
- [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#)
- [Utilisation CloudWatch pour surveiller les performances de vos contrôleurs de domaine Microsoft AD AWS gérés](#)
- [Désactivation du transfert de CloudWatch journaux Amazon pour AWS Managed Microsoft AD](#)
- [Surveillance du serveur DNS avec Microsoft Event Viewer](#)

Comprendre le statut de votre annuaire Microsoft AD AWS géré

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le [centre AWS Support](#).

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Il s'agit notamment des activités de maintenance opérationnelle normales telles que l'application de correctifs ou la rotation des EC2 instances, le repérage temporaire par une application sur l'un de vos contrôleurs de domaine ou les modifications que vous avez apportées à votre réseau qui perturbent par inadvertance les communications d'annuaire. Pour plus d'informations, veuillez consulter [Résolution des problèmes liés AWS à Managed Microsoft AD](#), [Résolution des problèmes liés à AD Connector](#), [Résolution des problèmes de Simple AD](#). Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le [centre AWS Support](#).

Important

Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#).

Demandé

La demande de création de votre annuaire est actuellement en attente.

RestoreFailed

Échec de la restauration de l'annuaire à partir d'un instantané. Renouvelez l'opération de restauration. Si le problème persiste, utilisez un autre instantané ou contactez le [centre AWS Support](#).

Restauration en cours

L'annuaire est en cours de restauration à partir d'un instantané automatique ou manuel. La restauration à partir d'un instantané prend généralement plusieurs minutes, selon la taille des données de l'annuaire dans l'instantané.

Activation des notifications d'état de l'annuaire Microsoft AD AWS géré avec Amazon Simple Notification Service

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti si votre annuaire passe du statut Actif à l'[état Inactif](#). Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article Directory Service en tant qu'éditeur à une rubrique Amazon SNS. Lorsqu'il Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de répertoire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter [Qu'est-ce qu'Amazon SNS ?](#)

Note

Les notifications d'état du répertoire sont une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Activation d'Amazon SNS

Ce qui suit explique comment activer Amazon SNS pour votre AWS Microsoft AD géré :

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :

- Si plusieurs régions apparaissent sous Réplication multi-régions, sélectionnez la région dans laquelle vous souhaitez activer la messagerie SNS, puis cliquez sur l'onglet Maintenance. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication multi-régions, sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Create notification (Créer une notification).
 5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

 Note

Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.

Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

 Note

Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique [DirectoryServiceFullAccess](#) gérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre sujet, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Choisissez Créer.

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambda ou, vous pouvez le faire depuis la console Amazon [SNS](#).

Suppression des messages d'état d'annuaire d'une rubrique Amazon SNS

Ce qui suit explique comment supprimer les messages d'état de votre annuaire Microsoft AD AWS géré d'une rubrique Amazon SNS :

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication multi-régions, sélectionnez la région dans laquelle vous souhaitez supprimer les messages de statut, puis cliquez sur l'onglet Maintenance. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication multi-régions, sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée.

Supprimer une rubrique Amazon SNS

Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console [Amazon SNS](#).

Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.

Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant le sujet supprimé, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance du répertoire indiquant que le sujet est introuvable.

Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Pour plus d'informations sur la façon de supprimer une rubrique Amazon SNS, consultez [Supprimer une rubrique Amazon SNS](#) et un abonnement.

Comprendre les journaux de votre annuaire Microsoft AD AWS géré

Les journaux de sécurité des instances de contrôleurs de domaine Microsoft AD AWS gérés sont archivés pendant un an. Vous pouvez également configurer votre annuaire Microsoft AD AWS géré pour transférer les journaux des contrôleurs de domaine vers Amazon CloudWatch Logs en temps quasi réel. Pour de plus amples informations, veuillez consulter [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#).

AWS enregistre les événements suivants à des fins de conformité.

Catégorie de surveillance	Définition de stratégie	État d'audit
Connexion au compte	Audit de validation des identifiants	Réussite, échec
	Audit des autres événements d'ouverture de session de compte	Réussite, échec
	Audit du service d'authentification Kerberos	Réussite, échec
Gestion de compte	Audit de la gestion des comptes informatiques	Réussite, échec
	Audit des autres événements de gestion des comptes	Réussite, échec
	Audit de la gestion des groupes de sécurité	Réussite, échec

Catégorie de surveillance	Définition de stratégie	État d'audit
	Audit de la gestion des comptes d'utilisateur	Réussite, échec
Suivi détaillé	Audit d'activité DPAPI	Réussite, échec
	Audit d'activité PNP	Réussite
	Audit de la création de processus	Réussite, échec
Accès DS	Audit de l'accès aux services d'annuaire	Réussite, échec
	Audit des changements de services d'annuaire	Réussite, échec
Connexion/déconnexion	Audit de verrouillage de compte	Réussite, échec
	Audit de déconnexion	Réussite
	Audit de connexion	Réussite, échec
	Audit des autres événements d'ouverture/fermeture de session	Réussite, échec
	Audit des connexions spéciales	Réussite, échec
Accès aux objets	Audit des autres événements d'accès aux objets	Réussite, échec
	Audit des supports de stockage amovibles	Réussite, échec
	Audit du transfert des stratégies d'accès centrales	Réussite, échec

Catégorie de surveillance	Définition de stratégie	État d'audit
Modifications des stratégies	Audit de modification des stratégies	Réussite, échec
	Audit de modification des stratégies d'authentification	Réussite, échec
	Audit de modification des stratégies d'autorisation	Réussite, échec
	Audit de modification de la stratégie au niveau des règles MPSSVC	Réussite
	Audit des autres événements de modification de stratégie	Échec
Utilisation des privilèges	Audit de l'utilisation des privilèges sensibles	Réussite, échec
Système	IPsec Pilote d'audit	Réussite, échec
	Audit des autres événements système	Réussite, échec
	Audit des changements d'état de sécurité	Réussite, échec
	Audit de l'extension du système de sécurité	Réussite, échec
	Audit de l'intégrité du système	Réussite, échec

Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD

Vous pouvez utiliser la Directory Service console ou APIs pour transférer les journaux des événements de sécurité du contrôleur de domaine vers Amazon CloudWatch Logs pour votre

Microsoft AD AWS géré. Cela vous aide à répondre à vos exigences en matière de sécurité, d'audit et de conservation des journaux en assurant la transparence des événements de sécurité dans votre annuaire.

CloudWatch Les journaux peuvent également transmettre ces événements à d'autres AWS comptes, AWS services ou applications tierces. Cela facilite la surveillance et la configuration centralisées des alertes afin de détecter et de réagir de manière proactive aux activités inhabituelles en temps quasi réel.

Une fois activé, vous pouvez utiliser la console CloudWatch Logs pour récupérer les données du groupe de journaux que vous avez spécifié lorsque vous avez activé le service. Ce groupe de journaux contient les journaux de sécurité de vos contrôleurs de domaine.

Pour plus d'informations sur les groupes de journaux et sur la façon de lire leurs données, consultez la section [Utilisation des groupes de journaux et des flux](#) de CloudWatch journaux dans le guide de l'utilisateur Amazon Logs.

Note

Le transfert de journal est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Une fois activée, la fonctionnalité de transfert de journaux commencera à transmettre les journaux de vos contrôleurs de domaine au groupe de CloudWatch journaux spécifié. Les journaux créés avant l'activation du transfert de journaux ne seront pas transférés vers le groupe de CloudWatch journaux.

Rubriques

- [Utilisation du AWS Management Console pour activer le transfert de CloudWatch journaux Amazon Logs](#)
- [À l'aide de la CLI ou PowerShell pour activer le transfert de CloudWatch journaux Amazon Logs](#)

Utilisation du AWS Management Console pour activer le transfert de CloudWatch journaux Amazon Logs

Vous pouvez activer le transfert CloudWatch des journaux Amazon Logs pour votre AWS Managed Microsoft AD dans le AWS Management Console.

1. Dans le panneau de navigation de la [console Directory Service](#), choisissez Annuaire.
2. Choisissez l'ID de répertoire du répertoire Microsoft AD AWS géré que vous souhaitez partager.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez activer le transfert de journaux, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Multi-Regions replication (Réplication multi-régions), choisissez l'onglet Networking & security (Réseau et sécurité).
4. Dans la section Transfert de journaux, choisissez Activer.
5. Dans la boîte de CloudWatch dialogue Activer le transfert du journal vers, choisissez l'une des options suivantes :
 - a. Sélectionnez Créer un nouveau groupe de CloudWatch journaux, sous Nom du groupe de CloudWatch journaux, spécifiez un nom auquel vous pouvez faire référence dans CloudWatch Logs.
 - b. Sélectionnez Choisir un groupe de CloudWatch journaux existant, puis sous Groupes de CloudWatch journaux existants, sélectionnez un groupe de journaux dans le menu.
6. Passez en revue les informations de tarification et le lien, puis choisissez Activer.

À l'aide de la CLI ou PowerShell pour activer le transfert de CloudWatch journaux Amazon Logs

Avant de pouvoir utiliser la [ds create-log-subscription](#) commande, vous devez d'abord créer un groupe de CloudWatch journaux Amazon, puis créer une politique de ressources IAM qui accordera les autorisations nécessaires à ce groupe. Pour activer le transfert de journaux à l'aide de la CLI ou PowerShell, procédez comme suit.

Étape 1 : créer un groupe de CloudWatch journaux dans Logs

Créez un groupe de journaux qui servira à recevoir les journaux de sécurité de vos contrôleurs de domaine. Nous vous conseillons de faire précéder le nom de `/aws/directoryservice/`, mais ce n'est pas obligatoire. Par exemple :

CLI Command

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-CWLogGroup -LogGroupName '/aws/directoryservice/d-1111111111'
```

Pour savoir comment créer un groupe de CloudWatch journaux, consultez la section [Créer un groupe de CloudWatch journaux dans](#) la section Logs du guide de l'utilisateur Amazon CloudWatch Logs.

Étape 2 : créer une politique de ressources pour CloudWatch les journaux dans IAM

Créez une politique de ressources de CloudWatch journaux accordant le Directory Service droit d'ajouter des journaux dans le nouveau groupe de journaux que vous avez créé à l'étape 1. Vous pouvez soit spécifier l'ARN exact du groupe de journaux pour limiter Directory Service l'accès à d'autres groupes de journaux, soit utiliser un caractère générique pour inclure tous les groupes de journaux. L'exemple de politique suivant utilise la méthode des caractères génériques pour identifier que tous les groupes de journaux commençant `/aws/directoryservice/` par le AWS compte où réside votre répertoire seront inclus.

Vous devrez enregistrer cette politique dans un fichier texte (par exemple `DSPolicy.json`) sur votre poste de travail local car vous devrez l'exécuter à partir de la CLI. Par exemple :

CLI Command

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document  
file://DSPolicy.json
```

PowerShell Command

```
$PolicyDocument = Get-Content .\DSPolicy.json -Raw
```

```
Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument  
$PolicyDocument
```

Étape 3 : créer un abonnement au Directory Service journal

Dans cette étape finale, vous pouvez maintenant passer à l'activation du transfert de journaux en créant l'abonnement aux journaux. Par exemple :

CLI Command

```
aws ds create-log-subscription --directory-id 'd-1111111111' --log-group-name '/aws/  
directoryservice/d-1111111111'
```

PowerShell Command

```
New-DSLogSubscription -DirectoryId 'd-1111111111' -LogGroupName '/aws/  
directoryservice/d-1111111111'
```

Utilisation CloudWatch pour surveiller les performances de vos contrôleurs de domaine Microsoft AD AWS gérés

Directory Service s'intègre CloudWatch à Amazon pour vous fournir des indicateurs de performance importants pour chaque contrôleur de domaine de votre Active Directory. Cela signifie que vous pouvez surveiller les compteurs de performance des contrôleurs de domaine, tels que l'utilisation du processeur et de la mémoire. Vous pouvez également configurer des alarmes et lancer des actions automatisées pour répondre aux périodes de forte utilisation. Par exemple, vous pouvez configurer une alarme pour une utilisation du processeur du contrôleur de domaine supérieure à 70 % et créer une rubrique SNS pour vous avertir lorsque cela se produit. Vous pouvez utiliser cette rubrique SNS pour lancer des automatisations, telles que des AWS Lambda fonctions, afin d'augmenter le nombre de contrôleurs de domaine dans votre Active Directory.

Pour plus d'informations sur la surveillance des contrôleurs de domaine, veuillez consulter [Déterminer quand ajouter des contrôleurs de domaine avec des CloudWatch métriques](#).

Des frais sont associés à Amazon CloudWatch. Pour plus d'informations, consultez la section [CloudWatchfacturation et coûts](#).

 Important

Les indicateurs de performance des contrôleurs de domaine ne CloudWatch sont pas disponibles dans la région de l'Ouest du Canada (Calgary).

Pour l'activer CloudWatch, voir [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#).

Trouver les indicateurs de performance des contrôleurs de domaine dans CloudWatch

Dans la CloudWatch console Amazon, les métriques d'un service donné sont d'abord regroupées en fonction de l'espace de noms du service. Vous pouvez ajouter des filtres métriques subordonnés à cet espace de noms. Utilisez la procédure suivante pour localiser l'espace de noms et la métrique subordonnée appropriés requis pour configurer les métriques du contrôleur de domaine Managed AWS Microsoft AD dans CloudWatch.

Pour trouver les métriques du contrôleur de domaine dans la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Dans la liste des métriques, sélectionnez l'espace de noms Directory Service, puis dans la liste, sélectionnez la métrique AWS Managed Microsoft AD.

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez [Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation](#) dans le blog sur la AWS sécurité.

Déterminer quand ajouter des contrôleurs de domaine avec des CloudWatch métriques

L'équilibrage de charge entre tous vos contrôleurs de domaine est important pour la résilience et les performances de votre Active Directory. Pour vous aider à optimiser les performances de vos contrôleurs de domaine dans AWS Managed Microsoft AD, nous vous recommandons de commencer par surveiller les indicateurs importants CloudWatch afin de constituer une base de référence. Au cours de ce processus, vous analysez votre Active Directory au fil du temps afin d'identifier votre utilisation moyenne et maximale d'Active Directory. Après avoir déterminé votre base

de référence, vous pouvez surveiller régulièrement ces indicateurs afin de déterminer à quel moment ajouter un contrôleur de domaine à votre Active Directory.

Les métriques suivantes sont importantes à surveiller de façon régulière. Pour obtenir la liste complète des métriques de contrôleur de domaine disponibles dans CloudWatch, voir [AWS Compteurs de performance Microsoft AD gérés](#).

- Métriques spécifiques au contrôleur de domaine, telles que :
 - Processeur
 - Mémoire
 - Disque logique
 - Interface réseau
- AWS Mesures spécifiques à l'annuaire Microsoft AD gérées, telles que :
 - Recherches LDAP
 - Liaisons
 - Requêtes DNS
 - Lectures de l'annuaire
 - Écritures de l'annuaire

Pour obtenir des instructions sur la façon de configurer les métriques du contrôleur de domaine à l'aide de la CloudWatch console, consultez [Comment automatiser le dimensionnement de AWS Managed Microsoft AD en fonction des métriques d'utilisation](#) dans le blog sur la AWS sécurité. Pour obtenir des informations générales sur les métriques dans CloudWatch, consultez la section [Utilisation CloudWatch des métriques Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations générales sur la planification des contrôleurs de domaine, veuillez consulter la section [Capacity planning for Active Directory Domain Services](#) (français non garanti) sur le site de Microsoft.

AWS Compteurs de performance Microsoft AD gérés

Le tableau suivant répertorie tous les compteurs de performance disponibles sur Amazon CloudWatch pour suivre les performances des contrôleurs de domaine et des annuaires dans AWS Managed Microsoft AD.

Catégorie de la métrique	Nom de la métrique
Base de données ==> Instances (NTDSA)	Résultats en % du cache de bases de données
	Latence de moyenne de lectures de bases de données I/O
	I/O Database Reads/sec
	Latence de moyenne d'écritures de journaux I/O
	Temps de liaison LDAP
DirectoryServices (MNT)	Opérations de réplication en attente de DRA
	Synchronisations des réplications en attente de DRA
DNS	Requêtes récursives par seconde
	Échec de la requête récursive par seconde
	Requête TCP reçue par seconde
	Total requête reçue par seconde
	Réponse totale envoyée par seconde
	Requête UDP reçue par seconde
LogicalDisk	Avg. Longueur de la file d'attente de disque
	Espace libre en %
Mémoire	% d'octets validés en cours d'utilisation
	Durée de vie moyenne du cache en veille à long terme(s)
Interface réseau	Octets envoyés/s

Catégorie de la métrique	Nom de la métrique
NTDS	Octets reçus/s
	Bande passante actuelle
	Délai d'attente estimé ATQ
	Latence des demandes ATQ
	Lectures de l'annuaire DS par seconde
	Recherches de l'annuaire DS par seconde
	Écritures de l'annuaire DS par seconde
	Sessions client LDAP
	Recherches LDAP par seconde
Processeur	Liaisons réussies LDAP par seconde
Statistiques de sécurité à l'échelle du système	Temps de traitement en %
	Authentifications Kerberos
	Authentifications NTLM

Désactivation du transfert de CloudWatch journaux Amazon pour AWS Managed Microsoft AD

Vous pouvez désactiver le transfert CloudWatch des journaux pour votre AWS compte Microsoft AD géré dans le AWS Management Console. Pour plus d'informations sur le transfert de journaux, consultez [the section called “Utilisation CloudWatch pour surveiller votre annuaire”](#).

1. Dans le panneau de navigation de la [console Directory Service](#), choisissez Annuaire.
2. Choisissez l'ID de répertoire du répertoire Microsoft AD AWS géré que vous souhaitez partager.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :

- Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez désactiver le transfert de journaux, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Multi-Regions replication (Réplication multi-régions), choisissez l'onglet Networking & security (Réseau et sécurité).
4. Dans la section Transfert de journaux, choisissez Désactiver.
 5. Après avoir lu les informations de la boîte de dialogue Désactiver le transfert de journal, choisissez Désactiver.

Surveillance du serveur DNS avec Microsoft Event Viewer

Vous pouvez auditer vos événements DNS Microsoft AD AWS gérés, ce qui facilite l'identification et la résolution des problèmes de DNS. Par exemple, si un enregistrement DNS est manquant, vous pouvez utiliser le journal des événements d'audit DNS pour vous aider à identifier la cause première et résoudre le problème. Vous pouvez également utiliser les journaux des événements d'audit DNS pour améliorer la sécurité en détectant et en bloquant les demandes en provenance d'adresses IP suspectes.

Pour ce faire, vous devez être connecté avec le compte Admin ou avec un compte qui est un membre du groupe AWS Administrateurs des systèmes de noms de domaine . Pour en savoir plus sur ce groupe, veuillez consulter [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Pour accéder à l'Observateur d'événements pour votre DNS Microsoft AD AWS géré

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez Instances.
3. Localisez une EC2 instance Amazon jointe à votre répertoire AWS Managed Microsoft AD. Sélectionnez l'instance, puis choisissez Connecter.
4. Une fois connecté à l' EC2 instance Amazon, ouvrez le menu Démarrer et sélectionnez le dossier Windows Administrative Tools. Dans le dossier Administrative Tools (Outils d'administration), sélectionnez Event Viewer.
5. Dans la fenêtre Observateur d'événements, choisissez Action, puis choisissez Connecter à un autre ordinateur.

6. Sélectionnez Un autre ordinateur, saisissez le nom ou l'adresse IP de l'un de vos serveurs DNS Microsoft AD AWS gérés, puis cliquez sur OK.
7. Dans le volet de gauche, accédez à Journaux d'applications et de services>Microsoft>WindowsServeur DNS, puis sélectionnez Audit.

Accès aux AWS applications et aux services depuis votre Microsoft AD AWS géré

Vous pouvez accorder l'accès à vos utilisateurs Microsoft AD AWS gérés pour accéder aux AWS applications et aux services. Parmi ces AWS applications et services, on peut citer :

- Amazon Chime
- Amazon EC2
- Suite rapide
- AWS Management Console
- Amazon WorkSpaces

Vous pouvez également utiliser l'accès URLs et l'authentification unique avec votre Microsoft AD AWS géré.

Tâches d'accès aux AWS applications et aux services depuis AWS Managed Microsoft AD

- [Compatibilité des applications pour AWS Managed Microsoft AD](#)
- [Permettre l'accès aux AWS applications et aux services pour votre Microsoft AD AWS géré](#)
- [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#)
- [Création d'une URL d'accès pour AWS Managed Microsoft AD](#)
- [Activation de l'authentification unique pour AWS Managed Microsoft AD](#)

Compatibilité des applications pour AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) est compatible avec de nombreux AWS services et applications tierces.

Voici une liste des AWS applications et services compatibles :

- Amazon Chime
- Amazon Connect
- Amazon EC2
- Suite rapide
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- AWS Management Console
- FSx pour le serveur de fichiers Windows
- WorkSpaces

Pour de plus amples informations, veuillez consulter [Permettre l'accès aux AWS applications et aux services pour votre Microsoft AD AWS géré](#).

En raison de l'ampleur des off-the-shelf applications personnalisées et commerciales qui utilisent Active Directory, AWS ne peut pas effectuer de vérification formelle ou étendue de la compatibilité des applications tierces avec AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Bien que AWS nous travaillons avec les clients pour tenter de surmonter les éventuels problèmes d'installation d'applications qu'ils pourraient rencontrer, nous ne sommes pas en mesure de garantir qu'une application est ou continuera d'être compatible avec AWS Managed Microsoft AD.

Les applications tierces suivantes sont compatibles avec AWS Managed Microsoft AD :

- Activation Active Directory (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra (anciennement connu sous le nom de Azure Active Directory (AzureAD))
- Microsoft Entra Connect (anciennement connu sous le nom de Azure Active Directory Connect)

- Réplication de systèmes de fichiers distribués (DFSR)
- Espaces de noms de système de fichiers distribués (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(y compris les groupes de disponibilité Always On de SQL Server)
- Microsoft System Center Configuration Manager(SCCM) - L'utilisateur qui déploie SCCM doit être membre du groupe des administrateurs de gestion du système AWS délégués.
- Microsoft Windows and Windows Server OS
- Office 365

Remarque : il se peut que certaines des configurations de ces applications ne soient pas prises en charge.

Directives de compatibilité

Bien que les applications peuvent parfois avoir des configurations qui ne sont pas compatibles, les configurations de déploiement d'applications sont souvent capables de surmonter une incompatibilité. La section suivante décrit les motifs les plus courants d'incompatibilité d'une application. Les clients peuvent utiliser ces informations pour étudier les caractéristiques de compatibilité d'une application donnée et identifier les éventuelles modifications à apporter à son déploiement.

- Autorisations de l'administrateur du domaine ou autres autorisations privilégiées – Certaines applications requièrent que vous les installiez en tant qu'administrateur du domaine. Étant donné que vous AWS devez conserver le contrôle exclusif de ce niveau d'autorisation afin de fournir Active Directory en tant que service géré, vous ne pouvez pas agir en tant qu'administrateur de domaine pour installer de telles applications. Cependant, vous pouvez souvent installer de telles applications en déléguant des autorisations spécifiques, moins privilégiées et AWS prises en charge à la personne qui effectue l'installation. Contactez votre fournisseur d'applications pour en savoir plus sur les autorisations précises que requiert votre application. Pour plus d'informations sur les autorisations qui vous AWS permettent de déléguer, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré.](#)
- Accès à des conteneurs Active Directory privilégiés : au sein de votre annuaire, AWS Managed Microsoft AD fournit une unité organisationnelle (UO) sur laquelle vous avez un contrôle administratif total. Vous ne possédez pas d'autorisations de création ou d'écriture, mais vous pouvez détenir des autorisations limitées de lecture des conteneurs qui se trouvent à un niveau supérieur dans l'arborescence Active Directory que votre unité d'organisation. Les applications

qui créent ou accèdent à des conteneurs, et pour lesquelles vous n'avez pas d'autorisation, peuvent ne pas fonctionner. Toutefois, ces applications ont souvent la capacité d'utiliser un conteneur que vous créez dans votre unité d'organisation comme alternative. Consultez votre fournisseur d'applications pour trouver des moyens de créer et d'utiliser un conteneur dans votre unité d'organisation comme alternative. Pour plus d'informations sur votre unité d'organisation, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

- Modifications de schéma pendant le processus d'installation – Certaines applications Active Directory nécessitent la modification du schéma Active Directory par défaut, et elles peuvent essayer d'installer ces modifications pendant le processus d'installation de l'application. En raison de la nature privilégiée des extensions de schéma, cela AWS est possible en important des fichiers LDIF (Lightweight Directory Interchange Format) uniquement via la console Directory Service, la CLI ou le SDK. Ces applications sont souvent accompagnées d'un fichier LDIF que vous pouvez appliquer au répertoire par le biais du processus de mise à jour du Directory Service schéma. Pour en savoir plus sur le fonctionnement du processus d'importation LDIF, veuillez consulter la section [Tutoriel : extension de votre schéma Microsoft AD AWS géré](#). Vous pouvez installer l'application de sorte à contourner l'installation du schéma pendant le processus d'installation.

Applications incompatibles connues

La liste suivante répertorie les off-the-shelf applications commerciales fréquemment demandées pour lesquelles nous n'avons pas trouvé de configuration compatible avec AWS Managed Microsoft AD. AWS met à jour cette liste de temps à autre, à sa seule discrétion, par courtoisie afin de vous aider à éviter des efforts improductifs. AWS fournit ces informations sans garantie ni réclamation concernant la compatibilité actuelle ou future.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

Permettre l'accès aux AWS applications et aux services pour votre Microsoft AD AWS géré

Les utilisateurs peuvent autoriser AWS Managed Microsoft AD à donner à AWS des applications et à des services, tels qu'Amazon WorkSpaces, l'accès à votre Active Directory. Les AWS applications et

services suivants peuvent être activés ou désactivés pour fonctionner avec AWS Managed Microsoft AD.

AWS application/service	En savoir plus...
Amazon Chime	Pour plus d'informations, consultez la section Connexion à Active Directory .
Amazon Connect	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Connect .
Amazon EC2	Pour de plus amples informations, veuillez consulter Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré .
Serveur FSx de fichiers Amazon pour Windows	Pour plus d'informations, consultez la section Utilisation FSx d'Amazon avec AWS Directory Service pour Microsoft Active Directory .
Suite rapide	Pour plus d'informations, consultez l' édition Utilisation d'Active Directory avec Quick Suite Enterprise .
Amazon Relational Database Service	Pour plus d'informations, consultez les ressources suivantes : • Utilisation de l'authentification Kerberos pour MySQL • Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle • Utilisation de l'authentification Kerberos avec Amazon RDS for PostgreSQL • Utilisation de AWS Managed Microsoft AD avec Amazon RDS for SQL Server
Amazon WorkDocs	Pour plus d'informations, consultez le document Activer Amazon WorkDocs pour AWS Managed Microsoft AD .

AWS application/service	En savoir plus...
Amazon WorkMail	Pour plus d'informations, consultez la section Création d'une organisation .
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez la section Enregistrer un Directory Service répertoire existant auprès de WorkSpaces Personal.
AWS Client VPN	Pour plus d'informations, consultez l' authentification Active Directory dans Client VPN .
AWS IAM Identity Center	Pour plus d'informations, consultez la section Connect to a Microsoft AD directory .
AWS License Manager	Pour plus d'informations, consultez la section Gérer les abonnements basés sur les utilisateurs dans License Manager .
AWS Management Console	Pour de plus amples informations, veuillez consulter Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées .
AWS Autorité de certification privée	Pour plus d'informations, veuillez consulter AWS CA privée Connector for Active Directory (français non garanti).
AWS Transfer Family	Pour plus d'informations, consultez la section Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP .

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire.

Trouvez des AWS applications et des services

Pour rechercher les AWS applications et les services décrits précédemment dans la Directory Service console, effectuez les opérations suivantes.

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Consultez la liste dans la section Applications et services AWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant Directory Service, consultez [Autorisation pour AWS les applications et les services utilisant Directory Service](#).

Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées

Directory Service vous permet d'accorder aux membres de votre annuaire l'accès au AWS Management Console. Par défaut, les membres de votre répertoire n'ont accès à aucune AWS ressource. Vous attribuez des rôles IAM aux membres de votre annuaire pour leur donner accès aux différents AWS services et ressources. Le rôle IAM définit les services, les ressources et le niveau d'accès des membres de votre annuaire.

Avant que vous puissiez accorder l'accès à la console aux membres de votre annuaire, celui-ci doit disposer d'une URL d'accès. Pour plus d'informations sur la manière d'afficher les détails de l'annuaire et d'obtenir votre URL d'accès, veuillez consulter [Affichage des informations de l'annuaire Microsoft AD AWS géré](#). Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter [Création d'une URL d'accès pour AWS Managed Microsoft AD](#).

Pour plus d'informations sur la façon de créer et d'attribuer des rôles IAM aux membres de votre annuaire, veuillez consulter [Octroi aux utilisateurs et aux groupes de AWS Managed Microsoft AD d'accéder aux AWS ressources avec des rôles IAM](#).

Rubriques

- [Permettre AWS Management Console l'accès](#)
- [Désactivation AWS Management Console de l'accès](#)
- [Configuration de la durée AWS Management Console de la session de connexion](#)

Article AWS de blog sur la sécurité connexe

- [Comment accéder à l' AWS Management Console aide de AWS Managed Microsoft AD et de vos informations d'identification locales](#)

AWS re:Post Article connexe

- [Comment puis-je accorder l'accès au AWS Management Console pour les utilisateurs d'Active Directory locaux ?](#)

 Note

L'accès au AWS Management Console est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Permettre AWS Management Console l'accès

Par défaut, l'accès à la console n'est activé pour aucun annuaire. Pour activer l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour activer l'accès à la console

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez autoriser l'accès à la AWS Management Console, puis cliquez sur l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Dans la section AWS Management Console, choisissez Activer. L'accès à la console est désormais activé pour votre annuaire.

Important

Avant que les utilisateurs puissent se connecter à la console avec votre URL d'accès, vous devez d'abord les ajouter au rôle IAM. Pour des informations générales sur l'attribution d'utilisateurs à des rôles IAM, veuillez consulter [Affectation d'utilisateurs ou de groupes à un rôle IAM existant](#). Une fois les rôles IAM attribués, les utilisateurs peuvent accéder à la console à l'aide de votre URL d'accès. Par exemple, si l'URL d'accès au répertoire est `example-corp.awsapps.com`, l'URL permettant d'accéder à la console est `https://example-corp.awsapps.com/console/`.

Désactivation AWS Management Console de l'accès

Pour désactiver AWS Management Console l'accès des utilisateurs et des groupes de votre annuaire Microsoft AD AWS géré, effectuez les opérations suivantes :

Pour désactiver l'accès à la console

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication multirégionale, sélectionnez la région dans laquelle vous souhaitez désactiver l'accès AWS Management Console, puis choisissez l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Dans la section AWS Management Console, choisissez Désactiver. L'accès à la console est désormais désactivé pour votre annuaire.
5. Si des rôles IAM ont été attribués à des utilisateurs ou à des groupes dans l'annuaire, le bouton Désactiver n'est peut-être pas disponible. Dans ce cas, vous devez supprimer toutes

les affectations de rôles IAM correspondant à l'annuaire avant de continuer, y compris les affectations d'utilisateurs ou de groupes de votre annuaire qui ont été supprimées et qui apparaissent sous le libellé Utilisateur supprimé ou Groupe supprimé.

Une fois que toutes les affectations de rôles IAM ont été supprimées, répétez les étapes ci-dessus.

Configuration de la durée AWS Management Console de la session de connexion

Par défaut, les utilisateurs disposent d'une heure pour utiliser leur session après s'être connectés avec succès AWS Management Console avant d'être déconnectés. Ensuite, les utilisateurs doivent se reconnecter pour démarrer la prochaine session d'une heure avant d'être à nouveau déconnectés. Vous pouvez utiliser la procédure suivante pour modifier la durée jusqu'à 12 heures par session.

Pour définir la durée AWS Management Console de la session de connexion

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez définir la durée de la session de connexion, puis cliquez sur l'onglet Gestion d'applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, sélectionnez l'onglet Gestion d'applications.
4. Sous la section Applications et services AWS, choisissez AWS Management Console.
5. Dans la boîte de dialogue Gérer l'accès aux AWS ressources, choisissez Continuer.
6. Sur la page Affecter des utilisateurs et des groupes à des rôles IAM, sous Définir la durée de la session de connexion, modifiez la valeur numérotée, puis choisissez Enregistrer.

Création d'une URL d'accès pour AWS Managed Microsoft AD

Une URL d'accès est utilisée avec AWS des applications et des services, tels qu'Amazon WorkDocs, pour accéder à une page de connexion associée à votre annuaire. Vous pouvez créer une URL d'accès pour votre annuaire en effectuant les étapes suivantes.

Considérations

- L'URL doit être globalement unique.
- L'URL d'accès ne peut être configurée qu'à partir de la région principale lorsque vous utilisez des annuaires multirégionaux.
- Une fois l'URL d'accès aux applications créée pour cet annuaire, elle ne peut pas être modifiée. Une fois votre URL d'accès créée, personne d'autre que vous ne pourra l'utiliser. Si vous supprimez votre annuaire, l'URL d'accès sera également supprimée et pourra alors être utilisée par un autre compte.

Pour créer une URL d'accès

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaires).
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région principale, puis l'onglet Application management (Gestion des applications). Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Application management (Gestion des applications).
4. Dans la section Application access URL (URL d'accès à l'application), si aucune URL d'accès n'a été attribuée à l'annuaire, le bouton Créer s'affiche. Entrez un alias d'annuaire, puis choisissez Créer. Si l'erreur Entity Already Exists (entité déjà existante) est renvoyée, cela veut dire que l'alias de l'annuaire spécifié a déjà été alloué. Choisissez un autre alias et répétez cette procédure.

Votre URL d'accès est affichée au format *<alias>*.awsapps.com. Par défaut, cette URL vous redirige vers la page de connexion pour WorkDocs.

Activation de l'authentification unique pour AWS Managed Microsoft AD

AWS Directory Service permet à vos utilisateurs d'accéder à l'annuaire à WorkDocs partir d'un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Avant d'activer l'authentification unique, vous devez prendre des mesures supplémentaires pour permettre aux navigateurs Web de vos utilisateurs de prendre en charge l'authentification unique. Les utilisateurs peuvent avoir besoin de modifier les paramètres de leur navigateur Web pour activer l'authentification unique.

 Note

L'authentification unique fonctionne uniquement lorsqu'elle est utilisée sur un ordinateur qui est associé à l'annuaire Directory Service . Elle ne peut pas être utilisée sur les ordinateurs qui ne sont pas joints à l'annuaire.

Si votre annuaire est un annuaire AD Connector et que le compte de service AD Connector ne dispose pas de l'autorisation d'ajouter ou de supprimer son attribut de nom principal de service, vous disposez de deux options pour les étapes 5 et 6 ci-dessous :

1. Vous pouvez continuer et vous serez invité à saisir le nom d'utilisateur et le mot de passe d'un utilisateur d'annuaire qui dispose de cette autorisation pour ajouter ou supprimer l'attribut de nom principal de service sur le compte de service AD Connector. Ces informations d'identification servent uniquement à activer l'authentification unique et ne sont pas stockées par le service. Les autorisations du compte de service AD Connector ne sont pas modifiées.
2. Vous pouvez déléguer des autorisations pour permettre au compte de service AD Connector d'ajouter ou de supprimer l'attribut du nom principal du service sur lui-même. Vous pouvez exécuter les PowerShell commandes ci-dessous à partir d'un ordinateur joint au domaine à l'aide d'un compte autorisé à modifier les autorisations sur le compte de service AD Connector. La commande ci-dessous donnera au compte de service AD Connector la possibilité d'ajouter et de supprimer un attribut de nom principal de service uniquement pour lui-même.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
    $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
    Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
```

```
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
$AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Pour activer ou désactiver l'authentification unique avec WorkDocs

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section URL d'accès à l'application, choisissez Activer pour activer l'authentification unique pour WorkDocs.

Si vous ne voyez pas le bouton Activer, vous devez d'abord créer une URL d'accès pour pouvoir afficher cette option. Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter [Création d'une URL d'accès pour AWS Managed Microsoft AD](#).

5. Dans la boîte de dialogue Activer l'authentification unique pour cet annuaire, choisissez Activer. L'authentification unique est activée pour l'annuaire.
6. Si vous souhaitez désactiver ultérieurement l'authentification unique avec WorkDocs, choisissez Désactiver, puis dans la boîte de dialogue Désactiver l'authentification unique pour ce répertoire, sélectionnez à nouveau Désactiver.

Rubriques

- [Authentification unique pour IE et Chrome](#)
- [Authentification unique pour Firefox](#)

Authentification unique pour IE et Chrome

Pour permettre aux navigateurs Microsoft Internet Explorer (IE) et Google Chrome de prendre en charge l'authentification unique, les tâches suivantes doivent être effectuées sur l'ordinateur client :

- Ajoutez votre URL d'accès (par exemple, [https ://<alias>.awsapps.com](https://<alias>.awsapps.com)) à la liste des sites approuvés pour l'authentification unique.
- Activez le script actif (JavaScript).
- Autorisez l'ouverture de session automatique.
- Activez l'authentification intégrée.

Vous ou vos utilisateurs pouvez effectuer ces tâches manuellement, ou vous pouvez modifier ces paramètres à l'aide des paramètres de politique de groupe.

Rubriques

- [Mise à jour manuelle pour authentification unique sous Windows](#)
- [Mise à jour manuelle pour authentification unique sous OS X](#)
- [Paramètres de stratégie de groupe pour authentification unique](#)

Mise à jour manuelle pour authentification unique sous Windows

Pour activer manuellement l'authentification unique sur un ordinateur Windows, effectuez les étapes suivantes sur l'ordinateur client. Certains de ces paramètres sont peut-être déjà définis correctement.

Pour activer manuellement l'authentification unique pour Internet Explorer et Chrome sous Windows

1. Pour ouvrir la boîte de dialogue Propriétés Internet, sélectionnez le menu Démarrer, tapez Internet Options dans la zone de recherche, puis sélectionnez Options Internet.
2. Ajoutez votre URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
 - a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Sécurité.
 - b. Sélectionnez Intranet local, puis Sites.
 - c. Dans la boîte de dialogue Intranet local, sélectionnez Avancé.
 - d. Ajoutez votre URL d'accès à la liste des sites Web et choisissez Fermer.
 - e. Dans la boîte de dialogue Intranet local, sélectionnez OK.

3. Pour activer les scripts actifs, effectuez les opérations suivantes :
 - a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
 - b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler la page jusqu'à Scripts et sélectionnez Activer sous Scripts actifs.
 - c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
 - a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
 - b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler l'écran jusqu'à Authentification utilisateur et sélectionnez Connexion automatique uniquement dans la zone Intranet sous Connexion.
 - c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
 - d. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :
 - a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Avancé.
 - b. Faites défiler la page jusqu'à Sécurité et sélectionnez Activer l'authentification Windows intégrée.
 - c. Dans la boîte de dialogue Propriétés Internet, choisissez OK.
6. Fermez puis rouvrez votre navigateur pour que ces modifications prennent effet.

Mise à jour manuelle pour authentification unique sous OS X

Pour activer manuellement l'authentification unique pour Chrome sous OS X, effectuez les étapes suivantes sur l'ordinateur client. Vous devez disposer des droits d'administrateur sur votre ordinateur pour effectuer ces opérations.

Pour activer manuellement l'authentification unique pour Chrome sous OS X

1. Ajoutez votre URL d'accès à la [AuthServerAllowlist](#) politique en exécutant la commande suivante :

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```


2. Ouvrez les Préférences système, accédez au panneau Profils et supprimez le profil Chrome Kerberos Configuration.
3. Redémarrez Chrome et ouvrez `chrome://policy` dans Chrome pour vérifier que les nouveaux paramètres sont en place.

Paramètres de stratégie de groupe pour authentification unique

L'administrateur de domaine peut implémenter des paramètres de stratégie de groupe pour apporter les modifications d'authentification unique sur les ordinateurs clients joints au domaine.

Note

Si vous gérez les navigateurs Web Chrome sur les ordinateurs de votre domaine à l'aide des politiques Chrome, vous devez y ajouter votre URL d'[AuthServerAllowlist](#) accès. Pour plus d'informations sur la définition des politiques de Chrome, veuillez consulter la section [Policy Settings in Chrome](#) (français non garanti).

Pour activer l'authentification unique pour Internet Explorer et Chrome à l'aide des paramètres de stratégie de groupe

1. Créez un nouvel objet de stratégie de groupe en procédant comme suit :
 - a. Ouvrez l'outil de gestion des stratégies de groupe, accédez à votre domaine et sélectionnez Objets de stratégie de groupe.
 - b. Dans le menu principal, choisissez Action, puis Nouveau.
 - c. Dans la boîte de dialogue New GPO, entrez un nom descriptif pour l'objet de stratégie de groupe, tel que IAM Identity Center Policy et laissez Source Starter GPO défini sur (none). Cliquez sur OK.
2. Ajoutez l'URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.

- c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.
- d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

Action

Update

Hive

HKEY_CURRENT_USER

Chemin

Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com*<alias>*

La valeur de *<alias>* est dérivée de votre URL d'accès. Si votre URL d'accès est `https://examplecorp.awsapps.com`, l'alias est `examplecorp` et la clé de registre sera `Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\examplecorp`.

Nom de la valeur

https

Type de la valeur

REG_DWORD

Données de valeur

1

3. Pour activer les scripts actifs, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.

- c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Autoriser les scripts actifs et choisissez Modifier.
 - d. Dans la boîte de dialogue Autoriser les scripts actifs, entrez les paramètres suivants et cliquez sur OK :
 - Sélectionnez le bouton radio Activé.
 - Sous Options, définissez Autoriser les scripts actifs sur Activer.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique SSO (authentification unique), puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.
 - c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Options de connexion et choisissez Modifier.
 - d. Dans la boîte de dialogue Options de connexion, entrez les paramètres suivants et cliquez sur OK :
 - Sélectionnez le bouton radio Activé.
 - Sous Options, définissez les options de connexion sur Connexion automatique uniquement dans la zone Intranet.
5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.
 - c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.
 - d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

Action

Update

Hive

HKEY_CURRENT_USER

Chemin

Software\Microsoft\Windows\CurrentVersion\Internet Settings

Nom de la valeur

EnableNegotiate

Type de la valeur

REG_DWORD

Données de valeur

1

6. Fermez la fenêtre de l'éditeur de gestion des politiques de groupe si elle est toujours ouverte.
7. Attribuez la nouvelle politique à votre domaine en procédant comme suit :
 - a. Dans l'arborescence Gestion des politiques de groupe, ouvrez le menu contextuel (clic droit) de votre domaine et choisissez Lier un GPO existant.
 - b. Dans la liste Objets de politique de groupe, sélectionnez votre politique IAM Identity Center et cliquez sur OK.

Ces modifications prendront effet après la prochaine mise à jour de la politique de groupe sur le client, ou la prochaine fois que l'utilisateur se connectera.

Authentification unique pour Firefox

Pour autoriser le navigateur Mozilla Firefox à prendre en charge l'authentification unique, ajoutez votre URL d'accès (par exemple, `https ://<alias>.awsapps.com`) à la liste des sites approuvés pour l'authentification unique. Cela peut être fait manuellement ou automatiquement à l'aide d'un script.

Rubriques

- [Mise à jour manuelle pour authentification unique](#)

- [Mise à jour automatique pour authentification unique](#)

Mise à jour manuelle pour authentification unique

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox, effectuez les étapes suivantes sur l'ordinateur client.

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox

1. Ouvrez Firefox et ouvrez la page `about:config`.
2. Ouvrez la préférence `network.negotiate-auth.trusted-uris` et ajoutez votre URL d'accès à la liste des sites. Utilisez une virgule (,) pour séparer plusieurs entrées.

Mise à jour automatique pour authentification unique

En tant qu'administrateur de domaine, vous pouvez utiliser un script pour ajouter votre URL d'accès aux préférences utilisateur de Firefox `network.negotiate-auth.trusted-uris` sur tous les ordinateurs de votre réseau. Pour plus d'informations, rendez-vous sur <https://support.mozilla.org/en-US/questions/939037>.

Octroi aux utilisateurs et aux groupes de AWS Managed Microsoft AD d'accéder aux AWS ressources avec des rôles IAM

AWS Directory Service permet à vos utilisateurs et groupes Microsoft AD AWS gérés d'accéder à des AWS services et à des ressources, tels que l'accès à la EC2 console Amazon. Tout comme si vous accordiez aux utilisateurs IAM l'accès à la gestion des annuaires comme décrit dans [Politiques basées sur une identité \(politiques IAM\)](#), pour que les utilisateurs de votre annuaire aient accès à d'autres AWS ressources, telles qu'Amazon, EC2 vous devez attribuer des rôles et des politiques IAM à ces utilisateurs et groupes. Pour plus d'informations, consultez [Rôles IAM](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la manière d'autoriser les utilisateurs à accéder au AWS Management Console, consultez [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#).

Rubriques

- [Création d'un nouveau rôle IAM](#)

- [Modification de la relation de confiance pour un rôle IAM existant](#)
- [Affectation d'utilisateurs ou de groupes à un rôle IAM existant](#)
- [Affichage des utilisateurs et groupes attribués à un rôle](#)
- [Supprimer un utilisateur ou un groupe d'un rôle IAM](#)
- [Utilisation de politiques AWS gérées avec Directory Service](#)

Création d'un nouveau rôle IAM

Si vous devez créer un nouveau rôle IAM à utiliser avec Directory Service, vous devez le créer à l'aide de la console IAM. Une fois le rôle créé, vous devez établir une relation de confiance avec ce rôle avant de pouvoir le voir dans la Directory Service console. Pour de plus amples informations, veuillez consulter [Modification de la relation de confiance pour un rôle IAM existant](#).

Note

L'utilisateur exécutant cette tâche doit avoir l'autorisation d'effectuer les opérations IAM suivantes. Pour de plus amples informations, veuillez consulter [Politiques basées sur une identité \(politiques IAM\)](#).

- iam : PassRole
- iam : GetRole
- iam : CreateRole
- iam : PutRolePolicy

Pour créer un nouveau rôle dans la console IAM

1. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles). Pour plus d'informations, veuillez consulter [Creating a role \(AWS Management Console\)](#) (français non garanti) dans le Guide de l'utilisateur IAM.
2. Choisissez Créer un rôle.
3. Dans Choisir le service qui utilisera ce rôle, choisissez Directory Service, puis Suivant : Autorisations.
4. Cochez la case à côté de la politique (par exemple, Amazon EC2 FullAccess) que vous souhaitez appliquer aux utilisateurs de votre annuaire, puis choisissez Next.

5. Si nécessaire, ajoutez une balise au rôle, puis choisissez Suivant.
6. Fournissez le Nom du rôle et une Description (facultative), puis choisissez Créer un rôle.

Exemple : Création d'un rôle pour activer l'accès à AWS Management Console

La liste de contrôle suivante fournit un exemple des tâches que vous devez effectuer pour créer un nouveau rôle IAM qui permettra à des utilisateurs spécifiques de AWS Managed Microsoft AD d'accéder à la console Amazon EC2.

1. Créez un rôle avec la console IAM à l'aide de la procédure ci-dessus. Lorsque vous êtes invité à saisir une politique, choisissez Amazon EC2 FullAccess.
2. Suivez les étapes décrites dans [Modification de la relation de confiance pour un rôle IAM existant](#) pour modifier le rôle que vous venez de créer, puis ajoutez les informations de relation d'approbation requises au document de stratégie. Cette étape est nécessaire pour que le rôle soit visible immédiatement après avoir activé l'accès AWS Management Console à l'étape suivante.
3. Suivez les étapes de [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#) pour configurer l'accès général à AWS Management Console.
4. Suivez les étapes ci-dessous [Affectation d'utilisateurs ou de groupes à un rôle IAM existant](#) pour ajouter au nouveau rôle les utilisateurs qui ont besoin d'un accès complet aux EC2 ressources.

Modification de la relation de confiance pour un rôle IAM existant

Vous pouvez attribuer vos rôles IAM existants à vos Directory Service utilisateurs et à vos groupes. Pour ce faire, le rôle doit toutefois entretenir une relation de confiance avec Directory Service. Lorsque vous créez un rôle Directory Service à l'aide de la procédure dans [Création d'un nouveau rôle IAM](#), cette relation de confiance est automatiquement définie.

Note

Vous n'avez qu'à établir cette relation d'approbation pour les rôles IAM qui ne sont pas créés par Directory Service.

Pour établir une relation de confiance pour un rôle IAM existant pour Directory Service

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation de la console IAM, sous Gestion des accès, choisissez Rôles.

La console affiche les rôles de votre compte.

3. Choisissez le nom du rôle que vous voulez modifier, puis, une fois dans la page du rôle, sélectionnez Relations d'approbation.
4. Choisissez Edit trust policy (Modifier la politique d'approbation).
5. Sous Modifier la politique d'approbation, collez les informations suivantes, puis choisissez Mettre à jour la stratégie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Vous pouvez également mettre à jour ce document de stratégie à l'aide de AWS CLI. Pour plus d'informations, veuillez consulter [update-trust](#) dans AWS CLI Command Reference (français non garanti).

Affectation d'utilisateurs ou de groupes à un rôle IAM existant

Vous pouvez attribuer un rôle IAM existant à un utilisateur ou à un groupe Microsoft AD AWS géré. Pour ce faire, assurez-vous d'avoir effectué les étapes suivantes.

Prérequis

- [Créez un Microsoft AD AWS géré.](#)
- [Créez un utilisateur IAM](#) ou [un groupe IAM](#).
- [Créez un rôle](#) qui entretient une relation de confiance avec Directory Service. Pour les rôles IAM existants, vous devez [modifier la relation de confiance associée à un rôle existant](#).

Important

L'accès des utilisateurs de AWS Managed Microsoft AD dans les groupes imbriqués de votre annuaire n'est pas pris en charge. Les membres du groupe parent ont accès à la console, mais pas les membres des groupes enfants.

Pour attribuer des utilisateurs ou des groupes Microsoft AD AWS gérés à un rôle IAM existant

1. Dans le volet de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaires.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - a. Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
 - b. Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez effectuer vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
4. Faites défiler la page jusqu'à la AWS Management Console section, sélectionnez Actions et Activer.
5. Dans la section Accès à la console déléguée, choisissez le nom du rôle IAM existant auquel vous souhaitez attribuer des utilisateurs.
6. Sur la page Selected rôle (Rôle sélectionné) sous Manage users and groups for this role (Gérer les utilisateurs et les groupes pour ce rôle), choisissez Add (Ajouter).
7. Sur la page Add users and groups to the role (Ajouter des utilisateurs et groupes aux rôles), en regard de Select Active Directory Forest (Sélectionner la forêt Active Directory), choisissez

la forêt AWS Managed Microsoft AD (cette forêt) ou la forêt sur site (forêt approuvée), selon celle qui contient les comptes qui ont besoin d'accéder à AWS Management Console. Pour plus d'informations sur la mise en place d'une forêt approuvée, veuillez consulter [Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory](#).

8. Sous Specify which users or groups to add (Spécifier les utilisateurs ou les groupes à ajouter), sélectionnez Find by user (Rechercher par utilisateur) ou Find by group (Rechercher par groupe), puis tapez le nom de l'utilisateur ou du groupe. Dans la liste de correspondances possibles, choisissez l'utilisateur ou le groupe que vous souhaitez ajouter.
9. Choisissez Add (Ajouter) pour mettre fin à l'affectation des utilisateurs et des groupes au rôle.

Affichage des utilisateurs et groupes attribués à un rôle

Pour afficher les utilisateurs et les groupes Microsoft AD AWS gérés affectés à un rôle IAM, effectuez les étapes suivantes.

Prérequis

- [Créez un Microsoft AD AWS géré](#).
- [Créez un utilisateur IAM](#) ou [un groupe IAM](#).
- [Créez un rôle](#) qui entretient une relation de confiance avec Directory Service. Pour les rôles IAM existants, vous devez [modifier la relation de confiance associée à un rôle existant](#).
- [Assignez vos utilisateurs ou groupes à un rôle IAM existant](#).

Pour afficher les utilisateurs AWS gérés de Microsoft AD et les groupes assignés à un rôle IAM

1. Dans le volet de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaires.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - a. Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez afficher vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- b. Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
4. Faites défiler la page jusqu'à la AWS Management Console section. Le statut doit être activé. Dans le cas contraire, sélectionnez Actions et Activer. Pour de plus amples informations, veuillez consulter [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#).

 Note

Vous ne verrez aucun groupe ou utilisateur s'il AWS Management Console est désactivé.

5. Dans la section Accès à la console déléguée, sélectionnez le lien hypertexte du rôle IAM que vous souhaitez afficher. Vous pouvez également sélectionner Afficher la politique dans IAM pour afficher la politique IAM dans la console IAM.
6. Sur la page Rôle sélectionné, sous la section Gérer les utilisateurs et les groupes pour ce rôle, vous pouvez afficher les utilisateurs et les groupes affectés au rôle IAM.

Supprimer un utilisateur ou un groupe d'un rôle IAM

Pour supprimer un utilisateur ou un groupe Microsoft AD AWS géré d'un rôle IAM, effectuez les étapes suivantes.

Pour supprimer un utilisateur ou un groupe d'un rôle IAM

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, exécutez l'une des opérations suivantes :
 - a. Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez supprimer vos affectations, puis cliquez sur l'onglet Gestion des applications. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - b. Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Gestion des applications.
4. Dans la AWS Management Console section, choisissez le rôle IAM dont vous souhaitez supprimer des utilisateurs et des groupes.

5. Sur la page Selected role (Rôle sélectionné), sous Manage users and groups for this role (Gérer les utilisateurs et les groupes pour ce rôle), sélectionnez les utilisateurs ou les groupes pour lesquels supprimer le rôle, puis choisissez Remove (Supprimer). Le rôle est supprimé pour les utilisateurs et les groupes spécifiés, mais il n'est pas supprimé de votre compte.

 Note

Si vous souhaitez supprimer un rôle, consultez [Supprimer des rôles ou des profils d'instance](#).

Utilisation de politiques AWS gérées avec Directory Service

Directory Service fournit les politiques AWS gérées suivantes pour permettre à vos utilisateurs et à vos groupes d'accéder aux AWS services et aux ressources, tels que l'accès à la EC2 console Amazon. Vous devez vous connecter à AWS Management Console avant de pouvoir afficher ces stratégies.

- [Accès en lecture seule](#)
- [Accès utilisateur avec pouvoir](#)
- [Directory Service accès complet](#)
- [Directory Service accès en lecture seule](#)
- [AWS Accès complet aux données du service de répertoire](#)
- [AWS Accès en lecture seule aux données du Directory Service](#)
- [Accès complet à Amazon Cloud Directory](#)
- [Accès en lecture seule à Amazon Cloud Directory](#)
- [Accès EC2 complet à Amazon](#)
- [Accès en EC2 lecture seule à Amazon](#)
- [Accès complet à Amazon VPC](#)
- [Accès en lecture seule à Amazon VPC](#)
- [Accès complet à Amazon RDS](#)
- [Accès en lecture seule à Amazon RDS](#)
- [Accès complet à Amazon DynamoDB](#)
- [Accès en lecture seule à Amazon DynamoDB](#)

- [Accès complet à Amazon S3](#)
- [Accès en lecture seule à Amazon S3](#)
- [AWS CloudTrail accès complet](#)
- [AWS CloudTrail accès en lecture seule](#)
- [Accès CloudWatch complet à Amazon](#)
- [Accès en CloudWatch lecture seule à Amazon](#)
- [Accès complet à Amazon CloudWatch Logs](#)
- [Accès en lecture seule à Amazon CloudWatch Logs](#)

Pour plus d'informations sur la création de vos propres politiques, consultez la section [Exemples de politiques pour l'administration AWS des ressources](#) dans le Guide de l'utilisateur IAM.

Configuration de la réplication multirégionale pour AWS Managed Microsoft AD

La réplication multirégionale peut être utilisée pour répliquer automatiquement les données de votre annuaire AWS Microsoft AD géré sur plusieurs régions AWS. Cette réplication peut améliorer les performances des utilisateurs et des applications dans des zones géographiques dispersées. AWS Managed Microsoft AD utilise la réplication native d'Active Directory pour répliquer les données de votre annuaire en toute sécurité dans la nouvelle région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Vous pouvez utiliser la réplication multirégionale automatisée dans la plupart des régions où AWS Managed Microsoft AD est disponible.

Important

La réplication multirégionale n'est pas disponible dans les régions optionnelles. Les régions suivantes sont facultatives :

- Afrique (Le Cap) af-south-1
- Asie-Pacifique (Hong Kong) ap-east-1
- Asie-Pacifique (Hyderabad) ap-south-2
- Asie-Pacifique (Jakarta) ap-southeast-3

- Asie-Pacifique (Melbourne) ap-southeast-4
- Asie-Pacifique (Thaïlande) ap-southeast-7
- Canada Ouest (Calgary) ca-west-1
- Europe (Milan) eu-south-1
- Europe (Espagne) eu-south-2
- Europe (Zurich) eu-central-2
- Israël (Tel Aviv) il-central-1
- Moyen-Orient (Bahreïn) me-south-1
- Moyen-Orient (Émirats arabes unis) me-central-1
- Mexique (Centre) mx-central-1

Pour plus d'informations sur les régions d'adhésion et comment les activer, veuillez consulter la section [Specify which Régions AWS your account can use](#) (français non garanti) dans le Guide Gestion de compte AWS .

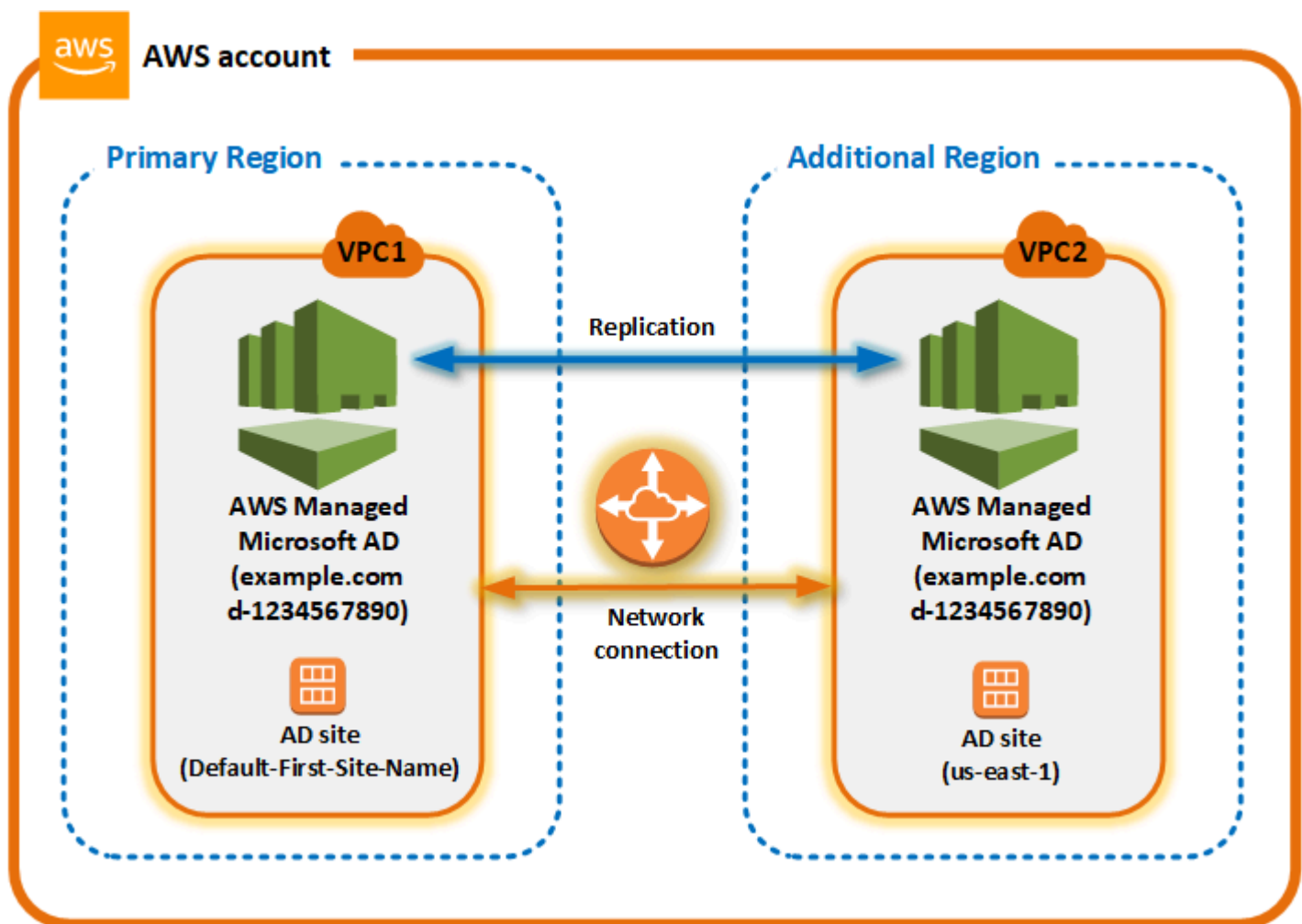
Comment fonctionne la réplication multirégionale

Grâce à la fonctionnalité de réplication multirégionale, AWS Managed Microsoft AD élimine le fardeau indifférencié lié à la gestion d'une infrastructure Active Directory mondiale. Une fois configuré, il AWS réplique toutes les données de l'annuaire des clients, y compris les utilisateurs, les groupes, les politiques de groupe et le schéma sur plusieurs Régions AWS sites.

Une fois qu'une nouvelle région a été ajoutée, les opérations suivantes se produisent automatiquement, comme indiqué dans l'illustration :

- AWS Managed Microsoft AD crée deux contrôleurs de domaine dans le VPC sélectionné et les déploie dans la nouvelle région avec le même compte. AWS L'identifiant de votre annuaire (`directory_id`) reste le même dans toutes les régions. Vous pouvez ajouter d'autres contrôleurs de domaine ultérieurement si vous le souhaitez.
- AWS Managed Microsoft AD configure la connexion réseau entre la région principale et la nouvelle région.
- AWS Managed Microsoft AD crée un nouveau site Active Directory et lui donne le même nom que la région, tel que us-east-1. Vous pouvez également le renommer ultérieurement à l'aide de l'outil Active Directory Sites and Services.

- AWS Managed Microsoft AD réplique tous les objets et configurations Active Directory dans la nouvelle région, y compris les utilisateurs, les groupes, les politiques de groupe, les approbations Active Directory, les unités organisationnelles et le schéma Active Directory. Les liens de sites Active Directory sont configurés pour utiliser [Change Notification](#) (Notification de modification). Lorsque la notification des modifications entre sites est activée, les modifications sont propagées vers le site distant à la même fréquence qu'au sein du site source, y compris les modifications qui nécessitent une réplication urgente.
- S'il s'agit de la première région que vous ajoutez, AWS Managed Microsoft AD rend toutes les fonctionnalités compatibles avec plusieurs régions. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).



Sites Active Directory

La réplication multirégionale prend en charge plusieurs sites Active Directory (un site Active Directory par région). Lorsqu'une nouvelle région est ajoutée, elle reçoit le même nom que la région, par exemple, us-east-1. Vous pouvez également le renommer ultérieurement à l'aide de Active Directory Sites and Services.

AWS services

AWS des services tels qu'Amazon RDS for SQL Server et FSx Amazon se connectent aux instances locales de l'annuaire global. Cela permet à vos utilisateurs de se connecter une seule fois aux applications compatibles avec Active Directory qui s'exécutent, AWS ainsi qu'à des AWS services tels qu'Amazon RDS for SQL Server dans n'importe quelle région. AWS Pour ce faire, les utilisateurs ont besoin d'informations d'identification provenant de AWS Managed Microsoft AD ou d'Active Directory local lorsque vous avez confiance en votre AWS Managed Microsoft AD.

Vous pouvez utiliser les AWS services suivants avec la fonctionnalité de réplication multirégionale.

- Amazon EC2
- Serveur FSx de fichiers Amazon pour Windows
- Amazon Relational Database Service pour SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

Basculement

Si tous les contrôleurs de domaine d'une région sont en panne, AWS Managed Microsoft AD récupère les contrôleurs de domaine et réplique automatiquement les données de l'annuaire. Pendant ce temps, les contrôleurs de domaine des autres régions restent opérationnels.

Avantages de la réplication multirégionale

Avec la réplication multirégionale dans AWS Managed Microsoft AD, les applications compatibles avec Active Directory utilisent l'annuaire localement pour des performances élevées et la fonctionnalité multirégion pour la résilience. Vous pouvez utiliser la réplication multirégionale avec des applications compatibles avec Active Directory telles que SharePoint SQL Server Always On, ainsi que des AWS services tels qu'Amazon RDS for SQL Server et FSx pour Windows File Server. Voici d'autres avantages de la réplication multi-régions.

- Il vous permet de déployer rapidement une seule instance Microsoft AD AWS gérée dans le monde entier et élimine le lourd fardeau lié à l'autogestion d'une infrastructure Active Directory mondiale.
- Il vous permet de déployer et de gérer les charges de travail Windows et Linux plus facilement et à moindre coût dans plusieurs AWS régions. La réplication multirégionale automatisée permet d'optimiser les performances de vos applications globales compatibles avec Active Directory. Toutes les applications déployées dans des instances Windows ou Linux utilisent Microsoft AD AWS géré localement dans la région, ce qui permet de répondre aux demandes des utilisateurs depuis la région la plus proche possible.
- Elle assure la résilience multi-régions. Déployé dans l'infrastructure AWS gérée à haute disponibilité, AWS Managed Microsoft AD gère les mises à jour logicielles automatisées, la surveillance, la restauration et la sécurité de l'infrastructure Active Directory sous-jacente dans toutes les régions. Cela vous permet de vous concentrer sur le développement de vos applications.

Rubriques

- [Caractéristiques mondiales et régionales](#)
- [Régions principales et régions supplémentaires](#)
- [Ajouter une région répliquée pour AWS Managed Microsoft AD](#)
- [Suppression d'une région répliquée pour AWS Managed Microsoft AD](#)

Caractéristiques mondiales et régionales

Lorsque vous ajoutez une AWS région à votre répertoire à l'aide de la réplication multirégionale, cela Directory Service améliore la portée de toutes les fonctionnalités afin qu'elles prennent en compte les régions. Ces fonctionnalités sont répertoriées dans différents onglets de la page de détails qui apparaît lorsque vous choisissez l'ID de l'annuaire dans la console Directory Service . Cela signifie que toutes les fonctionnalités sont activées, configurées ou gérées en fonction de la région que vous

sélectionnez dans la section Réplication multi-régions de la console. Les modifications que vous apportez aux fonctionnalités de chaque région sont appliquées à l'échelle mondiale ou par région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Fonctionnalités mondiales

Toutes les modifications que vous apportez aux fonctionnalités mondiales alors que la [Région principale](#) est sélectionnée seront appliquées à toutes les régions.

Vous pouvez identifier les fonctionnalités utilisées à l'échelle mondiale sur la page Directory details (Détails de l'annuaire), car la mention Applied to all replicated Regions (Appliquée à toutes les régions répliquées) s'affiche à côté. Sinon, si vous avez sélectionné une autre région dans la liste qui n'est pas la région principale, vous pouvez identifier les fonctionnalités utilisées à l'échelle mondiale, car elles affichent la mention Inherited from primary Region (Hérité de la région principale).

Caractéristiques régionales

Toutes les modifications que vous apportez à une fonctionnalité dans une [Région supplémentaire](#) seront appliquées uniquement à cette région.

Vous pouvez identifier les fonctionnalités qui sont régionales sur la page Directory details (Détails de l'annuaire), car les mentions Applied to all replicated Regions (Appliquée à toutes les régions répliquées) ou Inherited from primary Region (Hérité de la région principale) ne s'affichent pas à côté.

Régions principales et régions supplémentaires

Avec la réplication multirégionale, AWS Managed Microsoft AD utilise les deux types de régions suivants pour différencier la manière dont les fonctionnalités globales ou régionales doivent être appliquées dans votre annuaire.

Région principale

La région initiale dans laquelle vous avez créé votre annuaire pour la première fois est appelée région principale. Vous ne pouvez effectuer que des opérations mondiales au niveau de l'annuaire, telles que la création d'approbations Active Directory et la mise à jour du schéma AD à partir de la région principale.

La région principale peut toujours être identifiée comme étant la première région, car elle figure en haut de la liste dans la section Multi-Region replication (Réplication multi-régions) et se termine par - Primary (Principale). Par exemple, USA Est (Virginie du Nord) - Principale.

Toutes les modifications que vous apportez aux [Fonctionnalités mondiales](#) alors que la région principale est sélectionnée seront appliquées à toutes les régions.

Vous ne pouvez ajouter des régions que lorsque la région principale est sélectionnée. Pour de plus amples informations, veuillez consulter [Ajouter une région répliquée pour AWS Managed Microsoft AD](#).

Région supplémentaire

Toutes les régions que vous avez ajoutées à votre annuaire sont appelées régions supplémentaires.

Bien que certaines fonctionnalités puissent être gérées à l'échelle mondiale pour toutes les régions, d'autres sont gérées individuellement par région. Pour gérer une fonctionnalité pour une région supplémentaire (région non principale), vous devez d'abord sélectionner la région supplémentaire dans la liste de la section Multi-Region replication (Réplication multi-régions) de la page Directory details (Détails de l'annuaire). Vous pouvez ensuite procéder à la gestion de la fonctionnalité.

Toutes les modifications que vous apportez aux [Caractéristiques régionales](#) alors qu'une région supplémentaire est sélectionnée ne seront appliquées qu'à cette région.

Ajouter une région répliquée pour AWS Managed Microsoft AD

Lorsque vous ajoutez une région à l'aide de [Configuration de la réplication multirégionale pour AWS Managed Microsoft AD](#) cette fonctionnalité, AWS Managed Microsoft AD crée deux contrôleurs de domaine dans la AWS région sélectionnée, Amazon Virtual Private Cloud (VPC) et le sous-réseau. AWS Managed Microsoft AD crée également les groupes de sécurité associés qui permettent aux charges de travail Windows de se connecter à votre annuaire dans la nouvelle région. Il crée également ces ressources en utilisant le même compte AWS sur lequel votre annuaire est déjà déployé. Pour ce faire, choisissez la région, spécifiez le VPC et fournissez les configurations pour la nouvelle région.

La réplication multirégionale n'est prise en charge que pour l'édition Enterprise de AWS Managed Microsoft AD.

Prérequis

Avant de poursuivre les étapes d'ajout d'une nouvelle région de réplication, nous vous recommandons de consulter d'abord les tâches préalables suivantes.

- Vérifiez que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires, de la configuration Amazon VPC et de la configuration du sous-réseau dans la nouvelle région vers laquelle vous souhaitez répliquer le répertoire.
- Si vous souhaitez utiliser vos informations d'identification Active Directory locales existantes pour accéder aux charges de travail compatibles avec Active Directory et les gérer dans AWS, vous devez créer une relation de confiance Active Directory entre Managed AWS Microsoft AD et votre infrastructure AD locale. Pour plus d'informations sur les approbations, veuillez consulter [Connect AWS Managed Microsoft AD à votre infrastructure Active Directory existante](#).
- Si vous avez déjà établi une relation de confiance entre votre instance Active Directory locale et que vous souhaitez ajouter une région répliquée, vous devez vérifier que vous disposez de la configuration du VPC Amazon et du sous-réseau nécessaires dans la nouvelle région vers laquelle vous souhaitez répliquer l'annuaire.

Vous pouvez également créer une relation de confiance entre votre infrastructure Microsoft AD AWS gérée et votre infrastructure AD sur site, afin de pouvoir utiliser les informations d'identification Active Directory locales existantes pour gérer les charges de travail compatibles avec la publicité. Pour de plus amples informations, veuillez consulter [Connect AWS Managed Microsoft AD à votre infrastructure Active Directory existante](#).

Ajouter une région

Utilisez la procédure suivante pour ajouter une région répliquée à votre répertoire Microsoft AD AWS géré.

Pour ajouter une région répliquée

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sous Multi-Region replication (Réplication multi-régions), choisissez la région principale dans la liste, puis choisissez Add Region (Ajouter une région).

 Note

Vous ne pouvez ajouter des régions que lorsque la région principale est sélectionnée. Pour de plus amples informations, veuillez consulter [Région principale](#).

4. Sur la page Add Region (Ajouter une région), sous Region, choisissez la région que vous souhaitez ajouter dans la liste.
5. Sous VPC, sélectionnez le VPC à utiliser pour cette région.

 Note

Ce VPC ne doit pas avoir de routage inter-domaines sans classe (CIDR) qui est identique à celui d'un VPC utilisé par cet annuaire dans une autre région.

6. Sous Subnets (Sous-réseaux), sélectionnez le sous-réseau à utiliser pour cette région.
7. Passez en revue les informations sous Pricing (Tarification), puis choisissez Add (Ajouter).
8. Lorsque AWS Managed Microsoft AD termine le processus de déploiement du contrôleur de domaine, la région affiche le statut Actif. Vous pouvez désormais apporter des mises à jour à cette région selon vos besoins.

Étapes suivantes

Une fois que vous avez ajouté votre nouvelle région, vous devez envisager les étapes suivantes :

- Déployez des contrôleurs de domaine supplémentaires (jusqu'à 20) dans votre nouvelle région selon vos besoins. Le nombre de contrôleurs de domaine lorsque vous ajoutez une nouvelle région est de 2 par défaut, qui est le minimum requis pour des raisons de tolérance aux pannes et de haute disponibilité. Pour de plus amples informations, veuillez consulter [Ajouter ou supprimer des contrôleurs de domaine supplémentaires à l'aide du AWS Management Console](#).

 Note

Lorsque vous ajoutez un répliqué Région AWS à votre Microsoft AD AWS géré, deux contrôleurs de domaine sont créés par défaut, ce qui correspond au nombre minimum de contrôleurs de domaine requis pour garantir la tolérance aux pannes et la haute disponibilité.

- Partagez votre annuaire avec un plus grand nombre de AWS comptes par région. Les configurations de partage d'annuaires ne sont pas répliquées automatiquement depuis la région principale. Pour de plus amples informations, veuillez consulter [Partagez votre Microsoft AD AWS géré](#).

 Note

Les configurations de partage d'annuaires ne sont pas automatiquement répliquées dans le répertoire principal Région AWS.

- Activez le transfert de journaux pour récupérer les journaux de sécurité de votre annuaire à l'aide d'Amazon CloudWatch Logs depuis la nouvelle région. Lorsque vous activez le transfert de journaux, vous devez fournir un nom de groupe de journaux dans chaque région dans laquelle vous avez répliqué votre annuaire. Pour de plus amples informations, veuillez consulter [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#).

 Note

Lorsque vous activez le transfert de journaux, vous devez fournir un nom pour le groupe de journaux dans chaque Région AWS endroit où vous avez répliqué votre répertoire.

- Activez Amazon Simple Notification Service (Amazon SNS) pour la nouvelle région afin de suivre l'état d'intégrité de votre annuaire par région. Pour de plus amples informations, veuillez consulter [Activation des notifications d'état de l'annuaire Microsoft AD AWS géré avec Amazon Simple Notification Service](#).

Suppression d'une région répliquée pour AWS Managed Microsoft AD

Utilisez la procédure suivante pour supprimer une région pour votre répertoire Microsoft AD AWS géré. Avant de supprimer une région, assurez-vous qu'elle ne possède aucun des éléments suivants :

- Applications autorisées qui y sont associées.
- Annuaires partagés qui lui sont associés.

Pour supprimer une région répliquée

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Dans la barre de navigation, sélectionnez le sélecteur Regions (Régions), puis sélectionnez la région où votre annuaire est stocké.
3. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
4. Sur la page Directory details (Détails de l'annuaire), sous Multi-Region replication (Réplication multi-régions), choisissez Delete Region (Supprimer la région).
5. Dans la boîte de dialogue Delete Region (Supprimer la région), passez en revue les informations, puis saisissez le nom de la région pour confirmer. Ensuite, choisissez Supprimer.

Note

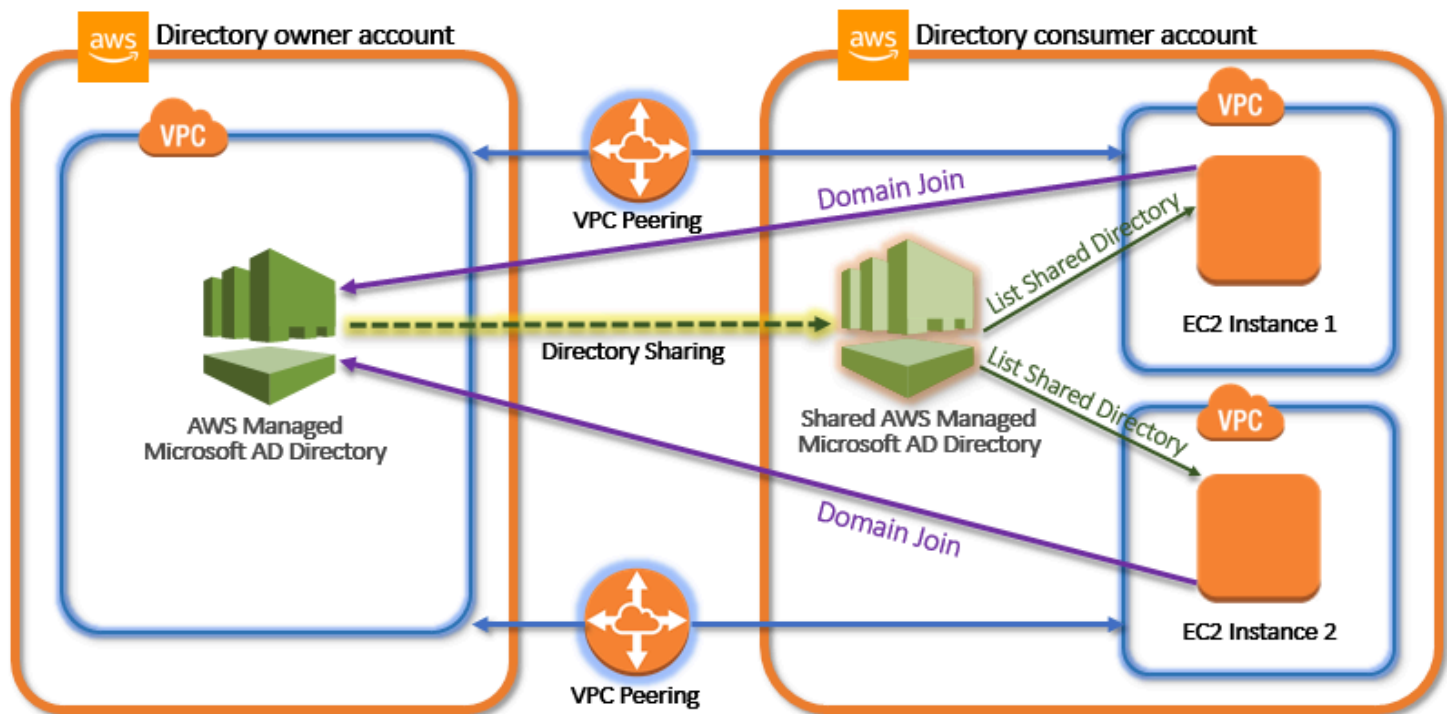
Vous ne pouvez pas mettre à jour la région pendant sa suppression.

Partagez votre Microsoft AD AWS géré

AWS Managed Microsoft AD s'intègre étroitement AWS Organizations pour permettre un partage fluide d'annuaires entre plusieurs Comptes AWS. Vous pouvez partager un seul annuaire avec d'autres personnes de confiance Comptes AWS au sein de la même organisation ou partager le répertoire avec d'autres Comptes AWS personnes extérieures à votre organisation. Vous pouvez également partager votre annuaire lorsque vous Compte AWS n'êtes pas actuellement membre d'une organisation.

Concepts clés du partage d'annuaire

Vous tirerez le meilleur parti de la fonctionnalité de partage d'annuaires si vous vous familiarisez avec les concepts clés suivants.



Compte propriétaire de l'annuaire

Un propriétaire de répertoire est le Compte AWS titulaire du répertoire d'origine dans la relation de répertoire partagé. Un administrateur de ce compte lance le flux de travail de partage d'annuaire en spécifiant avec qui Comptes AWS partager son répertoire. Les propriétaires d'annuaires peuvent voir avec qui ils ont partagé un annuaire depuis l'onglet Mettre à l'échelle et partager pour un annuaire donné dans la console Directory Service .

Compte consommateur de l'annuaire

Dans une relation d'annuaire partagé, le consommateur de l'annuaire représente le Compte AWS avec lequel le propriétaire de l'annuaire a partagé l'annuaire. En fonction de la méthode de partage utilisée, un administrateur de ce compte peut avoir besoin d'accepter une invitation envoyée depuis le propriétaire de l'annuaire avant de pouvoir commencer à utiliser l'annuaire partagé.

Le processus de partage d'annuaire crée un annuaire partagé dans le compte consommateur de l'annuaire. Ce répertoire partagé contient les métadonnées qui permettent à l' EC2 instance de rejoindre facilement le domaine, qui localise le répertoire d'origine dans le compte du propriétaire du répertoire. Chaque annuaire partagé dans le compte consommateur de l'annuaire possède un identifiant unique (ID de l'annuaire partagé).

Méthodes de partage

AWS Managed Microsoft AD propose les deux méthodes de partage d'annuaires suivantes :

- **AWS Organizations** : cette méthode simplifie le partage de l'annuaire au sein de votre organisation. En effet, elle vous permet de parcourir et de confirmer les comptes consommateurs de l'annuaire. Pour utiliser cette option, votre organisation doit avoir Toutes les fonctions activées et votre annuaire doit être situé dans le compte de gestion de l'organisation. Cette méthode de partage simplifie votre configuration car elle n'oblige pas les comptes utilisateurs de l'annuaire à accepter votre demande de partage d'annuaire. Dans la console, cette méthode est appelée Partager ce répertoire au Comptes AWS sein de votre organisation.
- **Handshake** — Cette méthode permet le partage de répertoires lorsque vous ne l'utilisez AWS Organizations pas. Cette méthode de la « poignée de main » oblige le compte consommateur de l'annuaire à accepter la demande de partage d'annuaire. Dans la console, cette méthode est appelée Partager cet annuaire avec d'autres Comptes AWS.

La connectivité réseau

La connectivité réseau est une condition préalable à l'utilisation d'une relation de partage d'annuaires entre les deux Comptes AWS. AWS [prend en charge de nombreuses solutions pour vous connecter VPCs, notamment le peering VPC, Transit Gateway et VPN](#). Consultez [Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de EC2 domaine fluide](#) pour démarrer.

Considérations

Voici quelques points à prendre en compte lors de l'utilisation du partage d'annuaire avec votre Microsoft AD AWS géré :

Tarification

- AWS facture des frais supplémentaires pour le partage d'annuaires. Le compte Compte AWS qui utilise le AWS Managed Microsoft AD partagé est le compte débité des frais de partage. Pour en savoir plus, consultez la page de [tarification](#) du Directory Service site Web.
- Le partage d'annuaires fait de AWS Managed Microsoft AD un moyen plus rentable d'intégrer Amazon sur EC2 plusieurs comptes et VPCs.

Disponibilité dans les Régions

- Le partage d'annuaires est disponible dans toutes les [AWS régions où AWS Managed Microsoft AD est proposé](#).
- En AWS Chine (Ningxia), cette fonctionnalité n'est disponible que lorsque vous utilisez [AWS Systems Manager](#)(SSM) pour rejoindre facilement vos instances Amazon EC2 .

Pour plus d'informations sur le partage d'annuaires et sur la manière d'étendre la portée de votre annuaire Microsoft AD AWS géré au-delà des limites du AWS compte, consultez les rubriques suivantes.

Rubriques

- [Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de EC2 domaine fluide](#)
- [Annulation du partage de votre répertoire](#)

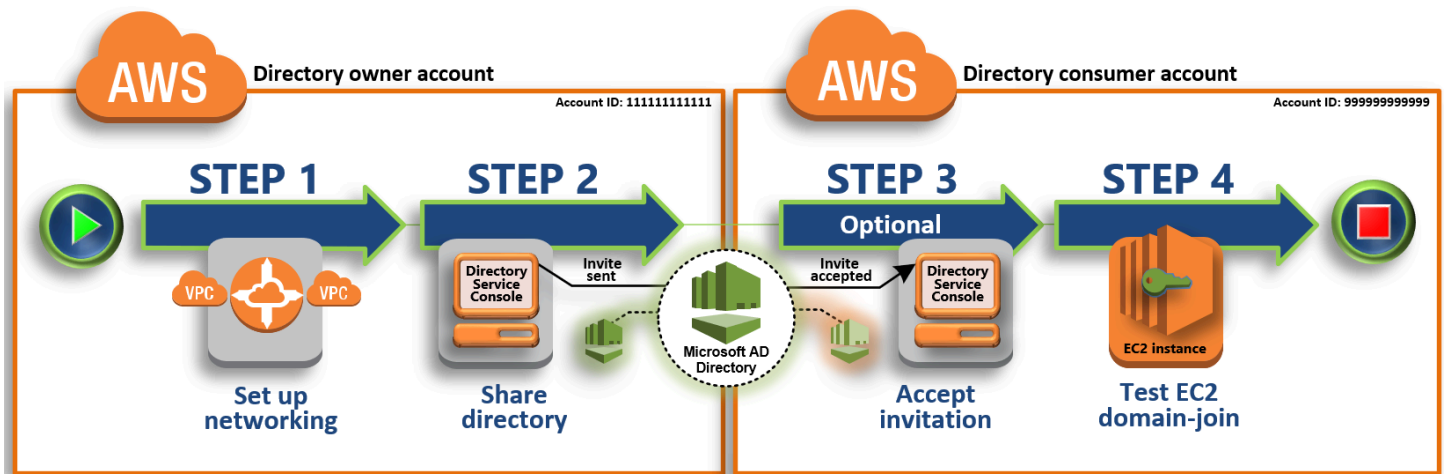
Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de EC2 domaine fluide

Ce didacticiel explique comment partager votre annuaire Microsoft AD AWS géré (le compte du propriétaire du répertoire) avec un autre Compte AWS (le compte client de l'annuaire). Une fois que les conditions préalables à la mise en réseau sont remplies, vous partagerez un répertoire entre deux Comptes AWS. Vous apprendrez ensuite comment joindre facilement une EC2 instance à un domaine dans le compte consommateur de l'annuaire.

Nous vous recommandons d'examiner les concepts clés du partage d'annuaire et le contenu des cas d'utilisation avant de commencer à travailler avec ce didacticiel. Pour de plus amples informations, veuillez consulter [Concepts clés du partage d'annuaire](#).

Le processus de partage de votre annuaire varie selon que vous le partagez avec un autre Compte AWS membre de la même AWS organisation ou avec un compte externe à l' AWS organisation. Pour plus d'informations sur le partage, veuillez consulter [Méthodes de partage](#).

Ce flux de travail se compose de quatre étapes de base.



Étape 1 : configurez votre environnement de mise en réseau

Dans le compte propriétaire de l'annuaire, vous configurez tous les prérequis de mise en réseau nécessaires pour le processus de partage d'annuaire.

Étape 2 : partagez votre annuaire

Une fois connecté avec les informations d'identification d'administrateur propriétaire de l'annuaire, vous ouvrez la console Directory Service et démarrez le flux de partage d'annuaire. Celui-ci envoie une invitation au compte consommateur de l'annuaire.

Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif

Lorsque vous êtes connecté avec les informations d'identification de l'administrateur utilisateur de l'annuaire, vous ouvrez la Directory Service console et acceptez l'invitation de partage d'annuaire.

Étape 4 : tester la liaison fluide d'une EC2 instance pour Windows Server à un domaine

Enfin, en tant qu'administrateur consommateur de l'annuaire, vous essayez de joindre une EC2 instance à votre domaine et de vérifier qu'elle fonctionne.

Ressources supplémentaires

- [Cas d'utilisation : partagez votre annuaire pour associer facilement EC2 des instances Amazon à un domaine sur Comptes AWS](#)
- [AWS Article de blog sur la sécurité : Comment joindre EC2 des instances Amazon à partir de plusieurs comptes et VPCs à un seul annuaire Microsoft AD AWS géré](#)

Étape 1 : configurez votre environnement de mise en réseau

Vous devrez établir une connexion d'appairage Amazon VPC pour partager votre annuaire AWS Microsoft AD géré (propriétaire du compte d'annuaire) avec un autre Compte AWS (compte client de l'annuaire). Consultez les procédures suivantes pour savoir comment configurer votre environnement réseau pour un Microsoft AD AWS géré partagé.

Prérequis

Avant d'exécuter les procédures fournies dans ce didacticiel, vous devez commencer par effectuer les opérations suivantes :

- Créez-en deux nouveaux Comptes AWS à des fins de test dans la même région. Lorsque vous créez un Compte AWS, il crée automatiquement un cloud privé virtuel (VPC) dédié dans chaque compte. Prenez note de l'ID du VPC dans chaque compte. Vous en aurez besoin ultérieurement.
- [Créez un Microsoft AD AWS géré.](#)
- Lors de la création d'une connexion d'appairage VPC, le propriétaire du compte d'annuaire et le compte consommateur de l'annuaire auront besoin des autorisations nécessaires pour créer et accepter la connexion d'appairage. Pour plus d'informations, consultez [Exemple : création d'une connexion d'appairage VPC](#) et [Exemple : Accepter une connexion d'appairage VPC](#).

Note

Bien qu'il existe de nombreuses manières de connecter le propriétaire du répertoire et le compte client du répertoire VPCs, ce didacticiel utilisera la méthode d'appairage VPC. Pour plus d'options d'appairage de VPC, reportez-vous à la section [La connectivité réseau](#).

Configurez une connexion d'appairage de VPC entre le compte propriétaire de l'annuaire et le compte consommateur de l'annuaire

La connexion d'appairage VPC que vous allez créer se fait entre le consommateur de l'annuaire et le propriétaire du répertoire. VPCs Procédez comme suit pour configurer une connexion d'appairage de VPC pour accéder au compte consommateur de l'annuaire. Avec cette connexion, vous pouvez acheminer le trafic entre les deux VPCs en utilisant des adresses IP privées.

Pour créer une connexion d'appairage de VPC entre le compte propriétaire de l'annuaire et le compte consommateur de l'annuaire

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>. Assurez-vous de vous connecter en tant qu'utilisateur avec des informations d'identification d'administrateur dans le compte du propriétaire de l'annuaire avec les autorisations nécessaires pour créer une connexion d'appairage VPC. Pour plus d'informations, consultez [Prérequis](#).
2. Dans le volet de navigation, choisissez Peering Connections (Connexions d'appairage). Ensuite, choisissez Créer une connexion d'appairage.
3. Configurez les informations suivantes :
 - Balise de nom de connexion d'appairage : Choisissez un nom qui identifie clairement cette connexion avec le VPC du compte consommateur de l'annuaire.
 - VPC (Demandeur) : Sélectionnez l'ID de VPC correspondant au compte propriétaire de l'annuaire.
 - Dans Sélectionner un autre VPC auquel s'appairer, assurez-vous que les options Mon compte et Cette région sont sélectionnées.
 - VPC (Accepteur) : Sélectionnez l'ID de VPC correspondant au compte consommateur de l'annuaire.
4. Choisissez Créer une connexion d'appairage. Dans la boîte de dialogue de confirmation, choisissez OK.

Pour accepter la demande d'appairage au nom du compte consommateur de l'annuaire

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>. Assurez-vous de vous connecter en tant qu'utilisateur disposant des autorisations nécessaires pour accepter la demande de peering. Pour plus d'informations, consultez [Prérequis](#).
2. Dans le volet de navigation, choisissez Peering Connections (Connexions d'appairage).
3. Sélectionnez la connexion d'appairage de VPC en attente. (Son statut est En attente d'acceptation.) Choisissez Actions, Accepter la demande.
4. Dans la boîte de dialogue de confirmation, choisissez Yes, Accept (Oui, accepter). Dans la boîte de dialogue de confirmation qui suit, choisissez Modifier mes tables de routage maintenant pour accéder directement à la page des tables de routage.

Maintenant que votre connexion d'appairage de VPC est active, vous devez ajouter une entrée dans la table de routage de votre VPC dans le compte propriétaire de l'annuaire. Ceci permet d'acheminer le trafic vers le VPC du compte consommateur de l'annuaire.

Pour ajouter une entrée dans la table de routage du VPC dans le compte propriétaire de l'annuaire

1. Dans la section Tables de routage de la console Amazon VPC, sélectionnez la table de routage correspondant au VPC propriétaire de l'annuaire.
2. Choisissez l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.
3. Dans la colonne Destination, saisissez le bloc d'adresse CIDR pour le VPC consommateur de l'annuaire.
4. Dans la colonne Cible, saisissez l'ID de la connexion d'appairage de VPC (par exemple, **pcx-123456789abcde000**) correspondant à la connexion d'appairage que vous avez créée précédemment dans le compte propriétaire de l'annuaire.
5. Sélectionnez Enregistrer les modifications.

Pour ajouter une entrée dans la table de routage du VPC dans le compte consommateur de l'annuaire

1. Dans la section Tables de routage de la console Amazon VPC, sélectionnez la table de routage correspondant au VPC consommateur de l'annuaire.
2. Choisissez l'onglet Routes, choisissez Modifier les routes, puis Ajouter une route.
3. Dans la colonne Destination, saisissez le bloc d'adresse CIDR pour le VPC propriétaire de l'annuaire.
4. Dans la colonne Cible, saisissez l'ID de la connexion d'appairage de VPC (par exemple, **pcx-123456789abcde001**) correspondant à la connexion d'appairage que vous avez créée précédemment dans le compte consommateur de l'annuaire.
5. Sélectionnez Enregistrer les modifications.

Ajoutez des protocoles et des ports Active Directory aux règles de sortie pour les groupes de sécurité dans Directory Consumer VPCs. Pour plus d'informations, veuillez consulter [Security groups for your VPC](#) et [AWS Managed Microsoft AD prerequisites](#) (français non garanti).

Étape suivante

[Étape 2 : partagez votre annuaire](#)

Étape 2 : partagez votre annuaire

Utilisez les procédures suivantes pour commencer le flux de partage d'annuaire depuis le compte propriétaire de l'annuaire.

Note

Le partage d'annuaires est une fonctionnalité régionale de AWS Managed Microsoft AD. Si vous utilisez [la réplication multirégionale](#), les procédures suivantes doivent être appliquées séparément dans chaque région. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Pour partager votre annuaire depuis le compte propriétaire de l'annuaire

1. Connectez-vous au compte du propriétaire du répertoire à l' AWS Management Console aide des informations d'identification d'administrateur et ouvrez la [AWS Directory Service console](#) à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Choisissez l'ID de répertoire du répertoire Microsoft AD AWS géré que vous souhaitez partager.
4. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région dans laquelle vous souhaitez partager votre annuaire, puis cliquez sur l'onglet Mettre à l'échelle et partager. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Mettre à l'échelle et partager.
5. Dans la section Annuaire partagé, choisissez Actions, puis Créer un nouvel annuaire partagé.
6. Sur la page Choisissez avec qui Comptes AWS partager, choisissez l'une des méthodes de partage suivantes en fonction des besoins de votre entreprise :
 - a. Partager ce répertoire avec les Comptes AWS membres de votre organisation : avec cette option, vous pouvez sélectionner le répertoire avec lequel Comptes AWS vous souhaitez partager votre répertoire dans une liste répertoriant tous les éléments Comptes AWS internes de votre AWS organisation. Vous devez activer l'accès sécurisé avec Directory

Service avant de partager un annuaire. Pour plus d'informations, veuillez consulter [How to enable or disable trusted access](#) (français non garanti).

 Note

Pour utiliser cette option, votre organisation doit avoir Toutes les fonctions activées et votre annuaire doit être situé dans le compte de gestion de l'organisation.

- i. Comptes AWS Dans votre organisation, sélectionnez le répertoire avec Comptes AWS lequel vous souhaitez partager le répertoire et cliquez sur Ajouter.
- ii. Passez en revue les informations de tarification, puis choisissez Partager.
- iii. Passez à l'[étape 4](#) de ce guide. Comme tous Comptes AWS font partie de la même organisation, il n'est pas nécessaire de suivre l'étape 3.
- b. Partager ce répertoire avec d'autres Comptes AWS personnes : avec cette option, vous pouvez partager un répertoire avec des comptes internes ou externes à votre AWS organisation. Vous pouvez également utiliser cette option lorsque votre annuaire n'est pas membre d'une AWS organisation et que vous souhaitez le partager avec une autre Compte AWS.
 - i. Dans Compte AWS ID (s), entrez tous ceux avec Compte AWS IDs lesquels vous souhaitez partager le répertoire, puis cliquez sur Ajouter.
 - ii. Dans Envoyer un message, saisissez un message à l'attention de l'administrateur de l'autre Compte AWS.
 - iii. Passez en revue les informations de tarification, puis choisissez Partager.
 - iv. Passez à l'étape 3.

Étape suivante

[Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif](#)

Étape 3 : Accepter l'invitation à un répertoire partagé - Facultatif

Si vous avez choisi l'option Partager cet annuaire avec d'autres Comptes AWS (méthode de l'établissement de liaison) dans la procédure précédente, procédez comme suit pour terminer le flux de partage d'annuaire. Si vous avez choisi l'option Partager ce répertoire avec Comptes AWS les membres de votre organisation, ignorez cette étape et passez à l'étape 4.

Pour accepter l'invitation de partage d'annuaire

1. Connectez-vous au compte consommateur du répertoire AWS Management Console avec les informations d'identification de l'administrateur et ouvrez la [AWS Directory Service console](https://console.aws.amazon.com/directoryservicev2/) à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Annuaire partagé avec moi.
3. Dans la colonne ID de l'annuaire partagé, choisissez l'ID de l'annuaire qui affiche l'état En attente d'acceptation.
4. Dans la page Détails de l'annuaire partagé, choisissez Vérifier.
5. Dans la boîte de dialogue Invitation en attente pour l'annuaire partagé, passez en revue le message, les détails sur le propriétaire de l'annuaire et les informations de tarification. Si vous êtes d'accord, choisissez Accepter pour commencer à utiliser l'annuaire.

Étape suivante

[Étape 4 : tester la liaison fluide d'une EC2 instance pour Windows Server à un domaine](#)

Étape 4 : tester la liaison fluide d'une EC2 instance pour Windows Server à un domaine

Vous pouvez utiliser l'une des deux méthodes suivantes pour tester la liaison fluide d'une EC2 instance à un domaine.

Méthode 1 : tester la jonction de domaines à l'aide de la EC2 console Amazon

Effectuez ces étapes dans le compte consommateur de l'annuaire.

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Windows.
5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.

6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.
 - a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.
 - b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.
 - c. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez .pem. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez .ppk.
 - d. Choisissez Créer une paire de clés.
 - e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

 Important

C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

 Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM SSMDirectoryServiceAccess auquel sont associées les politiques AWS gérées Amazon SSMManged InstanceCore et Amazon dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :

1. Choisissez Créer un rôle.

2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
3. Sous Use case (Cas d'utilisation), choisissez EC2.
4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les SSMDirectory ServiceAccess politiques Amazon SSManaged InstanceCore et Amazon. Pour filtrer la liste, tapez **SSM** dans la zone de recherche. Choisissez Suivant.

 Note

Amazon SSMDirectory ServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. Amazon SSManaged InstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section [Create an IAM instance profile for Systems Manager](#) (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'associer à l' EC2instance.
 6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
 7. Choisissez Créer un rôle.
 8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.
16. Choisissez Launch instance (Lancer une instance).

Méthode 2 : test de la jonction de domaines via AWS Systems Manager

Effectuez ces étapes dans le compte consommateur de l'annuaire. Pour effectuer cette procédure, vous aurez besoin de certaines informations sur le compte du propriétaire du répertoire, telles que l'ID du répertoire, le nom du répertoire et les adresses IP DNS.

Prérequis

- Configuration AWS Systems Manager.
 - Pour de plus amples informations sur Systems Manager, veuillez consulter [General setup for AWS Systems Manager](#) (français non garanti).
- Les instances auxquelles vous souhaitez rejoindre le domaine Microsoft Active Directory AWS géré doivent être associées à un rôle IAM contenant les politiques SSMDirectory ServiceAccess gérées par Amazon SSMManged InstanceCore et Amazon.
- Pour plus d'informations sur ces stratégies gérées et sur les autres stratégies que vous pouvez attacher à un profil d'instance pour Systems Manager consultez [Création d'un profil d'instance IAM pour Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager . Pour plus d'informations sur les stratégies gérées, veuillez consulter [AWS Managed policies](#) (français non garanti) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur l'utilisation de Systems Manager pour joindre des EC2 instances à un domaine Microsoft Active Directory AWS géré, voir [AWS Systems Manager Comment associer une instance EC2 Windows en cours d'exécution à mon domaine AWS Directory Service ?](#) .

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.
2. Dans le panneau de navigation, sous Gestion des nœuds, choisissez Exécuter la commande.
3. Sélectionnez Run Command (Exécuter la commande).
4. Sur la page Exécuter la commande, recherchez AWS-JoinDirectoryServiceDomain. Lorsqu'elle s'affiche dans les résultats de recherche, sélectionnez l'option AWS-JoinDirectoryServiceDomain.
5. Faites défiler jusqu'à la section Paramètres de la commande. Vous devez fournir les paramètres suivants :

 Note

Vous pouvez localiser l'ID du répertoire, le nom du répertoire et les adresses IP DNS en revenant à la Directory Service console, en sélectionnant Répertoires partagés avec moi, puis en sélectionnant votre répertoire. L'ID de votre annuaire se trouve dans la section Détails du répertoire partagé. Vous pouvez trouver les valeurs du nom du répertoire et des adresses IP DNS dans la section Détails de l'annuaire propriétaire.

- Pour ID de l'annuaire, entrez le nom de l'annuaire AWS Managed Microsoft Active Directory.
 - Pour Nom de l'annuaire, entrez le nom de l'annuaire AWS Managed Microsoft Active Directory (pour le compte du propriétaire de l'annuaire).
 - Pour les adresses IP DNS, entrez les adresses IP des serveurs DNS dans le répertoire Microsoft Active Directory AWS géré (pour le compte du propriétaire de l'annuaire).
6. Pour Cibles, choisissez Choisir les instances manuellement, puis sélectionnez les instances que vous souhaitez joindre au domaine.
 7. Pour le reste du formulaire, laissez les valeurs par défaut, faites défiler la page, puis choisissez Exécuter.
 8. Le statut de la commande passe de En attente à Réussi une fois que les instances ont joint le domaine avec succès. Vous pouvez afficher le résultat de la commande en sélectionnant l'ID d'instance de l'instance qui a joint le domaine et Afficher le résultat.

Après avoir effectué l'une ou l'autre de ces étapes, vous devriez maintenant être en mesure de joindre votre EC2 instance au domaine. Une fois cela fait, vous pouvez vous connecter à votre instance à l'aide d'un client RDP (Remote Desktop Protocol) avec les informations d'identification de votre compte utilisateur Microsoft AD AWS géré.

Annulation du partage de votre répertoire

Utilisez la procédure suivante pour annuler le partage d'un annuaire Microsoft AD AWS géré.

Pour annuler le partage de votre annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaire.
2. Choisissez l'ID de répertoire du répertoire Microsoft AD AWS géré dont vous souhaitez annuler le partage.
3. Sur la page Directory details (Détails de l'annuaire), procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Multi-Region replication (Réplication multi-régions), sélectionnez la région dans laquelle vous souhaitez annuler le partage de votre annuaire, puis cliquez sur l'onglet Scale & share (Mettre à l'échelle et partager). Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- Si aucune région n'apparaît sous Multi-Region replication (Réplication multi-régions), choisissez l'onglet Mettre à l'échelle et partager.
4. Dans la section Annuaire partagés, sélectionnez l'annuaire partagé dont vous souhaitez annuler le partage, choisissez Actions, puis choisissez Annuler le partage.
 5. Dans la boîte de dialogue Annuler le partage de l'annuaire, choisissez Annuler le partage.

Ressources supplémentaires

- [Cas d'utilisation : partagez votre annuaire pour associer facilement EC2 des instances Amazon à un domaine sur plusieurs AWS comptes](#)
- [AWS article de blog sur la sécurité : Comment joindre EC2 des instances Amazon à partir de plusieurs comptes et VPCs à un seul annuaire Microsoft AD AWS géré](#)
- [Regrouper vos instances Amazon RDS DB des différents comptes dans un seul domaine partagé](#)

Migration des utilisateurs d'Active Directory vers AWS Managed Microsoft AD

Vous pouvez utiliser le Active Directory Migration Toolkit (ADMT) ainsi que le service d'exportation de mots de passe (PES) pour migrer les utilisateurs de votre Active Directory autogéré vers votre annuaire AWS Microsoft AD géré. Cela vous permet de migrer plus facilement les objets Active Directory et les mots de passe chiffrés pour vos utilisateurs.

Pour obtenir des instructions détaillées, consultez [Comment migrer votre domaine local vers AWS Managed Microsoft AD à l'aide d'ADMT](#) sur le blog de AWS sécurité.

Connect AWS Managed Microsoft AD à votre infrastructure Active Directory existante

Cette section décrit comment configurer les relations de confiance entre AWS Managed Microsoft AD et votre infrastructure Active Directory existante.

Tâches pour connecter votre Microsoft AD AWS géré à votre Active Directory existant :

- [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#)
- [Ajout de routes IP lors de l'utilisation d'adresses IP publiques avec votre Microsoft AD AWS géré](#)

- [Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.](#)
- [Didacticiel : créer une relation d'approbation entre deux domaines AWS Managed Microsoft AD](#)

Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré

Vous pouvez configurer des relations d'approbation externes et forestières unidirectionnelles ou bidirectionnelles entre votre Service d' AWS annuaire pour Microsoft Active Directory et les annuaires autogérés (sur site), ainsi qu'entre plusieurs annuaires AWS Microsoft AD gérés dans le cloud. AWS AWS Managed Microsoft AD prend en charge les trois directions des relations de confiance : entrante, sortante et bidirectionnelle (bidirectionnelle).

Pour plus d'informations sur les relations de confiance, voir [Tout ce que vous vouliez savoir sur les approbations avec AWS Managed Microsoft AD.](#)

Note

Lorsque vous configurez des relations de confiance, vous devez vous assurer que votre annuaire autogéré est et reste compatible avec Directory Service s. Pour plus d'informations sur vos responsabilités, veuillez consulter notre [modèle de responsabilité partagée.](#)

AWS Managed Microsoft AD prend en charge les approbations externes et forestières. Pour passer en revue un exemple de scénario montrant comment créer une approbation de forêt, veuillez consulter [Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory..](#)

Une confiance bidirectionnelle est requise pour les applications AWS d'entreprise telles qu'Amazon Chime, Amazon Connect, Quick Suite AWS IAM Identity Center, WorkDocs, Amazon WorkMail, WorkSpaces Amazon et le. AWS Management Console AWS Managed Microsoft AD doit être en mesure d'interroger les utilisateurs et les groupes de votre Active Directory autogéré.

Vous pouvez activer l'authentification sélective afin que seul le compte de service spécifique à AWS l'application puisse interroger votre Active Directory autogéré. Pour plus d'informations, voir [Renforcer la sécurité de AWS l'intégration de votre application avec AWS Managed Microsoft AD.](#)

Amazon EC2, Amazon RDS et Amazon FSx travailleront dans le cadre d'une confiance unidirectionnelle ou bidirectionnelle.

Prérequis

La création de l'approbation s'effectue en quelques étapes seulement, mais vous devez d'abord effectuer plusieurs étapes préalables à la phase de configuration de la relation d'approbation.

Note

AWS Managed Microsoft AD ne prend pas en charge la confiance avec les [domaines à étiquette unique](#).

Connexion au VPC

Si vous créez une relation de confiance avec votre annuaire autogéré, vous devez d'abord connecter votre réseau autogéré au VPC Amazon contenant votre Microsoft AD géré AWS . Le pare-feu de vos réseaux Microsoft AD AWS autogérés et gérés doit avoir les ports réseau ouverts répertoriés dans [WindowsServer 2008 et versions ultérieures](#) dans Microsoft la documentation.

Pour utiliser votre nom NetBIOS au lieu de votre nom de domaine complet pour l'authentification auprès de vos AWS applications telles qu'Amazon ou WorkDocs Amazon Quick Suite, vous devez autoriser le port 9389. Pour plus d'informations sur les ports et protocoles Active Directory, consultez la section [Présentation des services et exigences relatives aux ports réseau Windows](#) dans Microsoft la documentation.

Il s'agit des ports minimum requis pour vous permettre de vous connecter à votre annuaire. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Configuration de votre VPC

Le VPC qui contient votre AWS Microsoft AD géré doit disposer des règles sortantes et entrantes appropriées.

Pour configurer vos règles sortantes VPC

1. Dans la [AWS Directory Service console](#), sur la page Détails du répertoire, notez votre ID d'annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

3. Choisissez Security Groups.
4. Recherchez votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez l'élément avec la description « groupe de sécurité AWS créé pour les contrôleurs d'annuaire avec ID de répertoire ».

 Note

Le groupe de sécurité sélectionné est un groupe de sécurité qui est créé automatiquement lorsque vous créez initialement votre annuaire.

5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Sélectionnez Edit, puis Add another rule. Pour la nouvelle règle, saisissez les valeurs suivantes :
 - Type : All Traffic
 - Protocole : All
 - La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et les directions possible sur votre réseau autogéré. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour de plus amples informations, veuillez consulter [Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire](#).
6. Sélectionnez Save.

Activation de l'authentification préalable Kerberos

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Pour plus d'informations sur ce paramètre, consultez la section [Préauthentification](#) sur Microsoft TechNet.

Configuration des redirecteurs conditionnels DNS sur votre domaine autogéré

Vous devez configurer des redirecteurs conditionnels DNS sur votre domaine autogéré. Reportez-vous à la section [Affecter un redirecteur conditionnel pour un nom de domaine](#) sur Microsoft TechNet pour plus de détails sur les redirecteurs conditionnels.

Pour effectuer les étapes suivantes, vous devez avoir accès aux outils Windows Server suivants pour votre domaine autogéré :

- Outils AD DS et AD LDS

- DNS

Pour configurer les redirecteurs conditionnels sur votre domaine autogéré

1. Vous devez d'abord obtenir des informations sur votre AWS Managed Microsoft AD. Connectez-vous à AWS Management Console et ouvrez la [console AWS Directory Service](#).
2. Dans le volet de navigation, sélectionnez Directories.
3. Choisissez l'ID de répertoire de votre AWS Managed Microsoft AD.
4. Prenez note du nom de domaine complet (FQDN) et des adresses DNS de votre annuaire.
5. Retournez maintenant à votre contrôleur de domaine autogéré. Ouvrez le Gestionnaire de serveur.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez la relation d'approbation.
8. Dans l'arborescence de la console, sélectionnez Conditional Forwarders.
9. Dans le menu Action, choisissez New conditional forwarder.
10. Dans le domaine DNS, tapez le nom de domaine complet (FQDN) de votre AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment.
11. Choisissez les adresses IP des serveurs principaux et saisissez les adresses DNS de votre répertoire AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment.

Après avoir saisi les adresses DNS, il se peut que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.

12. Sélectionnez Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain. Choisissez OK.

Mot de passe de relation d'approbation

Si vous créez une relation d'approbation avec un domaine existant, configurez la relation d'approbation sur ce domaine à l'aide des outils d'administration de Windows Server. Pensez à relever le mot de passe de la relation d'approbation que vous utilisez. Vous devrez utiliser ce même mot de passe lors de la configuration de la relation de confiance sur AWS Managed Microsoft AD. Pour plus d'informations, consultez [la section Gestion des approbations](#) sur Microsoft TechNet.

Vous êtes maintenant prêt à créer la relation de confiance sur votre AWS Managed Microsoft AD.

Noms de domaine et NetBIOS

Les noms de domaine et NetBIOS doivent être uniques et ne peuvent pas être identiques pour établir une relation d'approbation.

Création, vérification ou suppression d'une relation d'approbation

Note

Les relations de confiance sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez [Configuration de la réplication multirégionale pour AWS Managed Microsoft AD](#), les procédures suivantes doivent être effectuées dans [Région principale](#). Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Pour créer une relation de confiance avec votre Microsoft AD AWS géré

1. Ouvrez la [AWS Directory Service console](#).
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation d'approbation, fournissez les informations requises, y compris le type d'approbation, le nom de domaine complet (FQDN) de votre domaine approuvé, le mot de passe et la direction d'approbation.
6. (Facultatif) Si vous souhaitez autoriser uniquement les utilisateurs autorisés à accéder aux ressources de votre répertoire AWS Managed Microsoft AD, vous pouvez éventuellement cocher la case Authentification sélective. Pour obtenir des informations générales sur l'authentification sélective, consultez la section [Considérations relatives à la sécurité pour les entreprises de confiance](#) chez Microsoft TechNet.

7. Pour Redirecteur conditionnel, saisissez l'adresse IP de votre serveur DNS autogéré. Si vous avez créé précédemment des redirecteurs conditionnels, vous pouvez saisir le nom de domaine complet de votre domaine autogéré au lieu d'une adresse IP DNS.
8. (Facultatif) Choisissez Add another IP (Ajouter une autre adresse IP) et entrez l'adresse IP d'un autre serveur DNS autogéré. Vous pouvez répéter cette étape pour chaque adresse de serveur DNS applicable pour un total de quatre adresses.
9. Choisissez Ajouter.
10. Si le serveur DNS ou le réseau de votre domaine autogéré utilise un espace d'adresse IP publique (non RFC 1918), accédez à la section IP routing (Routage IP) et choisissez Actions, puis Add route (Ajouter une route). Tapez le bloc d'adresse IP de votre serveur DNS ou réseau autogéré selon le format CIDR, par exemple 203.0.113.0/24. Cette étape n'est pas nécessaire si votre serveur DNS et votre réseau autogéré utilisent des espaces d'adressage IP RFC 1918.

 Note

Lorsque vous définissez un espace d'adressage IP publique, assurez-vous de ne pas utiliser l'une des [plages d'adresses IP AWS](#) ; en effet, celles-ci ne peuvent pas être exploitées dans ce type de cas.

11. (Facultatif) Nous vous recommandons de sélectionner Add routes to the security group for this directory's VPC (Ajouter des routes au groupe de sécurité pour le VPC de cet annuaire) pendant que vous êtes sur la page Add routes (Ajouter des routes). Cela va permettre de configurer les groupes de sécurité comme indiqué ci-dessus dans la section « Configuration de votre VPC ». Ces règles de sécurité ont un impact sur une interface réseau interne qui n'est pas exposée publiquement. Si cette option n'est pas disponible, un message s'affichera pour indiquer que vous avez déjà personnalisé vos groupes de sécurité.

Vous devez configurer la relation d'approbation sur les deux domaines. Les relations doivent être complémentaires. Par exemple, si vous créez une relation d'approbation sortante sur un domaine, vous devez créer une relation d'approbation entrante sur l'autre.

Si vous créez une relation d'approbation avec un domaine existant, configurez la relation d'approbation sur ce domaine à l'aide des outils d'administration de Windows Server.

Vous pouvez créer plusieurs approbations entre votre Microsoft AD AWS géré et différents domaines Active Directory. Cependant, vous ne pouvez avoir qu'une seule relation d'approbation par paire. Par exemple, si vous avez déjà une relation de confiance unidirectionnelle dans le « sens entrant » et que

vous souhaitez ensuite établir une autre relation de confiance dans le « sens sortant », vous devrez supprimer le lien de confiance existant et créer un nouveau lien de confiance « bidirectionnel ».

Pour vérifier une relation d'approbation sortante

1. Ouvrez la [AWS Directory Service console](#).
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), sélectionnez la relation d'approbation que vous voulez vérifier et choisissez Actions, puis Verify trust relationship (Vérifier la relation d'approbation).

Ce processus vérifie uniquement la direction sortante d'une confiance bidirectionnelle. AWS ne prend pas en charge la vérification des trusts entrants. Pour plus d'informations sur la façon de vérifier une approbation depuis ou vers votre Active Directory autogéré, consultez [Vérifier une approbation](#) sur Microsoft TechNet.

Suppression d'une relation d'approbation existante

1. Ouvrez la [AWS Directory Service console](#).
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), sélectionnez la relation d'approbation que vous voulez supprimer et choisissez Actions, puis Delete trust relationship (Supprimer la relation d'approbation).

5. Sélectionnez Supprimer.

Ajout de routes IP lors de l'utilisation d'adresses IP publiques avec votre Microsoft AD AWS géré

Vous pouvez utiliser AWS Directory Service for Microsoft Active Directory pour tirer parti de nombreuses fonctionnalités puissantes d'Active Directory, notamment pour établir des approbations avec d'autres annuaires. Toutefois, si les serveurs DNS des réseaux d'autres annuaires utilisent des adresses IP publiques (non RFC 1918), vous devez spécifier ces adresses IP dans le cadre de la configuration de la relation d'approbation. Vous pourrez trouver des informations à ce sujet dans [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#).

De même, vous devez également saisir les informations d'adresse IP lorsque vous acheminez le trafic depuis votre AWS Managed Microsoft AD AWS vers un VPC homologue, si le AWS VPC utilise des plages d'adresses IP publiques.

Lorsque vous ajoutez les adresses IP comme décrit dans [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#), vous avez la possibilité de sélectionner Add routes to the security group for this directory's VPC. Cette option doit être sélectionnée, sauf si vous avez déjà personnalisé votre [groupe de sécurité](#) pour autoriser le trafic nécessaire comme indiqué ci-dessous. Pour de plus amples informations, veuillez consulter [Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire](#).

Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory.

Ce didacticiel explique toutes les étapes nécessaires à la mise en place d'une relation de confiance entre AWS Directory Service for Microsoft Active Directory et votre Microsoft Active Directory autogéré (sur site). Même si la création de la relation d'approbation ne requiert que quelques étapes, vous devez d'abord effectuer les étapes préalables suivantes.

Rubriques

- [Prérequis](#)
- [Étape 1 : préparer votre domaine AD autogéré](#)
- [Étape 2 : préparer votre AWS Managed Microsoft AD](#)
- [Étape 3 : créer la relation d'approbation](#)

Voir aussi

[Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#)

Prérequis

Le didacticiel présume que vous avez déjà effectué les étapes suivantes :

Note

AWS Managed Microsoft AD ne prend pas en charge la confiance avec les [domaines à étiquette unique](#).

- Un répertoire Microsoft AD AWS géré créé le AWS. Si vous avez besoin d'aide pour effectuer l'opération, veuillez consulter [Commencer à utiliser AWS Managed Microsoft AD](#).
- Une EC2 instance en cours d'exécution Windows a été ajoutée à ce AWS Managed Microsoft AD. Si vous avez besoin d'aide pour effectuer l'opération, veuillez consulter [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).

Important

Le compte administrateur de votre AWS Managed Microsoft AD doit disposer d'un accès administratif à cette instance.

- Les outils de Windows serveur suivants sont installés sur cette instance :
 - Outils AD DS et AD LDS
 - DNS

Si vous avez besoin d'aide pour effectuer l'opération, veuillez consulter [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

- Annuaire Microsoft Active Directory (sur site) autogéré

Vous devez disposer d'un accès administratif à cet annuaire. Les mêmes outils de Windows serveur que ceux répertoriés ci-dessus doivent également être disponibles pour ce répertoire.

- Une connexion active entre votre réseau autogéré et le VPC contenant votre Microsoft AD AWS géré. Si vous avez besoin d'aide pour effectuer l'opération, veuillez consulter la section [Amazon Virtual Private Cloud Connectivity Options](#) (français non garanti).

- Une politique de sécurité locale définie correctement. Vérifiez Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously et assurez-vous que ce paramètre contient au moins les trois canaux nommés suivants :
 - netlogon
 - samr
 - lsarpc
- Les noms de domaine et NetBIOS doivent être uniques et ne peuvent pas être identiques pour établir une relation de confiance.

Pour plus d'informations sur les prérequis relatifs à la création d'une relation de confiance, veuillez consulter [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#).

Configuration du didacticiel

Pour ce didacticiel, nous avons déjà créé un domaine Microsoft AD AWS géré et un domaine autogéré. Le réseau autogéré est connecté au VPC de AWS Managed Microsoft AD. Voici les propriétés des deux annuaires :

AWS Microsoft AD géré s'exécutant sur AWS

- Nom de domaine (FQDN) : MyManaged AD.Example.com
- Nom NetBIOS : AD MyManaged
- Adresses DNS : 10.0.10.246, 10.0.20.121
- CIDR VPC : 10.0.0.0/16

Le Microsoft AD AWS géré réside dans l'ID VPC : vpc-12345678.

Domaine Microsoft AD AWS autogéré ou géré

- Nom de domaine (FQDN) : corp.example.com
- Nom NetBIOS : CORP
- Adresses DNS : 172.16.10.153
- CIDR autogéré : 172.16.0.0/16

Étape suivante

[Étape 1 : préparer votre domaine AD autogéré](#)

Étape 1 : préparer votre domaine AD autogéré

Tout d'abord, vous devez suivre plusieurs étapes préalables sur votre domaine (sur site) autogéré.

Configurer votre pare-feu autogéré

Vous devez configurer votre pare-feu autogéré de manière à ce que les ports suivants soient ouverts à tous CIDRs les sous-réseaux utilisés par le VPC qui contient votre Microsoft AD géré AWS . Dans ce didacticiel, nous autorisons le trafic entrant et sortant depuis la version 10.0.0.0/16 (le bloc CIDR du VPC de notre Managed AWS Microsoft AD) sur les ports suivants :

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- TCP/UDP 389 - Protocole LDAP (Lightweight Directory Access Protocol)
- TCP 445 - Bloc de messages du serveur (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (facultatif - Ce port doit être ouvert si vous souhaitez utiliser votre nom NetBIOS au lieu de votre nom de domaine complet pour vous authentifier auprès d'applications telles qu'Amazon ou AWS WorkDocs Amazon Quick Suite.)

Note

SMBv1 n'est plus pris en charge.

Il s'agit des ports minimum nécessaires pour connecter le VPC à l'annuaire autogéré. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

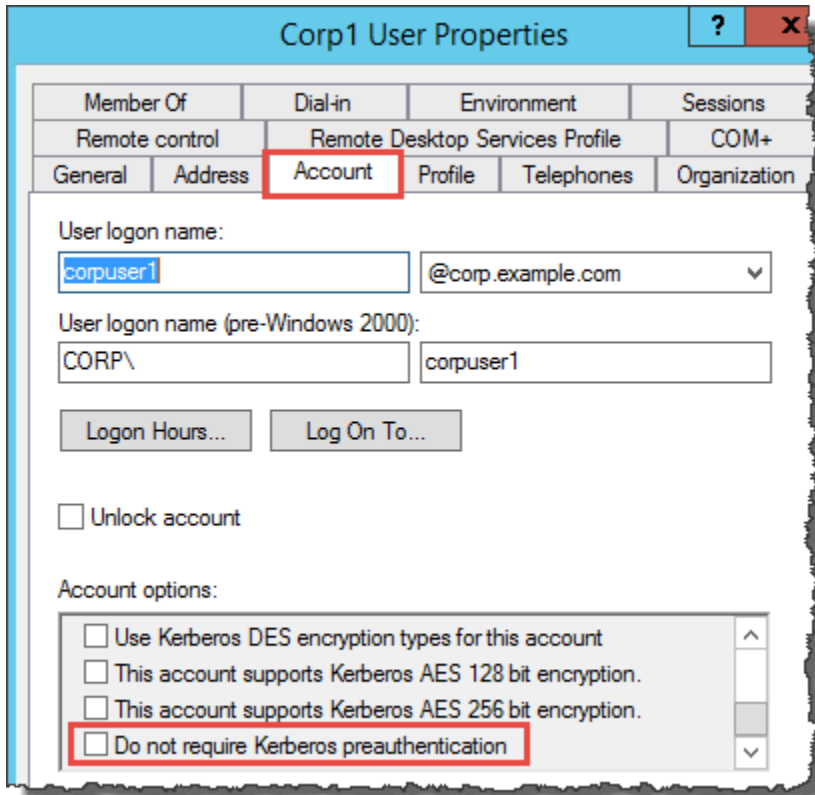
Vérification de l'activation de l'authentification préalable Kerberos

Les comptes d'utilisateur dans les deux annuaires doivent avoir une pré-authentification Kerberos activée. Il s'agit de la configuration par défaut, mais vérifiez les propriétés d'un utilisateur choisi de manière aléatoire afin de vous assurer que rien n'a changé.

Pour afficher les paramètres Kerberos de l'utilisateur

1. Sur votre contrôleur de domaine autogéré, ouvrez le Gestionnaire de serveur.

2. Dans le menu Tools, choisissez Active Directory Users and Computers.
3. Choisissez le dossier Utilisateurs et ouvrez le menu contextuel (clic droit). Sélectionnez un compte utilisateur de manière aléatoire parmi ceux répertoriés dans le volet droit. Choisissez Propriétés.
4. Choisissez l'onglet Account. Parcourez la liste Account options vers le bas pour vérifier que l'option Do not require Kerberos preauthentication n'est pas cochée.



Configuration des redirecteurs conditionnels DNS pour votre domaine autogéré

Vous devez configurer des redirecteurs conditionnels DNS sur chaque domaine. Avant de procéder à cette opération sur votre domaine autogéré, vous allez d'abord obtenir des informations sur votre AWS Managed Microsoft AD.

Pour configurer les redirecteurs conditionnels sur votre domaine autogéré

1. Connectez-vous à la [AWS Directory Service console AWS Management Console et ouvrez-la](#).
2. Dans le volet de navigation, sélectionnez Directories.
3. Choisissez l'ID de répertoire de votre AWS Managed Microsoft AD.

4. Sur la page Details (Détails), notez les valeurs des zones Directory name (Nom de l'annuaire) et DNS address (Adresse DNS) de votre annuaire.
5. Retournez maintenant à votre contrôleur de domaine autogéré. Ouvrez le Gestionnaire de serveur.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez la relation d'approbation. Notre serveur est WIN-5V70 CN7 VJ0.corp.example.com.
8. Dans l'arborescence de la console, sélectionnez Conditional Forwarders.
9. Dans le menu Action, choisissez New conditional forwarder.
10. Dans le domaine DNS, tapez le nom de domaine complet (FQDN) de votre AWS Managed Microsoft AD, comme vous l'avez indiqué précédemment. Dans cet exemple, le FQDN est MyManaged AD.Example.com.
11. Choisissez les adresses IP des serveurs principaux et saisissez les adresses DNS de votre annuaire Microsoft AD AWS géré, comme vous l'avez indiqué précédemment. Dans cet exemple, il s'agit de : 10.0.10.246, 10.0.20.121

Après avoir saisi les adresses DNS, il se peut que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.

New Conditional Forwarder

DNS Domain:
MyManagedAD.example.com

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...		
10.0.10.246	<Unable to resolve>	A timeout occurred duri...
10.0.20.121	<Unable to resolve>	A timeout occurred duri...

☒ Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this domain

This will not replicate to DNS Servers that are pre-Windows Server 2003 Domain Controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

OK Cancel

12. Sélectionnez Store this conditional forwarder in Active Directory, and replicate it as follows.
13. Sélectionnez All DNS servers in this domain, puis cliquez sur OK.

Étape suivante

[Étape 2 : préparer votre AWS Managed Microsoft AD](#)

Étape 2 : préparer votre AWS Managed Microsoft AD

Préparons maintenant votre Microsoft AD AWS géré pour la relation de confiance. Une grande partie des étapes suivantes est quasi-identique aux opérations que vous venez d'effectuer pour votre domaine autogéré. Toutefois, cette fois, vous travaillez avec votre AWS Managed Microsoft AD.

Configuration de vos groupes de sécurité et sous-réseaux VPC

Vous devez autoriser le trafic de votre réseau autogéré vers le VPC contenant votre Microsoft AD AWS géré. Pour ce faire, vous devez vous assurer que les règles ACLs associées aux sous-réseaux utilisés pour déployer votre AWS Managed Microsoft AD et les règles de groupe de sécurité configurées sur vos contrôleurs de domaine autorisent le trafic requis pour soutenir les approbations.

Les exigences relatives aux ports varient en fonction de la version de Windows Server utilisée par vos contrôleurs de domaine et les services ou applications qui utiliseront l'approbation. Dans le cadre de ce didacticiel, vous devez ouvrir les ports suivants :

Entrant

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Authentification Kerberos
- TCP 636 - LDAPS (LDAP sur TLS/SSL)
- TCP 3268-3269 - Catalogue global
- TCP/UDP 49152-65535 - Ports éphémères pour RPC

Note

SMBv1 n'est plus pris en charge.

Sortant

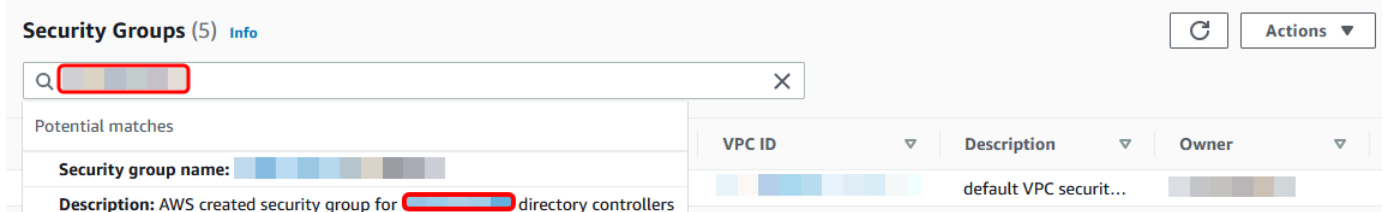
- ALL

Note

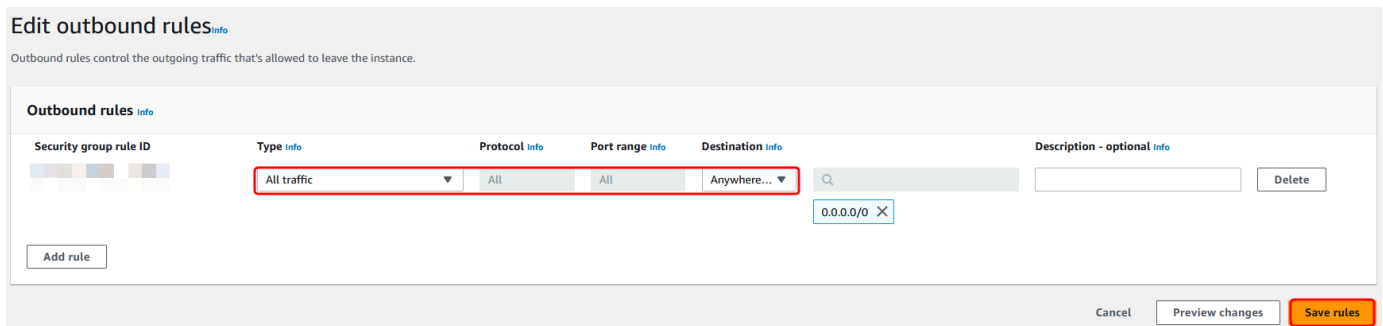
Il s'agit des ports minimum nécessaires pour connecter le VPC et l'annuaire autogéré. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Pour configurer les règles sortantes et entrantes de votre contrôleur de domaine Microsoft AD AWS géré

1. Revenez à la [console AWS Directory Service](#). Dans la liste des annuaires, notez l'ID du répertoire de votre annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Utilisez le champ de recherche pour rechercher votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez le groupe de sécurité avec la description **AWS created security group for *yourdirectoryID* directory controllers**.



5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Choisissez Modifier les règles sortantes, puis Ajouter une règle. Pour la nouvelle règle, saisissez les valeurs suivantes :
 - Type : ALL Traffic
 - Protocole : ALL
 - La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et où il peut aller. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour de plus amples informations, veuillez consulter [Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire](#).
6. Sélectionnez Enregistrer la règle.

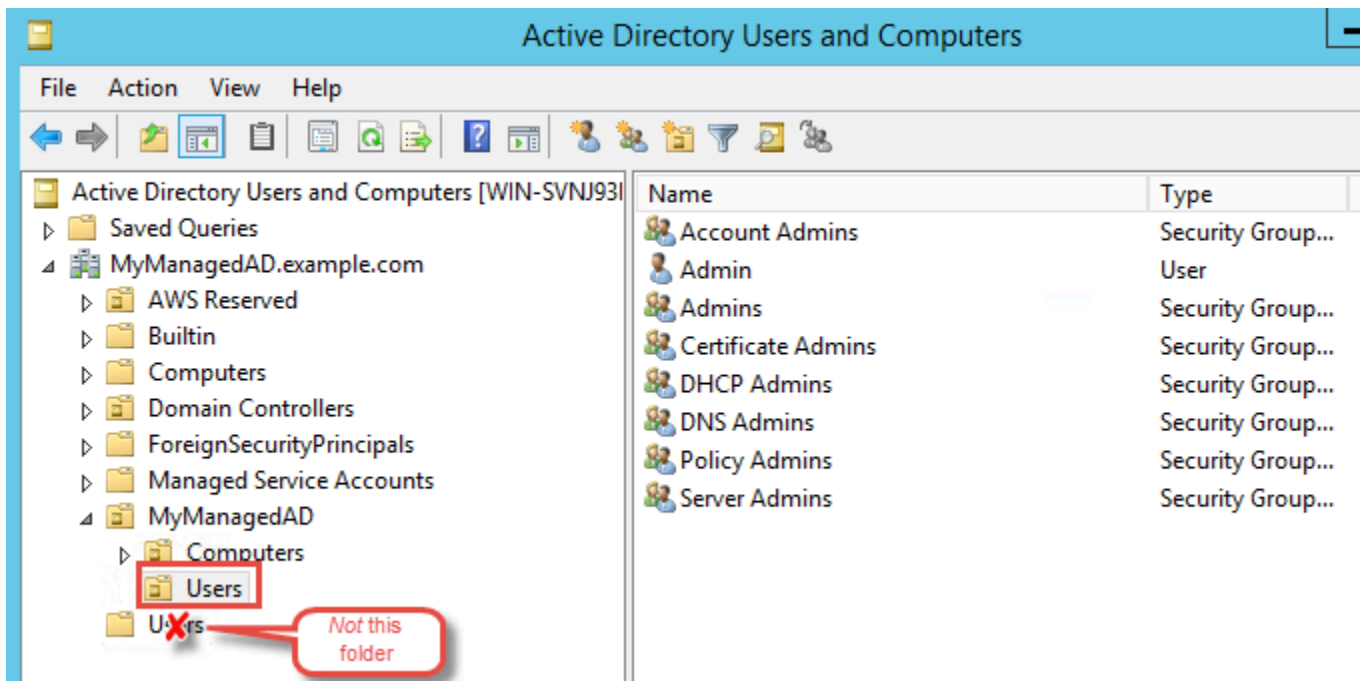


Vérification de l'activation de l'authentification préalable Kerberos

Vous voulez maintenant vérifier que la pré-authentification Kerberos est également activée pour les utilisateurs de votre Microsoft AD AWS géré. Il s'agit du même processus que celui que vous venez d'effectuer pour votre annuaire autogéré. Il s'agit de la valeur par défaut, mais nous allons vérifier que rien n'a changé.

Pour afficher les paramètres Kerberos utilisateur

1. Connectez-vous à une instance membre de votre annuaire Microsoft AD AWS géré en utilisant soit le compte correspondant au [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#) domaine, soit un compte auquel des autorisations ont été déléguées pour gérer les utilisateurs du domaine.
2. Si ce n'est pas encore fait, installez les outils Utilisateurs et ordinateurs Active Directory et DNS. Découvrez comment installer ces outils dans [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).
3. Ouvrez le Gestionnaire de serveur. Dans le menu Tools, choisissez Active Directory Users and Computers.
4. Choisissez le dossier Users dans votre domaine. Notez qu'il s'agit du dossier Users sous votre nom NetBIOS, et non du dossier Users sous le nom de domaine complet (FQDN).



5. Dans la liste des utilisateurs, cliquez avec le bouton droit sur un utilisateur, puis choisissez Propriétés (Propriétés).

6. Choisissez l'onglet Account. Dans la liste Account options, vérifiez que l'option Do not require Kerberos preauthentication n'est pas cochée.

Étape suivante

Étape 3 : créer la relation d'approbation

Étape 3 : créer la relation d'approbation

Maintenant que le travail de préparation est terminé, les étapes finales consistent à créer les approbations. Vous créez d'abord la confiance sur votre domaine autogéré, puis enfin sur votre AWS Managed Microsoft AD. Si vous avez des problèmes lors du processus de création de la relation d'approbation, veuillez consulter [Raisons liées aux statuts de création d'une relation d'approbation](#) pour obtenir de l'aide.

Configurer l'approbation dans votre annuaire Active Directory autogéré

Dans ce didacticiel, configurez une relation d'approbation de forêt bidirectionnelle. Toutefois, si vous créez une relation d'approbation de forêt unidirectionnelle, sachez que les directions d'approbation sur chacun de vos domaines doivent être complémentaires. Par exemple, si vous créez une approbation unidirectionnelle sortante sur votre domaine autogéré, vous devez créer une approbation unidirectionnelle entrante sur votre AWS Microsoft AD géré.

Note

AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt bidirectionnelle.

Pour configurer la confiance dans votre Active Directory autogéré

1. Ouvrez le Gestionnaire de serveur, puis dans le menu Tools, choisissez Active Directory Domains and Trusts.
2. Ouvrez le menu contextuel (clic droit) de votre domaine, puis choisissez Properties.
3. Choisissez l'onglet Trusts, puis choisissez New trust. Tapez le nom de votre Microsoft AD AWS géré et choisissez Next.
4. Choisissez Forest trust. Choisissez Suivant.

5. Choisissez Two-way. Choisissez Suivant.
6. Choisissez This domain only. Choisissez Suivant.
7. Choisissez Forest-wide authentication. Choisissez Suivant.
8. Saisissez un mot de passe d'approbation. N'oubliez pas ce mot de passe, car vous en aurez besoin lors de la configuration de l'approbation pour votre AWS Managed Microsoft AD.
9. Dans la boîte de dialogue suivante, confirmez vos paramètres et choisissez Next. Confirmez que la relation d'approbation a été créée avec succès, puis choisissez à nouveau Next.
10. Choisissez No, do not confirm the outgoing trust. Choisissez Suivant.
11. Choisissez No, do not confirm the incoming trust. Choisissez Suivant.

Configurez la confiance dans votre annuaire Microsoft AD AWS géré

Enfin, vous configurez la relation d'approbation de la forêt avec votre répertoire Microsoft AD AWS géré. Comme vous avez créé une approbation forestière bidirectionnelle sur le domaine autogéré, vous créez également une approbation bidirectionnelle à l'aide de votre répertoire AWS Microsoft AD géré.

 Note

Les relations de confiance sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez [Configuration de la réplication multirégionale pour AWS Managed Microsoft AD](#), les procédures suivantes doivent être effectuées dans [Région principale](#). Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Pour configurer la confiance dans votre annuaire Microsoft AD AWS géré

1. Revenez à la [console AWS Directory Service](#).
2. Sur la page Répertoires, choisissez votre identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

- Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
 5. Sur la page Ajouter une relation d'approbation, spécifiez le type de confiance. Dans ce cas, nous avons choisi Approbation de forêt. Entrez le nom de domaine complet de votre domaine autogéré (dans ce didacticiel **corp.example.com**). Tapez le même mot de passe de relation d'approbation que vous avez utilisé lors de la création de la relation d'approbation sur votre domaine autogéré. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
 6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre serveur DNS autogéré. Pour cet exemple, entrez 172.16.10.153.
 7. (Facultatif) Choisissez Ajouter une autre adresse IP, puis entrez une deuxième adresse IP pour votre serveur DNS sur site. Vous pouvez spécifier un maximum de quatre serveurs DNS.
 8. Choisissez Ajouter.

Félicitations ! Vous disposez désormais d'une relation de confiance entre votre domaine autogéré (corp.example.com) et votre AWS Microsoft AD géré (AD.example.com). MyManaged Une seule relation peut être configurée entre ces deux domaines. Si vous souhaitez par exemple passer à une direction d'approbation unidirectionnelle, vous devrez tout d'abord supprimer cette relation d'approbation existante, puis en créer une autre.

Pour plus d'informations, notamment pour obtenir les instructions de vérification ou de suppression d'une approbation, veuillez consulter [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#).

Didacticiel : créer une relation d'approbation entre deux domaines AWS Managed Microsoft AD

Ce didacticiel explique toutes les étapes nécessaires à la mise en place d'une relation d'approbation entre deux domaines AWS Directory Service for Microsoft Active Directory.

Rubriques

- [Étape 2 : préparer votre AWS Managed Microsoft AD](#)
- [Étape 2 : créer la relation de confiance avec un autre domaine Microsoft AD AWS géré](#)

Voir aussi

[Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#)

Étape 2 : préparer votre AWS Managed Microsoft AD

Dans cette section, vous préparerez votre Microsoft AD AWS géré à établir une relation de confiance avec un autre Microsoft AD AWS géré. Une grande partie des étapes suivantes est quasi-identique aux opérations que vous avez effectuées pour votre domaine dans [Didacticiel : créer une relation d'approbation entre votre AWS Managed Microsoft AD et votre domaine Active Directory](#). Toutefois, cette fois-ci, vous configurez vos environnements Microsoft AD AWS gérés pour qu'ils fonctionnent les uns avec les autres.

Configuration de vos groupes de sécurité et sous-réseaux VPC

Vous devez autoriser le trafic d'un réseau Microsoft AD AWS géré vers le VPC contenant votre autre réseau AWS Microsoft AD géré. Pour ce faire, vous devez vous assurer que les règles ACLs associées aux sous-réseaux utilisés pour déployer votre AWS Managed Microsoft AD et les règles de groupe de sécurité configurées sur vos contrôleurs de domaine autorisent le trafic requis pour soutenir les approbations.

Les exigences relatives aux ports varient en fonction de la version de Windows Server utilisée par vos contrôleurs de domaine et les services ou applications qui utiliseront l'approbation. Dans le cadre de ce didacticiel, vous devez ouvrir les ports suivants :

Entrant

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

Note

SMBv1 n'est plus pris en charge.

- TCP/UDP 464 - Authentification Kerberos
- TCP 636 - LDAPS (LDAP sur TLS/SSL)
- TCP 3268-3269 - Catalogue global
- TCP/UDP 1024-65535 - Ports éphémères pour RPC

Sortant

- ALL

Note

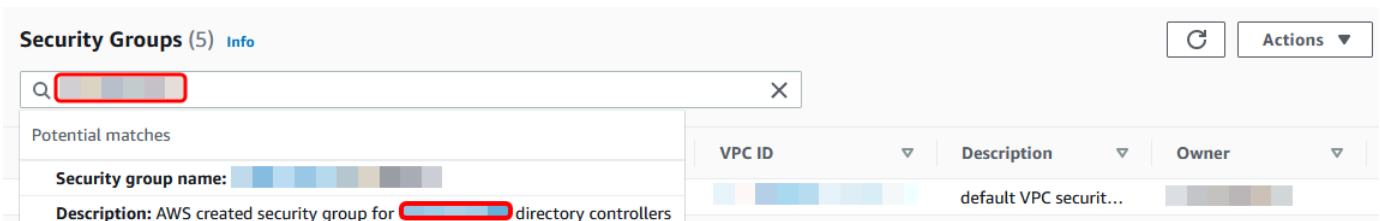
Il s'agit des ports minimaux nécessaires pour pouvoir se connecter à VPCs partir des deux AWS Managed Microsoft AD. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires. Pour en savoir plus, veuillez consulter [How to configure a firewall for Active Directory domains and trusts](#) (français non garanti) sur le site web de Microsoft.

Pour configurer les règles sortantes de votre contrôleur de domaine Microsoft AD AWS géré

Note

Répétez les étapes 1 à 6 ci-dessous pour chaque annuaire.

1. Accédez à la [console AWS Directory Service](#). Dans la liste des annuaires, notez l'ID du répertoire de votre annuaire Microsoft AD AWS géré.
2. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
3. Dans le panneau de navigation, choisissez Groupes de sécurité.
4. Utilisez le champ de recherche pour rechercher votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de recherche, sélectionnez l'élément avec la description **AWS created security group for *yourdirectoryID* directory controllers**.



5. Accédez à l'onglet Outbound Rules de ce groupe de sécurité. Choisissez Edit, puis Add another rule. Pour la nouvelle règle, saisissez les valeurs suivantes :
 - Type : ALL Traffic
 - Protocole : ALL
 - La Destination détermine le trafic qui peut quitter vos contrôleurs de domaine et où il peut aller. Indiquez une adresse IP unique ou une plage d'adresses IP dans une notation CIDR (par exemple, 203.0.113.5/32). Vous pouvez également indiquer le nom ou l'ID d'un autre groupe de sécurité dans la même région. Pour de plus amples informations, veuillez consulter [Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire](#).
6. Sélectionnez Save.

Edit outbound rules info

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules info

Security group rule ID	Type info	Protocol info	Port range info	Destination info	Description - optional info
	All traffic	All	All	Anywhere...	

0.0.0.0/0 X

Add rule

Cancel Preview changes **Save rules**

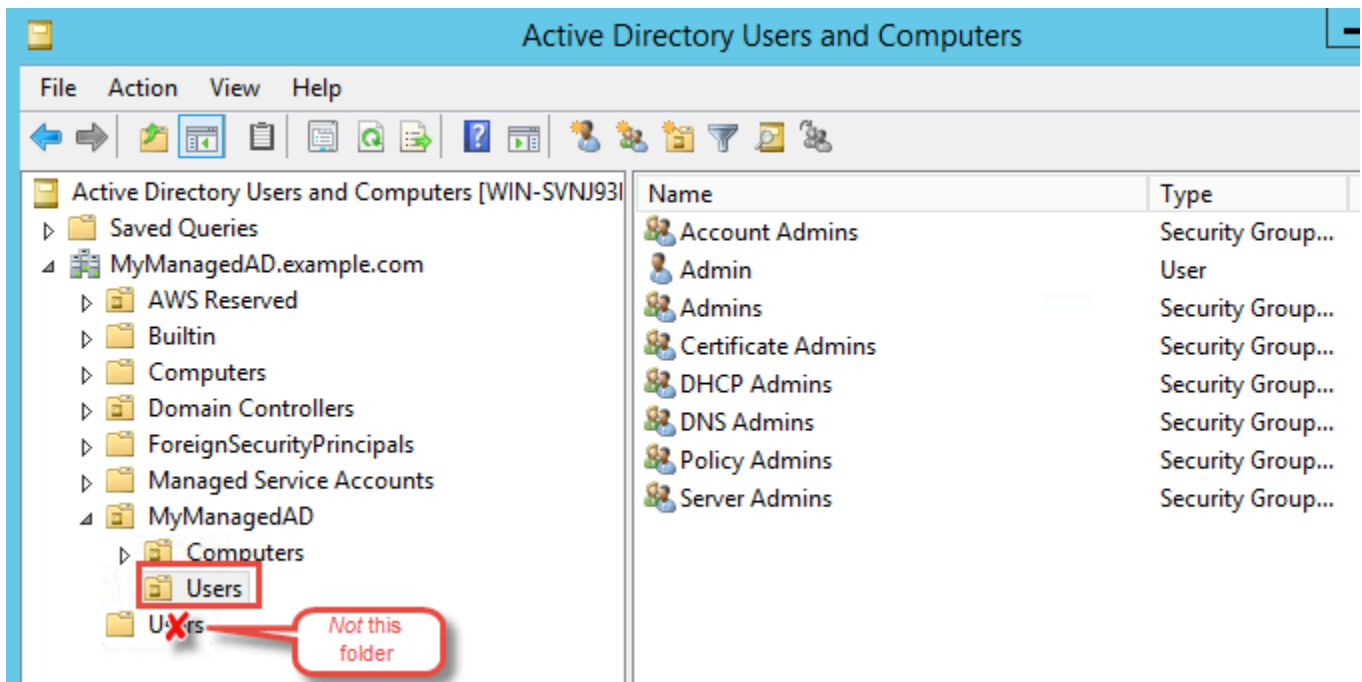
Vérification de l'activation de l'authentification préalable Kerberos

Vous voulez maintenant vérifier que la pré-authentification Kerberos est également activée pour les utilisateurs de votre Microsoft AD AWS géré. Il s'agit du même processus que celui que vous venez d'effectuer pour votre annuaire sur site. Il s'agit de la valeur par défaut, mais nous allons vérifier que rien n'a changé.

Pour afficher les paramètres Kerberos utilisateur

1. Connectez-vous à une instance membre de votre annuaire Microsoft AD AWS géré en utilisant soit le compte correspondant au [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#) domaine, soit un compte auquel des autorisations ont été déléguées pour gérer les utilisateurs du domaine.
2. Si ce n'est pas encore fait, installez les outils Utilisateurs et ordinateurs Active Directory et DNS. Découvrez comment installer ces outils dans [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

3. Ouvrez le Gestionnaire de serveur. Dans le menu Tools, choisissez Active Directory Users and Computers.
4. Choisissez le dossier Users dans votre domaine. Notez qu'il s'agit du dossier Users sous votre nom NetBIOS, et non du dossier Users sous le nom de domaine complet (FQDN).



5. Dans la liste des utilisateurs, cliquez avec le bouton droit sur un utilisateur, puis choisissez Properties (Propriétés).
6. Choisissez l'onglet Account. Dans la liste Account options, vérifiez que l'option Do not require Kerberos preauthentication n'est pas cochée.

Étape suivante

[Étape 2 : créer la relation de confiance avec un autre domaine Microsoft AD AWS géré](#)

Étape 2 : créer la relation de confiance avec un autre domaine Microsoft AD AWS géré

Maintenant que le travail de préparation est terminé, les dernières étapes consistent à créer les approbations entre vos deux domaines Microsoft AD AWS gérés. Si vous avez des problèmes lors du processus de création de la relation d'approbation, veuillez consulter [Raisons liées aux statuts de création d'une relation d'approbation](#) pour obtenir de l'aide.

Configurer la confiance dans votre premier domaine Microsoft AD AWS géré

Dans ce didacticiel, configurez une relation d'approbation de forêt bidirectionnelle. Toutefois, si vous créez une relation d'approbation de forêt unidirectionnelle, sachez que les directions d'approbation sur chacun de vos domaines doivent être complémentaires. Par exemple, si vous créez une approbation sortante unidirectionnelle sur ce premier domaine, vous devez créer une approbation unidirectionnelle entrante sur votre deuxième domaine AWS Microsoft AD géré.

Note

AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt bidirectionnelle.

Pour configurer la confiance dans votre premier domaine Microsoft AD AWS géré

1. Ouvrez la [AWS Directory Service console](#).
2. Sur la page Répertoires, choisissez votre premier identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation de confiance, saisissez le nom de domaine complet de votre deuxième domaine Microsoft AD AWS géré. N'oubliez pas ce mot de passe, car vous en aurez besoin lors de la configuration de la confiance pour votre deuxième AWS Managed Microsoft AD. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre deuxième serveur DNS Microsoft AD AWS géré.
7. (Facultatif) Choisissez Ajouter une autre adresse IP et entrez une deuxième adresse IP pour votre deuxième serveur DNS Microsoft AD AWS géré. Vous pouvez spécifier un maximum de quatre serveurs DNS.

8. Choisissez Ajouter. L'approbation échouera à ce stade, ce qui est prévisible jusqu'à ce que nous ayons créé l'autre côté de l'approbation.

Configurer la confiance dans votre deuxième domaine Microsoft AD AWS géré

À présent, vous configurez la relation d'approbation de la forêt avec votre deuxième annuaire Microsoft AD AWS géré. Comme vous avez créé une approbation forestière bidirectionnelle sur le premier domaine Microsoft AD AWS géré, vous créez également une approbation bidirectionnelle à l'aide de ce domaine AWS Microsoft AD géré.

Pour configurer la confiance dans votre deuxième domaine Microsoft AD AWS géré

1. Revenez à la [console AWS Directory Service](#).
2. Sur la page Répertoires, choisissez votre deuxième identifiant Microsoft AD AWS géré.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Sur la page Ajouter une relation de confiance, saisissez le nom de domaine complet de votre premier domaine Microsoft AD AWS géré. Tapez le même mot de passe de relation d'approbation que vous avez utilisé lors de la création de la relation d'approbation sur votre domaine sur site. Spécifiez la direction. Dans ce cas, nous choisissons Bidirectionnelle.
6. Dans le champ Redirecteur conditionnel, entrez l'adresse IP de votre premier serveur DNS AWS Managed Microsoft AD.
7. (Facultatif) Choisissez Ajouter une autre adresse IP et entrez une deuxième adresse IP pour votre premier serveur DNS Microsoft AD AWS géré. Vous pouvez spécifier un maximum de quatre serveurs DNS.
8. Choisissez Ajouter. L'approbation doit être vérifiée peu de temps après.
9. Revenez maintenant à l'approbation que vous avez créée dans le premier domaine et vérifiez à nouveau la relation d'approbation.

Félicitations ! Vous disposez désormais d'une relation de confiance entre vos deux domaines Microsoft AD AWS gérés. Une seule relation peut être configurée entre ces deux domaines. Si vous souhaitez par exemple passer à une direction d'approbation unidirectionnelle, vous devrez tout d'abord supprimer cette relation d'approbation existante, puis en créer une autre.

Étendez votre schéma AWS Managed Microsoft AD

AWS Managed Microsoft AD utilise des schémas pour organiser et appliquer le mode de stockage des données d'annuaire. Le processus d'ajout de définitions au schéma est appelé « extension du schéma ». Les extensions de schéma vous permettent de modifier le schéma de votre annuaire Microsoft AD AWS géré à l'aide d'un fichier LDIF (LDAP Data Interchange Format) valide. Pour plus d'informations sur les schémas AD et comment étendre votre schéma, veuillez consulter les rubriques ci-dessous.

Quand étendre votre schéma AWS Managed Microsoft AD

Vous pouvez étendre votre schéma AWS Managed Microsoft AD en ajoutant de nouvelles classes d'objets et de nouveaux attributs. Par exemple, vous pouvez exécuter cette action si vous disposez d'une application qui nécessite d'apporter des modifications à votre schéma afin de prendre en charge les fonctions d'authentification unique.

Vous pouvez également utiliser des extensions de schéma pour activer la prise en charge des applications qui reposent sur des attributs et classes d'objet Active Directory spécifiques. Cela peut être particulièrement utile dans le cas où vous devez migrer des applications d'entreprise qui dépendent de AWS Managed Microsoft AD vers le AWS cloud.

Chaque attribut ou classe ajouté(e) à un schéma Active Directory existant doit être défini(e) avec un ID unique. De cette manière, lorsque les entreprises ajoutent des extensions au schéma, ces dernières sont assurées d'être uniques et de ne pas entrer en conflit les unes avec les autres. Ils IDs sont appelés identificateurs d'objets AD (OIDs) et sont stockés dans AWS Managed Microsoft AD.

Consultez [Tutoriel : extension de votre schéma Microsoft AD AWS géré](#) pour démarrer.

Rubriques en relation

- [Étendez votre schéma AWS Managed Microsoft AD](#)
- [Éléments du schéma](#)

Rubriques

- [Tutoriel : extension de votre schéma Microsoft AD AWS géré](#)

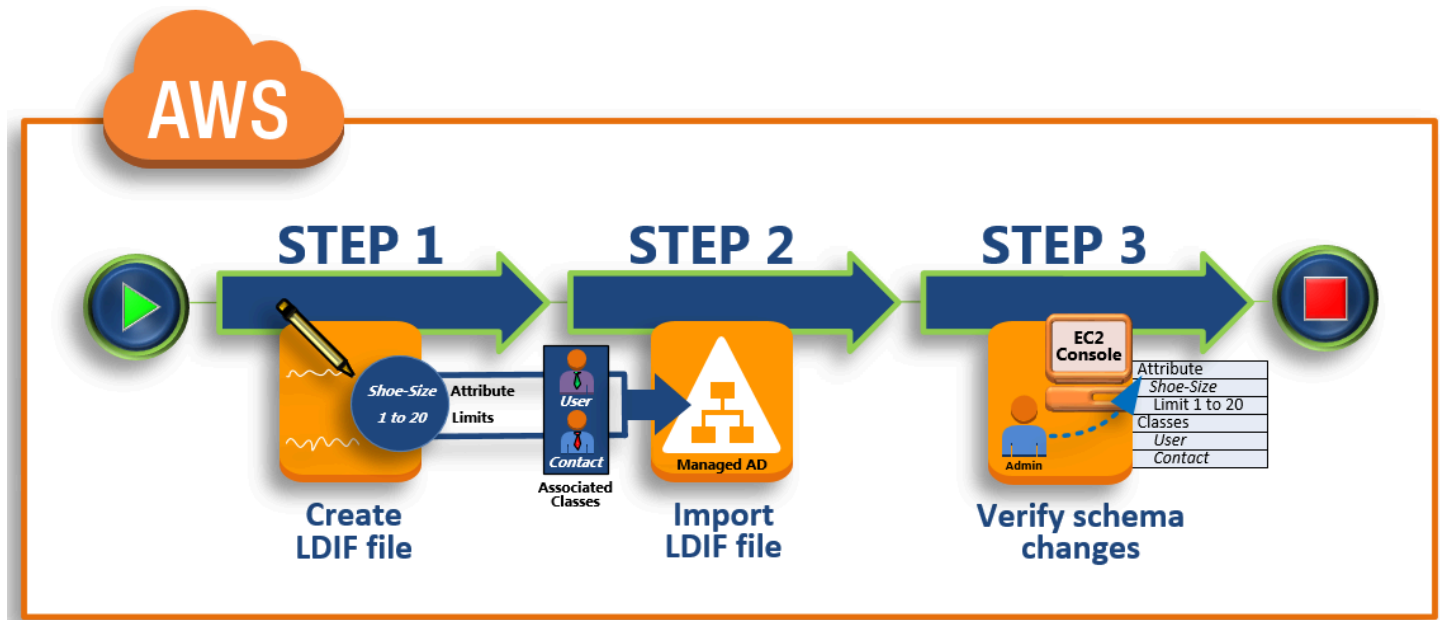
Tutoriel : extension de votre schéma Microsoft AD AWS géré

Dans ce didacticiel, vous allez apprendre à étendre le schéma de votre AWS annuaire Directory Service for Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD, en ajoutant des attributs et des classes uniques répondant à vos besoins spécifiques. AWS Les extensions de schéma Microsoft AD gérées ne peuvent être téléchargées et appliquées qu'à l'aide d'un fichier de script LDIF (Lightweight Directory Interchange Format) valide.

Les attributs (attributeSchema) définissent les champs de la base de données, tandis que les classes (classSchema) définissent les tables de la base de données. Par exemple, tous les objets utilisateur dans Active Directory sont définis par la classe de schéma Utilisateur, tandis que les propriétés individuelles d'un utilisateur, telles que l'adresse e-mail ou le numéro de téléphone, sont chacune définies par un attribut.

Si vous souhaitez ajouter une nouvelle propriété, telle que la taille de chaussure, vous définissez un nouvel attribut, qui serait de type entier. Vous pouvez également définir des limites inférieure et supérieure allant de 1 à 20. Une fois que l'objet attributeSchema taille de chaussure a été créé, vous modifiez ensuite l'objet classSchema Utilisateur pour contenir cet attribut. Les attributs peuvent être liés à plusieurs classes. La taille de chaussure peut être ajoutée à la classe Contact par exemple. Pour plus d'informations sur les schémas Active Directory, veuillez consulter [Quand étendre votre schéma AWS Managed Microsoft AD](#).

Ce flux de travail se compose de trois étapes de base.



Étape 1 : créer votre fichier LDIF

Tout d'abord, vous créez un fichier LDIF et définissez les nouveaux attributs et les classes auxquelles ils doivent être ajoutés. Vous utilisez ce fichier pour la prochaine étape du flux de travail.

Étape 2 : importer votre fichier LDIF

Au cours de cette étape, vous devez utiliser la AWS Directory Service console pour importer le fichier LDIF dans votre environnement Microsoft Active Directory.

Étape 3 : vérifier si l'extension de schéma a réussi

Enfin, en tant qu'administrateur, vous utilisez une EC2 instance pour vérifier que les nouvelles extensions apparaissent dans le composant logiciel enfichable du schéma Active Directory.

Étape 1 : créer votre fichier LDIF

Un fichier LDIF est un format d'échange de données standard en texte brut qui représente le contenu de l'annuaire [LDAP](#) (Lightweight Directory Access Protocol) et les demandes de mise à jour. LDIF transmet le contenu de l'annuaire en tant qu'ensemble d'enregistrements, un enregistrement pour chaque objet (ou entrée). Il représente également des demandes de mise à jour, comme Ajouter, Modifier, Supprimer et Renommer en tant qu'ensemble d'enregistrements, un enregistrement pour chaque demande de mise à jour.

AWS Directory Service importe ensuite votre fichier LDIF avec les modifications de schéma en exécutant l'`ldifde.exe` application sur votre répertoire AWS Microsoft AD géré. Il vous sera donc utile de comprendre la syntaxe du script LDIF. Pour plus d'informations, veuillez consulter [LDIF Scripts](#) (français non garanti).

Plusieurs outils LDIF tiers peuvent extraire, nettoyer et mettre à jour vos mises à jour de schéma. Quel que soit l'outil utilisé, vous devez comprendre que tous les identificateurs utilisés dans votre fichier LDIF doivent être uniques.

Nous vous recommandons vivement d'examiner les concepts et conseils suivants avant de créer votre fichier LDIF.

- **Éléments de schéma** : découvrez les éléments de schéma tels que les attributs, les classes, les objets IDs et les attributs liés. Pour de plus amples informations, veuillez consulter [Éléments du schéma](#).
- **Séquence d'éléments** : veillez à ce que l'ordre dans lequel les éléments de votre fichier LDIF sont disposés respecte le [Directory Information Tree \(DIT\)](#) de haut en bas. Les règles générales pour effectuer le séquençage d'un fichier LDIF incluent les éléments suivants :
 - Séparer les éléments par une ligne vide.
 - Répertorier les éléments enfants en fonction de leurs éléments parents.
 - Veillez à ce que des éléments tels que des attributs ou des classes d'objet existent dans le schéma. S'ils ne sont pas présents, vous devez les ajouter au schéma avant qu'ils puissent être utilisés. Par exemple, avant que vous puissiez assigner un attribut à une classe, ce dernier doit être créé.
- **Format du DN** : pour chaque nouvelle instruction dans le fichier LDIF, définissez le nom unique (DN) en tant que première ligne de l'instruction. Le DN identifie un objet Active Directory dans l'arborescence de l'objet Active Directory et doit contenir les composants de domaine de votre annuaire. Par exemple, les composants du domaine pour l'annuaire dans ce didacticiel sont `DC=example,DC=com`.

Le DN doit inclure le nom commun (CN) de l'objet Active Directory. La première entrée CN représente le nom de l'attribut ou de la classe. Pour étendre le schéma Active Directory, utilisez `CN=Schema,CN=Configuration`. N'oubliez pas que vous ne pouvez pas modifier le contenu des objets Active Directory. Le format DN général est le suivant.

```
dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
```

Pour ce didacticiel, le DN pour le nouvel attribut taille de chaussure ressemblerait à :

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- Avertissements – Examinez les avertissements avant d'étendre votre schéma.
 - Avant d'étendre votre schéma Active Directory, il est important d'examiner les avertissements de Microsoft sur l'impact de cette opération. Pour plus d'informations, veuillez consulter [What You Must Know Before Extending the Schema](#) (français non garanti).
 - Vous ne pouvez pas supprimer un attribut ou une classe de schéma. Par conséquent, si vous faites une erreur et que vous ne souhaitez pas effectuer de restauration à partir d'une sauvegarde, vous pouvez uniquement désactiver l'objet. Pour plus d'informations, veuillez consulter [Disabling Existing Classes and Attributes](#) (français non garanti).
 - Les modifications apportées à ne defaultSecurityDescriptor sont pas prises en charge.

Pour en savoir plus sur le mode de construction des fichiers LDIF et consulter un exemple de fichier LDIF pouvant être utilisé pour tester les extensions de schéma AWS Microsoft AD gérées, consultez l'article [Comment étendre votre schéma de répertoire AWS Microsoft AD géré sur le blog de sécurité AWS](#)

Étape suivante

[Étape 2 : importer votre fichier LDIF](#)

Étape 2 : importer votre fichier LDIF

Vous pouvez étendre votre schéma en important un fichier LDIF depuis la AWS Directory Service console ou à l'aide de l'API. Pour plus d'informations sur la procédure à suivre avec l'extension de schéma APIs, consultez la [référence AWS Directory Service d'API](#). Pour l'instant, AWS ne prend pas en charge les applications externes, telles que Microsoft Exchange, pour effectuer directement les mises à jour de schéma.

Important

Lorsque vous mettez à jour votre schéma d'annuaire Microsoft AD AWS géré, l'opération n'est pas réversible. En d'autres termes, une fois que vous avez créé une nouvelle classe ou

un nouvel attribut, Active Directory ne vous permet pas de le supprimer. Cependant, vous pouvez la ou le désactiver.

Si vous devez supprimer les modifications de schéma, une option consiste à restaurer l'annuaire à partir d'un instantané précédent. La restauration d'un instantané restaure à la fois le schéma et les données de l'annuaire à un point précédent, pas uniquement le schéma.

Remarque : la durée maximale prise en charge pour un instantané est de 180 jours. Pour plus d'informations, veuillez consulter la section [Useful shelf life of a system-state backup of Active Directory](#) (français non garanti) sur le site web Microsoft.

Avant le début du processus de mise à jour, AWS Managed Microsoft AD prend un instantané pour conserver l'état actuel de votre annuaire.

Note

Les extensions de schéma sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez [Configuration de la réplication multirégionale pour AWS Managed Microsoft AD](#), les procédures suivantes doivent être effectuées dans [Région principale](#). Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Pour importer votre fichier LDIF

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Maintenance. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Maintenance.
4. Dans la section Schema extensions (Extensions de schéma), choisissez Actions, puis sélectionnez Upload and update schema (Charger et mettre à jour le schéma).

5. Dans la boîte de dialogue, cliquez sur Parcourir, sélectionnez un fichier LDIF valide, saisissez une description, puis choisissez Update Schema.

 Important

L'extension du schéma est une opération critique. N'appliquez aucune mise à jour de schéma dans un environnement de production sans l'avoir d'abord testée avec votre application dans un environnement de développement ou de test.

Comment le fichier LDIF est appliqué

Une fois votre fichier LDIF chargé, Managed AWS Microsoft AD prend des mesures pour protéger votre répertoire contre les erreurs en appliquant les modifications dans l'ordre suivant.

1. Valide le fichier LDIF. Étant donné que les scripts LDIF peuvent manipuler n'importe quel objet du domaine, AWS Managed Microsoft AD effectue des vérifications juste après le téléchargement pour s'assurer que l'opération d'importation n'échouera pas. Ces vérifications garantissent les points suivants :
 - Les objets à mettre à jour se trouvent uniquement dans le conteneur de schéma
 - La partie des DC (contrôleurs de domaine) correspond au nom du domaine dans lequel le script LDIF est en cours d'exécution
2. Prend un instantané de votre annuaire. Vous pouvez utiliser l'instantané pour restaurer votre annuaire au cas où vous rencontrez des problèmes avec votre application après la mise à jour du schéma.
3. Applique les modifications à un seul DC. AWS Managed Microsoft AD isole l'un de vos contrôleurs DCs et applique les mises à jour du fichier LDIF au contrôleur de domaine isolé. Il sélectionne ensuite l'un de vos DCs schémas comme schéma principal, supprime ce contrôleur de domaine de la réplication de répertoire et applique votre fichier LDIF à l'aide de `Ldifde.exe`
4. La réplication s'applique à tous DCs. AWS Managed Microsoft AD réintègre le contrôleur de domaine isolé à la réplication pour terminer la mise à jour. Pendant ce temps, votre annuaire continue de fournir l'Active Directory Service à vos applications sans interruption.

Étape suivante

[Étape 3 : vérifier si l'extension de schéma a réussi](#)

Étape 3 : vérifier si l'extension de schéma a réussi

Lorsque vous avez terminé le processus d'importation, il est important de vérifier que les mises à jour de schéma ont été appliquées à votre annuaire. Cette étape est particulièrement importante avant de migrer ou mettre à jour toute application s'appuyant sur la mise à jour de schéma. Pour ce faire, utilisez différents outils LDAP ou écrivez un outil de test qui émet les commandes LDAP appropriées.

Cette procédure utilise le composant logiciel enfichable du schéma Active Directory and/or PowerShell pour vérifier que les mises à jour du schéma ont été appliquées. Vous devez exécuter ces outils à partir d'un ordinateur joint au domaine à votre AWS Managed Microsoft AD. Il peut s'agir d'un serveur Windows en cours d'exécution dans votre réseau sur site avec accès à votre Virtual Private Cloud (VPC) ou via une connexion de réseau privé virtuel (VPN). Vous pouvez également exécuter ces outils sur une instance Amazon EC2 Windows (voir [Comment lancer une nouvelle EC2 instance avec une jointure de domaine fluide](#)).

Pour vérifier à l'aide du composant logiciel enfichable du schéma Active Directory

1. Installez le composant logiciel enfichable du schéma Active Directory en suivant les instructions du site [TechNetWeb](#).
2. Ouvrez la Microsoft Management Console (MMC) et développez l'arborescence Schéma AD pour votre annuaire.
3. Parcourez les dossiers Classes et Attributs jusqu'à ce que vous trouviez les modifications de schéma que vous avez fait précédemment.

Pour vérifier en utilisant PowerShell

1. Ouvrez une PowerShell fenêtre.
2. Utilisez l'applet de commande Get-ADObject comme illustré ci-dessous pour vérifier la modification de schéma. Par exemple :

```
get-adobject -Identity 'CN=Shoe-  
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

Étape facultative

[Ajouter une valeur au nouvel attribut - Facultatif](#)

Ajouter une valeur au nouvel attribut - Facultatif

Utilisez cette étape facultative lorsque vous avez créé un nouvel attribut et que vous souhaitez ajouter une nouvelle valeur à l'attribut dans votre annuaire Microsoft AD AWS géré.

Pour ajouter une valeur à un attribut

1. Ouvrez l'utilitaire de ligne de PowerShell commande et définissez le nouvel attribut à l'aide de la commande suivante. Dans cet exemple, nous allons ajouter une nouvelle valeur EC2 InstanceID à l'attribut d'un ordinateur spécifique.

```
PS C:\> set-adcomputer -Identity computer name -add @{example-  
EC2InstanceID = 'EC2 instance ID'}
```

2. Vous pouvez vérifier si la valeur EC2 InstanceID a été ajoutée à l'objet ordinateur en exécutant la commande suivante :

```
PS C:\> get-adcomputer -Identity computer name -Property example-  
EC2InstanceID
```

Ressources connexes

Les liens de ressource suivants se trouvent sur le site web Microsoft et fournissent des informations connexes.

- [Extension du schéma \(Windows\)](#)
- [Schéma Active Directory \(Windows\)](#)
- [Schéma Active Directory](#)
- [Administration Windows : Extension du schéma Active Directory](#)
- [Restrictions sur l'extension du schéma \(Windows\)](#)
- [Ldifde](#)

Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré

Vous pouvez facilement joindre une EC2 instance Amazon à votre domaine Active Directory lorsque l'instance est lancée. Pour de plus amples informations, veuillez consulter [Joindre une instance](#)

[Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#). Vous pouvez également lancer une EC2 instance et la joindre à un domaine Active Directory directement depuis la Directory Service console avec [AWS Systems Manager Automation](#).

Si vous devez joindre manuellement une EC2 instance à votre domaine Active Directory, vous devez lancer l'instance dans la région et le groupe de sécurité ou le sous-réseau appropriés, puis joindre l'instance au domaine.

Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela nécessite qu'une passerelle Internet soit attachée à votre VPC et que l'instance possède une adresse IP publique.

Rubriques

- [Lancement d'une instance d'administration d'annuaire dans votre annuaire Microsoft AD Active Directory AWS géré](#)
- [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#)
- [Joindre une instance Amazon EC2 Linux à votre annuaire Microsoft AD Active Directory AWS géré](#)
- [Joindre une instance Amazon EC2 Mac à votre annuaire Microsoft AD Active Directory AWS géré](#)
- [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#)
- [Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD](#)

Lancement d'une instance d'administration d'annuaire dans votre annuaire Microsoft AD Active Directory AWS géré

Cette procédure lance une Windows instance d'administration d' EC2 annuaires Amazon en AWS Management Console utilisant AWS Systems Manager Automation pour gérer vos annuaires. Vous pouvez également y parvenir en exécutant directement l'automatisation [AWS-Create DSManagement Instance](#) dans la console AWS Systems Manager Automation.

Pour plus d'informations, consultez les liens suivants :

- [Simplification de la jonction de domaines Active Directory avec AWS Systems Manager](#)
- [Comment puis-je joindre une EC2 Windows instance en cours d'exécution à mon Directory Service domaine ? AWS Systems Manager](#)

Prérequis

Les prérequis suivants sont requis pour suivre ce didacticiel :

- Vous devrez configurer AWS Systems Manager. Pour plus d'informations, consultez [Configuration AWS Systems Manager](#).
- Vous aurez besoin d'un [rôle de profil d'instance IAM](#) qui autorise Systems Manager et AWS Managed Microsoft AD.
 - Pour plus d'informations sur Systems Manager, consultez [Configurer les autorisations d'instance requises pour Systems Manager](#).
 - Le rôle d'instance IAM nécessite les politiques AWS gérées suivantes afin que votre Windows instance d'administration d' EC2annuaire puisse rejoindre le domaine de votre Microsoft AD AWS géré :
 - **AmazonSSMManagedInstanceCore**
 - **AmazonSSMDirectoryServiceAccess**
- Le VPC connecté à votre AWS Microsoft AD géré doit autoriser l'accès aux points de terminaison publics Directory Service . Pour de plus amples informations, veuillez consulter [Conditions préalables à la création d'un Microsoft AWS AD géré](#).
- Les autorisations suivantes doivent être activées dans votre compte pour lancer une EC2 instance d'administration d'annuaire depuis la console :
 - ds:DescribeDirectories
 - ec2:AuthorizeSecurityGroupIngress
 - ec2:CreateSecurityGroup
 - ec2:CreateTags
 - ec2>DeleteSecurityGroup
 - ec2:DescribeInstances
 - ec2:DescribeInstanceStatus
 - ec2:DescribeKeyPairs
 - ec2:DescribeSecurityGroups
 - ec2:DescribeVpcs
 - ec2:RunInstances
 - ec2:TerminateInstances
 - **iam:AddRoleToInstanceProfile**

- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam>DeleteInstanceProfile
- iam>DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm>DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:GetDocument

Lancement d'une EC2 instance d'administration d'annuaire dans le AWS Management Console

1. Connectez-vous à la [console Directory Service](#).

2. Sous Active Directory, sélectionnez Directories (Annuaire).
3. Choisissez l'ID du répertoire dans lequel vous souhaitez lancer une EC2 instance d'administration d'annuaire.
4. Sur la page de l'annuaire, dans le coin supérieur droit, sélectionnez Actions.
5. Dans la liste déroulante Actions, choisissez Launch directory administration EC2 instance.
6. Sur la page Launch directory administration EC2 instance, sous Paramètres d'entrée, complétez les champs.
 - a. (Facultatif) Vous pouvez fournir une paire de clés pour l'instance. Dans la liste déroulante Nom de la paire de clés - facultatif, sélectionnez une paire de clés.
 - b. (Facultatif) Choisissez la AWS CLI commande Afficher pour voir un exemple que vous utilisez AWS CLI pour exécuter cette automatisation.
7. Sélectionnez Envoyer.
8. Vous êtes renvoyé à la page d'annuaire. Une barre de progression verte s'affiche en haut de votre écran pour indiquer que vous avez réussi le lancement.

Affichage d'une EC2 instance d'administration d'annuaire

Si vous n'avez lancé aucune EC2 instance pour un répertoire, un tiret (-) s'affiche sous EC2Instance d'administration du répertoire.

1. Sous Active Directory, choisissez Directories (Annuaire) et sélectionnez l'annuaire que vous souhaitez consulter.
2. Sous Détails du répertoire, sous EC2 Instance d'administration du répertoire, choisissez l'une ou l'ensemble de vos instances à afficher.
3. Lorsque vous choisissez une instance, vous êtes redirigé vers la page EC2 Connect to instance pour connecter un poste de travail distant à votre instance.

Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré

Vous pouvez lancer et joindre une EC2 Windows instance Amazon à un Microsoft AD AWS géré. Vous pouvez également joindre manuellement une EC2 Windows instance existante à un Microsoft AD AWS géré.

Seamlessly join EC2 Windows instance

Cette procédure permet de joindre facilement une EC2 Windows instance Amazon à votre Microsoft AD AWS géré. Si vous devez effectuer une jointure fluide entre plusieurs domaines Comptes AWS, consultez [Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de EC2 domaine fluide](#). Pour plus d'informations sur Amazon EC2, consultez [Qu'est-ce qu'Amazon EC2 ?](#).

Prérequis

Pour joindre facilement un domaine à une EC2 instance, vous devez effectuer les opérations suivantes :

- Disposez d'un Microsoft AD AWS géré. Pour en savoir plus, veuillez consulter la section [Création de votre AWS compte Microsoft AD géré](#).
- Vous aurez besoin des autorisations IAM suivantes pour rejoindre facilement une EC2 Windows instance :
 - Profil d'instance IAM avec les autorisations IAM suivantes :
 - AmazonSSManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Le domaine utilisateur qui rejoint facilement EC2 le domaine Microsoft AWS AD doit disposer des autorisations IAM suivantes :
 - Directory Service Autorisations :
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Autorisations Amazon VPC :
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - EC2 Autorisations :
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"

- "ec2:RunInstances"
- "ec2:CreateTags"
- AWS Systems Manager Autorisations :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Lorsque votre AWS Managed Microsoft AD est créé, un groupe de sécurité est créé avec des règles entrantes et sortantes. Pour en savoir plus sur ces règles et ces ports, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#). Pour joindre facilement un domaine à une EC2 Windows instance, le VPC sur lequel vous lancez votre instance doit autoriser les mêmes ports autorisés dans les règles entrantes et sortantes de votre groupe de sécurité AWS Microsoft AD géré.

- Selon les paramètres de sécurité et de pare-feu de votre réseau, il peut vous être demandé d'autoriser un trafic sortant supplémentaire. Ce trafic serait destiné au protocole HTTPS (port 443) vers les points de terminaison suivants :

Point de terminaison	Rôle
ec2messages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ssm. <i>region</i> .amazonaws.com	Endpoint pour AWS Systems Manager Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ssmmessages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .

Point de terminaison	Rôle
ds. <i>region</i> .amazonaws.com	Endpoint pour Directory Service. Pour de plus amples informations, veuillez consulter Disponibilité de la région pour Directory Service .

- Nous vous recommandons d'utiliser un serveur DNS qui résoudra votre nom de domaine Microsoft AD AWS géré. Pour ce faire, vous pouvez créer un jeu d'options DHCP. Pour plus d'informations, consultez [Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD](#).
- Si vous choisissez de ne pas créer de jeu d'options DHCP, vos serveurs DNS seront statiques et configurés par votre AWS Managed Microsoft AD.

Pour rejoindre facilement une EC2 Windows instance Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Windows.
5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.
6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).
7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.
 - a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.

- b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.
- c. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez .pem. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez .ppk.
- d. Choisissez Créer une paire de clés.
- e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

**Important**

C'est votre seule occasion d'enregistrer le fichier de clé privée.

- 9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
- 10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

- 11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

- 12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
- 13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
- 14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

 Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM SSMDirectory ServiceAccess auquel sont associées les politiques AWS gérées Amazon SSMManaged InstanceCore et Amazon dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :
 1. Choisissez Créer un rôle.
 2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
 3. Sous Use case (Cas d'utilisation), choisissez EC2.
 4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les SSMDirectory ServiceAccess politiques Amazon SSMManaged InstanceCore et Amazon. Pour filtrer la liste, tapez **SSM** dans la zone de recherche. Choisissez Suivant.

 Note

Amazon SSMDirectory ServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. Amazon SSMManged InstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section [Create an IAM instance profile for Systems Manager](#) (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'associer à l' EC2instance.
 6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
 7. Choisissez Créer un rôle.
 8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.
16. Choisissez Launch instance (Lancer une instance).

Manually join EC2 Windows instance

Pour joindre manuellement une EC2 Windows instance Amazon existante à un répertoire Microsoft AD Active Directory AWS géré, l'instance doit être lancée à l'aide des paramètres spécifiés dans [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).

Vous aurez besoin des adresses IP des serveurs DNS Microsoft AD AWS gérés. Ces informations se trouvent sous Directory Services (Services d'annuaire) > Directories (Annuaire) > le lien Directory ID (ID de l'annuaire) de votre annuaire > Directory details (Détails de l'annuaire) puis les sections Networking & Security Réseau et sécurité.

The screenshot shows the AWS Directory Service console. On the left, the 'Directory Service' sidebar is visible with 'Directories' highlighted. The main content area shows the details for directory 'd-1234567890'. The 'Directory details' section includes:

Property	Value
Directory type	Microsoft AD
Edition	Standard
Operating system version	Windows Server 2019
Directory DNS name	corp.example.com
Directory NetBIOS name	corp
Directory administration EC2 instance(s)	-

Below this, the 'Networking details' section is shown, which includes a VPC and subnets. The 'DNS address' for the subnets is listed as 192.0.2.1 and 198.51.100.1.

Pour joindre une instance Windows à un répertoire Microsoft AD Active Directory AWS géré

1. Connectez-vous à l'instance à l'aide d'un client RDP (Remote Desktop Protocol).
2. Ouvrez la boîte de dialogue IPv4 des propriétés TCP/ sur l'instance.
 - a. Ouvrez Network Connections (Connexions réseau).

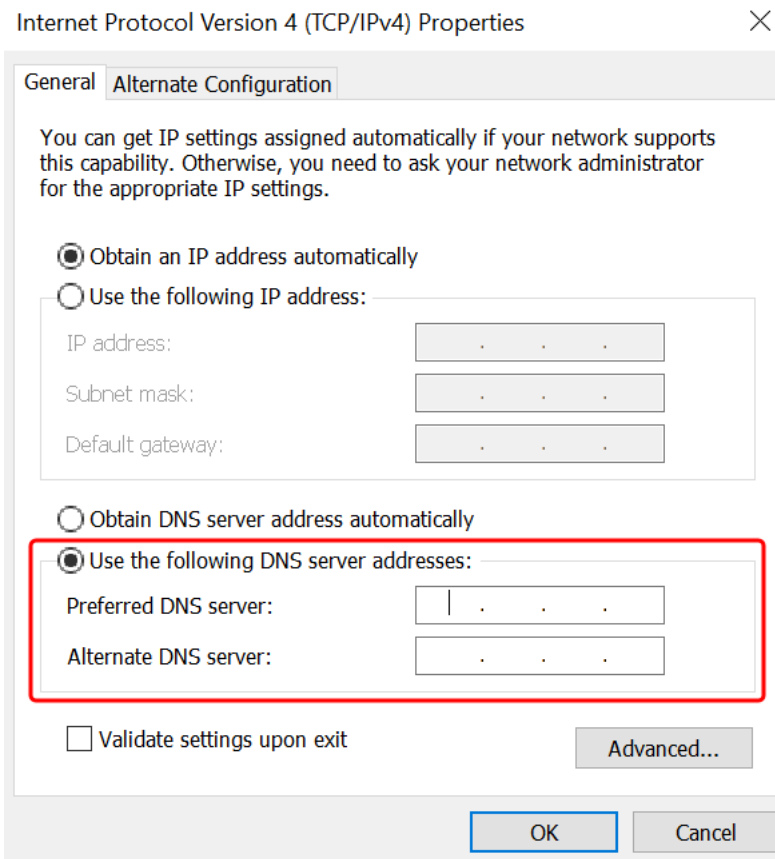
Tip

Vous pouvez ouvrir Network Connections (Connexions réseau) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. Ouvrez le menu contextuel (clic droit) pour toute connexion de réseau active, puis choisissez Properties (Propriétés).
- c. Dans la boîte de dialogue des propriétés de connexion, ouvrez (double-cliquez) Internet Protocol version 4.

3. Sélectionnez Utiliser les adresses de serveur DNS suivantes, remplacez les adresses du serveur DNS préféré et du serveur DNS secondaire par les adresses IP de vos serveurs DNS AWS gérés par Microsoft AD, puis cliquez sur OK.



4. Ouvrez la boîte de dialogue System Properties (Propriétés système) de l'instance, sélectionnez l'onglet Computer Name (Nom de l'ordinateur), puis choisissez Change (Modifier).

i Tip

Vous pouvez ouvrir la boîte de dialogue System Properties (Propriétés du système) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. Dans le champ Membre de, sélectionnez Domaine, entrez le nom complet de votre annuaire Microsoft AD Active Directory AWS géré, puis cliquez sur OK.
6. Lorsque vous êtes invité à saisir le nom et le mot de passe de l'administrateur du domaine, entrez le nom d'utilisateur et le mot de passe d'un compte doté de privilèges de connexion

au domaine. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

 Note

Vous pouvez saisir le nom complet de votre domaine ou le nom NetBIOS, suivi d'une barre oblique inverse (\), puis du nom d'utilisateur. Le nom d'utilisateur serait Admin. Par exemple, **corp.example.com\admin** ou **corp\admin**.

7. Après avoir reçu le message de bienvenue dans le domaine, redémarrez l'instance pour que les modifications prennent effet.

Maintenant que votre instance a été jointe au domaine Microsoft AD Active Directory AWS géré, vous pouvez vous connecter à distance à cette instance et installer des utilitaires pour gérer le répertoire, tels que l'ajout d'utilisateurs et de groupes. Les outils d'administration Active Directory peuvent être utilisés pour créer des utilisateurs et des groupes. Pour de plus amples informations, veuillez consulter [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

 Note

Vous pouvez également utiliser Amazon Route 53 pour traiter les requêtes DNS au lieu de modifier manuellement les adresses DNS de vos EC2 instances Amazon. Pour plus d'informations, voir [Intégration de la résolution DNS de votre service d'annuaire à votre réseau Amazon Route 53 Resolver](#) et [transfert de requêtes DNS sortantes vers votre réseau](#).

Joindre une instance Amazon EC2 Linux à votre annuaire Microsoft AD Active Directory AWS géré

Vous pouvez lancer et joindre une instance EC2 Linux à votre AWS Managed Microsoft AD dans le AWS Management Console. Vous pouvez également joindre manuellement une instance EC2 Linux à votre AWS Managed Microsoft AD. Des outils tels que Winbind peuvent également être utilisés pour joindre un domaine à une instance EC2 Linux à votre AWS Managed Microsoft AD.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

 Note

Les distributions antérieures à Ubuntu 14 et à Red Hat Enterprise Linux 7 et 8 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Méthodes pour joindre un domaine à une instance EC2 Linux :

- [Joindre facilement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré](#)
- [Joindre facilement une instance Amazon EC2 Linux à un Microsoft AD AWS géré partagé](#)
- [Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré](#)
- [Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré à l'aide de Winbind](#)

Joindre facilement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré

Cette procédure permet de joindre facilement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré. Pour terminer cette procédure, vous devez créer un AWS Secrets Manager secret qui peut entraîner des coûts supplémentaires. Pour plus d'informations, consultez [Tarification d'AWS Secrets Manager](#).

Si vous devez effectuer une jonction de domaine fluide entre plusieurs AWS comptes, vous pouvez éventuellement choisir d'activer le [partage d'annuaires](#).

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

Note

Les distributions antérieures à Ubuntu 14 et à Red Hat Enterprise Linux 7 et 8 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Pour une démonstration du processus permettant de joindre facilement une instance Linux à votre annuaire Microsoft AD Active Directory AWS géré, regardez la YouTube vidéo suivante.

[Démonstration EC2 de participation à un domaine AD sans faille d'Amazon pour Linux](#)

Prérequis

Avant de pouvoir configurer une jointure de domaine fluide à une instance EC2 Linux, vous devez suivre les procédures décrites dans ces sections.

Conditions préalables à la mise en réseau pour une jonction de domaine fluide

Pour joindre facilement un domaine à une instance EC2 Linux, vous devez effectuer les opérations suivantes :

- Vous aurez besoin des autorisations IAM suivantes pour rejoindre facilement une instance EC2 Linux :
 - Disposez d'un Microsoft AD AWS géré. Pour en savoir plus, veuillez consulter la section [Création de votre AWS compte Microsoft AD géré](#).
 - Vous aurez besoin des autorisations IAM suivantes pour rejoindre facilement une EC2 Windows instance :
 - Profil d'instance IAM avec les autorisations IAM suivantes :
 - AmazonSSMManagedInstanceCore

- AmazonSSMDirectoryServiceAccess
- Le domaine utilisateur qui rejoint facilement EC2 le domaine Microsoft AWS AD doit disposer des autorisations IAM suivantes :
 - Directory Service Autorisations :
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Autorisations Amazon VPC :
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - EC2 Autorisations :
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
 - AWS Systems Manager Autorisations :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"
- Lorsque votre AWS Managed Microsoft AD est créé, un groupe de sécurité est créé avec des règles entrantes et sortantes. Pour en savoir plus sur ces règles et ces ports, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#). Pour joindre facilement un domaine à une instance EC2 Linux, le VPC sur lequel vous lancez votre instance doit autoriser les mêmes ports autorisés dans les règles entrantes et sortantes de votre groupe de sécurité AWS Microsoft AD géré.
- Selon les paramètres de sécurité et de pare-feu de votre réseau, il peut vous être demandé d'autoriser un trafic sortant supplémentaire. Ce trafic serait destiné au protocole HTTPS (port 443) vers les points de terminaison suivants :

Point de terminaison	Rôle
ec2messages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ssm. <i>region</i> .amazonaws.com	Endpoint pour AWS Systems Manager Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ssmmessages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ds. <i>region</i> .amazonaws.com	Endpoint pour Directory Service. Pour de plus amples informations, veuillez consulter Disponibilité de la région pour Directory Service .
secretsmanager. <i>region</i> .amazonaws.com	Endpoint pour AWS Secrets Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Secrets Manager .

- Nous vous recommandons d'utiliser un serveur DNS qui résoudra votre nom de domaine Microsoft AD AWS géré. Pour ce faire, vous pouvez créer un jeu d'options DHCP. Pour plus d'informations, consultez [Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD](#).
- Si vous choisissez de ne pas créer de jeu d'options DHCP, vos serveurs DNS seront statiques et configurés par votre AWS Managed Microsoft AD.

Sélectionnez votre compte de service de jonction transparente à un domaine

Vous pouvez facilement associer des ordinateurs Linux à votre domaine Microsoft AD Active Directory AWS géré. Pour ce faire, vous devez utiliser un compte utilisateur autorisé à créer un compte d'ordinateur pour joindre les machines au domaine. Bien que les administrateurs délégués AWS ou les membres d'autres groupes puissent disposer de privilèges suffisants pour joindre des ordinateurs au domaine, nous vous déconseillons ce type d'utilisation. À titre de bonne pratique, nous vous recommandons d'utiliser un compte de service disposant des privilèges minimaux nécessaires pour joindre les ordinateurs au domaine.

Pour déléguer un compte doté des privilèges minimaux nécessaires pour associer les ordinateurs au domaine, vous pouvez exécuter les PowerShell commandes suivantes. Vous devez exécuter ces commandes à partir d'un ordinateur Windows joint au domaine sur lequel le [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#) est installé. En outre, vous devez utiliser un compte autorisé à modifier les autorisations sur l'unité d'organisation ou le conteneur de votre ordinateur. La PowerShell commande définit les autorisations permettant au compte de service de créer des objets informatiques dans le conteneur d'ordinateurs par défaut de votre domaine.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
    'schemaNamingContext'
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
    -Filter { LDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
    $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
    in the Computers container.
$AddAccessRule = New-Object -TypeName
    'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
    'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
```

```
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Si vous préférez utiliser une interface utilisateur graphique (GUI), vous pouvez utiliser le processus manuel décrit dans [Délégation de privilèges à votre compte de service](#).

Créer les secrets pour stocker le compte de service de domaine

Vous pouvez l'utiliser AWS Secrets Manager pour stocker le compte de service de domaine. Pour plus d'informations, voir [Création d'un AWS Secrets Manager secret](#).

 Note

Des frais sont associés à Secrets Manager. Pour plus d'informations, voir [Tarification](#) dans le guide de AWS Secrets Manager l'utilisateur.

Pour créer des secrets et stocker les informations du compte de service de domaine

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Store a new secret (Stocker un nouveau secret), procédez comme suit :
 - a. Sous Type de secret, sélectionnez Autre type de secret.
 - b. Sous Paires clé/valeur, procédez comme suit :
 - i. Dans la première case, saisissez **awsSeamlessDomainUsername**. Sur la même ligne, dans la case suivante, entrez le nom d'utilisateur de votre compte de service. Par exemple, si vous avez déjà utilisé la PowerShell commande, le nom du compte de service serait **awsSeamlessDomain**.

 Note

Vous devez saisir **awsSeamlessDomainUsername** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

The screenshot shows the AWS Secrets Manager console interface for creating a new secret. The breadcrumb trail is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows the steps: Step 1: Choose secret type, Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main content area is titled 'Choose secret type'. It has three sections: 'Secret type', 'Key/value pairs', and 'Encryption key'. In the 'Secret type' section, four options are listed: 'Credentials for Amazon RDS database', 'Credentials for Amazon DocumentDB database', 'Credentials for Amazon Redshift cluster', and 'Other type of secret'. The 'Other type of secret' option is selected and highlighted with a red box. Below this, the 'Key/value pairs' section has a table with two columns: 'Key/value' and 'Plaintext'. The first row has 'awsSeamlessDomainUsername' in the 'Key/value' column, which is highlighted with a red box. There is an '+ Add row' button below the table. The 'Encryption key' section has a dropdown menu with 'aws/secretsmanager' selected and a refresh button. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. Choisissez Add row (Ajouter une ligne).
- iii. Sur la nouvelle ligne, dans la première case, saisissez **awsSeamlessDomainPassword**. Sur la même ligne, dans la case suivante, saisissez le mot de passe de votre compte de service.

Note

Vous devez saisir **awsSeamlessDomainPassword** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

- iv. Sous Clé de chiffrement, laissez la valeur par défaut `aws/secretsmanager`. AWS Secrets Manager chiffre toujours le secret lorsque vous choisissez cette option. Vous pouvez également choisir une clé que vous avez créée.
- v. Choisissez Suivant.

4. Sous Nom secret, entrez un nom secret qui inclut votre identifiant de répertoire en utilisant le format suivant, en le **d-xxxxxxxx** remplaçant par votre identifiant de répertoire :

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

Cela servira à récupérer des secrets dans l'application.

 Note

Vous devez le saisir **aws/directory-services/d-xxxxxxxx/seamless-domain-join** exactement tel quel, mais le **d-xxxxxxxx** remplacer par votre identifiant de répertoire. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

Secret name must contain only alphanumeric characters and the characters /_+:@-

Description - optional

Maximum 250 characters.

Tags - optional
No tags associated with the secret.

Resource permissions - optional [Info](#)
Add or edit a resource policy to access secrets across AWS accounts.

Replicate secret - optional
Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

5. Laissez le reste des paramètres définis par défaut, puis choisissez Next (Suivant).
6. Sous Configure automatic rotation (Configurer la rotation automatique), choisissez Disable automatic rotation (Désactiver la rotation automatique), puis cliquez sur Next (Suivant).

Vous pouvez activer la rotation pour ce secret après l'avoir enregistré.

7. Vérifiez les paramètres, puis choisissez Store (Stocker) pour enregistrer vos modifications. La console Secrets Manager vous redirige à la liste des secrets de votre compte, où votre nouveau secret est désormais inclus.
8. Choisissez le nom du secret que vous venez de créer dans la liste et prenez note de la valeur de l'ARN secret. Vous en aurez besoin pour la section suivante.

Activer la rotation pour le secret du compte de service de domaine

Nous vous recommandons d'alterner régulièrement les secrets afin d'améliorer votre niveau de sécurité.

Pour activer la rotation pour le secret du compte de service de domaine

- Suivez les instructions de la section [Configurer la rotation automatique pour les AWS Secrets Manager secrets](#) dans le Guide de AWS Secrets Manager l'utilisateur.

Pour l'étape 5, utilisez le modèle de rotation des [informations d'identification Microsoft Active Directory](#) dans le guide de AWS Secrets Manager l'utilisateur.

Pour obtenir de l'aide, consultez la section [Résolution des problèmes AWS Secrets Manager de rotation](#) dans le Guide de AWS Secrets Manager l'utilisateur.

Créez le rôle et la politique IAM requis

Suivez les étapes préalables suivantes pour créer une politique personnalisée qui autorise un accès en lecture seule à votre secret de jonction de domaine transparent Secrets Manager (que vous avez créé précédemment) et pour créer un nouveau rôle Linux EC2 DomainJoin IAM.

Créer la politique de lecture IAM Secrets Manager

Utilisez la console IAM pour créer une politique qui accorde un accès en lecture seule à votre secret Secrets Manager.

Pour créer la politique de lecture IAM Secrets Manager

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez ensuite la console IAM à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation, Gestion des accès, sélectionnez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez-le ensuite dans la zone de texte JSON.

 Note

Assurez-vous de remplacer l'ARN de la région et de la ressource par la région et l'ARN réels du secret que vous avez créé précédemment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxx:secret:aws/directory-
services/d-xxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. Lorsque vous avez terminé, choisissez Next. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe. Pour plus d'informations, veuillez consulter la section [Validating IAM policies](#) (français non garanti).
6. Sur la page Review policy (Réviser la politique), saisissez un nom pour la politique, tel que **SM-Secret-Linux-DJ-d-xxxxxxx-Read**. Vérifiez la section Summary (Récapitulatif) pour voir les autorisations accordées par votre politique. Sélectionnez Create Policy (Créer une politique) pour enregistrer vos changements. La nouvelle politique s'affiche dans la liste des politiques gérées et est prête à être attachée à une identité.

 Note

Nous vous recommandons de créer une politique par secret. Cela garantit que les instances n'ont accès qu'au secret approprié et minimise les répercussions si une instance est compromise.

Création du EC2 DomainJoin rôle Linux

Vous utilisez la console IAM pour créer le rôle que vous utiliserez pour joindre un domaine à votre EC2 instance Linux.

Pour créer le EC2 DomainJoin rôle Linux

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez ensuite la console IAM à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
3. Dans le panneau de contenu, sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis cliquez sur Suivant.

The screenshot shows the 'Create role' wizard in the AWS IAM console. The 'Select trusted entity' step is active. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected. The 'EC2' use case description is highlighted with a red box.

6. Pour Filter policies (Filtrer les politiques), procédez comme suit :
 - a. Saisissez **AmazonSSMManagedInstanceCore**. Cochez ensuite la case correspondant à cet élément de la liste.
 - b. Saisissez **AmazonSSMDirectoryServiceAccess**. Cochez ensuite la case correspondant à cet élément de la liste.
 - c. Saisissez **SM-Secret-Linux-DJ-d-xxxxxxxxxxx-Read** (ou le nom de la politique que vous avez créée dans la procédure précédente). Cochez ensuite la case correspondant à cet élément de la liste.

- d. Après avoir ajouté les trois politiques répertoriées ci-dessus, sélectionnez Créer un rôle.

 Note

Amazon SSMDirectory ServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. Amazon SSMManged InstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section [Create an IAM instance profile for Systems Manager](#) (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. **LinuxEC2DomainJoin**
8. (Facultatif) Pour Role description (Description du rôle), entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Choisissez Créer un rôle.

Rejoignez facilement votre instance Linux

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Linux.
5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.

6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

 Note

L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter [Getting the currently installed SSM Agent version](#) (français non garanti). Si vous devez mettre à niveau l'agent SSM, consultez [Installation et configuration de l'agent SSM sur des EC2 instances pour Linux](#). SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un domaine Active Directory. Le plugin remplace le nom d'hôte des instances Linux par le format EC2 AMAZ-~~XXXXXXX~~. Pour plus d'informations sur `aws:domainJoin`, consultez la [référence du plug-in du document de AWS Systems Manager commande](#) dans le guide de AWS Systems Manager l'utilisateur.

7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez `.pem`. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez `.ppk`. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

 Important

C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section Conditions préalables Étape 2 : Création du rôle Linux. EC2 DomainJoin
16. Choisissez Launch instance (Lancer une instance).

Note

Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez `sudo reboot`.

Joindre facilement une instance Amazon EC2 Linux à un Microsoft AD AWS géré partagé

Dans le cadre de cette procédure, vous allez facilement associer une instance Amazon EC2 Linux à un AWS Managed Microsoft AD partagé. Pour ce faire, vous allez créer une politique de lecture AWS Secrets Manager IAM dans le rôle d' EC2instance du compte sur lequel vous souhaitez lancer l'instance EC2 Linux. C'est ce que l'on appellera cela Account 2 dans cette procédure. Cette instance utilisera le AWS Managed Microsoft AD qui est partagé depuis l'autre compte appeléAccount 1.

Prérequis

Avant de pouvoir joindre facilement une instance Amazon EC2 Linux à un Microsoft AD AWS géré partagé, vous devez effectuer les opérations suivantes :

- Étapes 1 à 3 du didacticiel, [Tutoriel : Partage de votre répertoire Microsoft AD AWS géré pour une jonction de EC2 domaine fluide](#). Ce didacticiel explique comment configurer votre réseau et partager votre AWS Managed Microsoft AD.
- La procédure décrite dans [Joindre facilement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré](#).

Étape 1. Créer un EC2 DomainJoin rôle Linux dans le compte 2

Au cours de cette étape, vous allez utiliser la console IAM pour créer le rôle IAM que vous utiliserez pour joindre un domaine à votre instance EC2 Linux lorsque vous êtes connecté à. Account 2

Création du EC2 DomainJoin rôle Linux

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles.
3. Sur la page Rôles, choisissez Créer un rôle.
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis cliquez sur Suivant
6. Pour Filter policies (Filtrer les politiques), procédez comme suit :
 - a. Saisissez AmazonSSMManagedInstanceCore. Cochez ensuite la case correspondant à cet élément dans la liste.
 - b. Saisissez AmazonSSMDirectoryServiceAccess. Cochez ensuite la case correspondant à cet élément dans la liste.
 - c. Après avoir ajouté ces politiques, sélectionnez Créer un rôle.

Note

AmazonSSMDirectoryServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. AmazonSSMManagedInstanceCore fournit les autorisations minimales nécessaires à l'utilisation AWS Systems Manager. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, consultez la section [Configurer les autorisations d'instance requises pour Systems Manager](#) dans le Guide de l'AWS Systems Manager utilisateur.

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. LinuxEC2DomainJoin
8. (Facultatif) Dans Description du rôle, entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Choisissez Créer un rôle.

Étape 2. Créez un accès aux ressources entre comptes pour partager des AWS Secrets Manager secrets

La section suivante présente les exigences supplémentaires qui doivent être satisfaites pour joindre facilement des instances EC2 Linux avec un Microsoft AD AWS géré partagé. Ces exigences incluent la création de politiques de ressources et leur rattachement aux services et ressources appropriés.

Pour permettre aux utilisateurs d'un compte d'accéder aux AWS Secrets Manager secrets d'un autre compte, vous devez autoriser l'accès à la fois dans le cadre d'une politique de ressources et d'une politique d'identité. Ce type d'accès est appelé [accès aux ressources entre comptes](#).

Ce type d'accès est différent de l'accès aux identités du même compte que le secret de Secrets Manager. Vous devez également autoriser la clé d'identité à utiliser [AWS Key Management Service](#) (KMS) avec laquelle le secret est chiffré. Cette autorisation est nécessaire car vous ne pouvez pas utiliser la clé AWS gérée (aws/secretsmanager) pour un accès entre comptes. Au lieu de cela, vous chiffrerez votre secret avec une clé KMS que vous aurez créée, puis vous y associerez une politique de clé. Pour modifier la clé de chiffrement d'un secret, voir [Modifier un AWS Secrets Manager secret](#).

Note

Des frais sont associés AWS Secrets Manager, selon le secret que vous utilisez. Pour obtenir la liste de prix actuelle complète, consultez [Tarification AWS Secrets Manager](#). Vous pouvez utiliser la Clé gérée par AWS aws/secretsmanager logiciel créé par Secrets Manager pour chiffrer vos secrets gratuitement. Si vous créez vos propres clés KMS pour chiffrer vos secrets, cela vous sera AWS facturé au tarif AWS KMS en vigueur. Pour plus d'informations, consultez [Tarification d'AWS Key Management Service](#).

Les étapes suivantes vous permettent de créer les politiques de ressources permettant aux utilisateurs de joindre facilement une instance EC2 Linux à un Microsoft AD AWS géré partagé.

Associez une politique de ressources au secret dans le compte 1

1. Ouvrez la console Secrets Manager à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Dans la liste des secrets, choisissez le secret que vous avez créé pendant le [Prérequis](#).
3. Sur la page des détails du secret, sous l'onglet Aperçu, faites défiler la page jusqu'à Autorisations relatives aux ressources.

4. Sélectionnez Modifier les autorisations.

- Dans le champ de stratégie, entrez la politique suivante. La politique suivante autorise Linux EC2 DomainJoin in Account 2 à accéder au secret dans Account 1. Remplacez la valeur ARN par la valeur ARN de votre Account 2 LinuxEC2DomainJoin rôle que vous avez créé à l'étape 1. Pour utiliser cette politique, voir [Associer une politique d'autorisation à un AWS Secrets Manager secret](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Ajoutez une déclaration à la politique clé pour la clé KMS dans le compte 1

- Ouvrez la console Secrets Manager à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
- Dans le volet de navigation de gauche, sélectionnez Clés gérées par le client.
- Sur la page Clés gérées par le client, sélectionnez la clé que vous avez créée.
- Sur la page Informations clés, accédez à Politique clé, puis sélectionnez Modifier.
- La déclaration de politique clé suivante permet Account 2 à ApplicationRole in d'utiliser la clé KMS Account 1 pour déchiffrer le secret dans Account 1. Pour utiliser cette déclaration, ajoutez-la à la stratégie de clé de votre clé KMS. Consultez [Modification d'une stratégie de clé](#) pour de plus amples informations.

```
{
```

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Créez une politique d'identité pour l'identité du compte 2

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Politiques.
3. Sélectionnez Create Policy (Créer une politique). Choisissez JSON dans l'éditeur de politiques.
4. La politique suivante permet d'accéder ApplicationRole Account 2 au secret Account 1 et de déchiffrer la valeur du secret en utilisant la clé de chiffrement qui se trouve également dans Account 1. Vous trouverez l'ARN de votre secret dans la console Secrets Manager, sur la page Détails du secret, sous Secret ARN. Vous pouvez également appeler [describe-secret](#) pour identifier l'ARN du secret. Remplacez l'ARN de ressource par l'ARN de ressource pour l'ARN secret et Account 1. Pour utiliser cette politique, voir [Associer une politique d'autorisation à un AWS Secrets Manager secret](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:secretName-AbCdEf"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "kms:Decrypt",
        "kms:Describekey"
    ],
    "Resource": "arn:aws:kms:us-  
east-1:111122223333:key/Your_Encryption_Key"
  }
]
```

5. Sélectionnez Suivant, puis sélectionnez Enregistrer les modifications.
6. Recherchez et sélectionnez le rôle que vous avez créé Account 2 dans [Attach a resource policy to the secret in Account 1](#).
7. Sous Ajouter des autorisations, sélectionnez Joindre des politiques.
8. Dans la barre de recherche, recherchez la politique que vous avez créée [Add a statement to the key policy for the KMS key in Account 1](#) et cochez la case pour ajouter la politique au rôle. Sélectionnez ensuite Ajouter des autorisations.

Étape 3. Rejoignez facilement votre instance Linux

Vous pouvez désormais utiliser la procédure suivante pour joindre facilement votre instance EC2 Linux à votre AWS Managed Microsoft AD partagé.

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Linux.
5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.
6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

 Note

L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter [Getting the currently installed SSM Agent version](#) (français non garanti). Si vous devez mettre à niveau l'agent SSM, consultez [Installation et configuration de l'agent SSM sur des EC2 instances pour Linux](#). SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un domaine Active Directory. Le plugin remplace le nom d'hôte des instances Linux par le format EC2 AMAZ-`XXXXXXX`. Pour plus d'informations sur `aws:domainJoin`, consultez la [référence du plug-in du document de AWS Systems Manager commande](#) dans le guide de AWS Systems Manager l'utilisateur.

7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez `.pem`. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez `.ppk`. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

 Important

C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section Conditions préalables Étape 2 : Création du rôle Linux. EC2 DomainJoin
16. Choisissez Launch instance (Lancer une instance).

 Note

Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez `sudo reboot`.

Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré

Outre les EC2 Windows instances Amazon, vous pouvez également joindre certaines instances Amazon EC2 Linux à votre annuaire Microsoft AD Active Directory AWS géré. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

 Note

D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Joindre une instance Linux à votre Microsoft AD AWS géré

Avant de pouvoir joindre une instance Amazon Linux, CentOS, Red Hat ou Ubuntu à votre annuaire, l'instance doit d'abord être lancée comme indiqué dans [Rejoignez facilement votre instance Linux](#).

 Important

Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance Amazon Linux - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les paquets Amazon Linux requis sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

Note

Pour vous aider à déterminer la version d'Amazon Linux que vous utilisez, consultez la section [Identification des images Amazon Linux](#) dans le guide de EC2 l'utilisateur Amazon pour les instances Linux.

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un compte du *example.com* domaine doté de privilèges de connexion au domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

CentOS

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance CentOS 7 est à jour.

```
sudo yum -y update
```

4. Installez les paquets CentOS 7 obligatoires sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés.
Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un compte du *example.com* domaine doté de privilèges de connexion au domaine.
À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

- a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

- b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Red Hat

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que l'instance Red Hat - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les packages Red Hat obligatoires sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

AMAccountNom s d'un compte du *example.com* domaine doté de privilèges d'adhésion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

SUSE

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance SUSE Linux 15 est à jour.
 - a. Connectez le référentiel de packages.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

b. Mettre à jour SUSE.

```
sudo zypper update -y
```

4. Installez les paquets SUSE Linux 15 requis sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account example.com --verbose
```

join_account

Le AMAccount nom s du *example.com* domaine doté de privilèges de jonction de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Notez que les deux retours suivants sont attendus.

```
! Couldn't authenticate with keytab while discovering which salt to use:  
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Activez manuellement SSSD dans PAM.

```
sudo pam-config --add --sss
```

7. Modifier nsswitch.conf pour activer SSSD dans nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Ajoutez la ligne suivante à /etc/pam.d/common-session pour créer automatiquement un répertoire personnel lors de la connexion initiale

```
sudo vi /etc/pam.d/common-session
```

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Redémarrez l'instance pour terminer le processus de jointure de domaine.

```
sudo reboot
```

10. Reconnectez-vous à l'instance à l'aide d'un client SSH pour vérifier que la jointure de domaine s'est terminée avec succès et finalisez les étapes supplémentaires.

a. Pour confirmer que l'instance a été inscrite sur le domaine

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
```



```
required-package: samba-client
login-formats: %U@example.com
login-policy: allow-realm-logins
```

b. Pour vérifier l'état du démon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor
  preset: disabled)
  Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
  Main PID: 479 (sssd)
  Tasks: 4
  CGroup: /system.slice/sss.service
          ##479 /usr/sbin/sss -i --logger=files
          ##505 /usr/lib/sss/sss_be --domain example.com --uid 0 --gid 0 --
  logger=files
          ##548 /usr/lib/sss/sss_nss --uid 0 --gid 0 --logger=files
          ##549 /usr/lib/sss/sss_pam --uid 0 --gid 0 --logger=files
```

11 Pour autoriser l'accès d'un utilisateur via SSH et la console

```
sudo realm permit join_account@example.com
```

Pour autoriser un accès à un groupe de domaines via SSH et la console

```
sudo realm permit -g 'AWS Delegated Administrators'
```

Ou pour permettre à tous les utilisateurs d'accéder

```
sudo realm permit --all
```

12 Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

13.13. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "Domain Admins" group from the awsad.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que l'instance Ubuntu - 64 bits est à jour.

```
sudo apt-get update  
sudo apt-get -y upgrade
```

4. Installez les packages Ubuntu obligatoires sur votre instance Linux.

Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Désactivez la résolution DNS inversée et définissez le domaine par défaut sur le nom de domaine complet de votre domaine. Les instances Ubuntu doivent pouvoir faire l'objet d'une résolution inverse dans le DNS pour qu'un domaine puisse fonctionner. Sinon, vous devez désactiver la résolution DNS inverse dans `/etc/krb5.conf` de la façon suivante :

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

AMAccountNom s d'un compte du *example.com* domaine doté de privilèges d'adhésion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

...

```
* Successfully enrolled machine in realm
```

7. Définissez le service SSH pour permettre l'authentification du mot de passe.

- Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

- Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

8. Une fois l'instance redémarrée, connectez-vous à celle-ci avec n'importe quel client SSH et ajoutez le groupe AWS Delegated Administrators à la liste des sudoers en effectuant les étapes suivantes :

- Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

- Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « `\<space>` » pour créer le caractère d'espace Linux.)

Restriction de l'accès de connexion à un compte

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande `ad_access_filter` dans `sssd.conf`. Exemples :

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'UO est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement `ad_access_filter` à votre `/etc/sss/sssd.conf`.

Ouvrez le fichier `/etc/sss/sssd.conf` dans un éditeur de texte.

```
sudo vi /etc/sss/sssd.conf
```

Une fois l'opération effectuée, votre commande `sssd.conf` pourrait ressembler à ce qui suit :

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
```

```
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande `ad_access_filter` dans `sssd.conf`.

Exemples :

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'UO est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement `ad_access_filter` à votre `/etc/sss/sssd.conf`.

1. Ouvrez le fichier `/etc/sss/sssd.conf` dans un éditeur de texte.

```
sudo vi /etc/sss/sssd.conf
```

2. Une fois l'opération effectuée, votre commande `sssd.conf` pourrait ressembler à ce qui suit :

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Pour que la configuration soit appliquée, vous devez redémarrer le service `sssd` :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Cartographie des identifiants

Le mappage des identifiants peut être effectué par deux méthodes afin de maintenir une expérience unifiée entre l'identifiant utilisateur (UID) UNIX/Linux et l'identifiant de groupe (GID) et les identités Windows et Active Directory Security Identifier (SID). Ces méthodes sont les suivantes :

1. Centralisée
2. Distribué

Note

Le mappage centralisé de l'identité utilisateur dans Active Directory nécessite une interface de système d'exploitation portable ou POSIX.

Cartographie centralisée de l'identité des utilisateurs

Active Directory ou un autre service LDAP (Lightweight Directory Access Protocol) fournit un UID et un GID aux utilisateurs de Linux. Dans Active Directory, ces identifiants sont stockés dans les attributs des utilisateurs si l'extension POSIX est configurée :

- UID - Le nom d'utilisateur Linux (chaîne)
- Numéro UID : numéro d'identification utilisateur Linux (entier)
- Numéro GID : numéro d'identification du groupe Linux (entier)

Pour configurer une instance Linux afin d'utiliser l'UID et le GID d'Active Directory, définissez-les `ldap_id_mapping = False` dans le fichier `sssd.conf`. Avant de définir cette valeur, vérifiez que vous avez ajouté un UID, un numéro UID et un numéro GID aux utilisateurs et aux groupes dans Active Directory.

Cartographie distribuée de l'identité des utilisateurs

Si Active Directory ne possède pas l'extension POSIX ou si vous choisissez de ne pas gérer de manière centralisée le mappage des identités, Linux peut calculer les valeurs UID et GID. Linux utilise l'identifiant de sécurité (SID) unique de l'utilisateur pour garantir la cohérence.

Pour configurer le mappage d'ID utilisateur distribué, définissez-le `ldap_id_mapping = True` dans le fichier `sssd.conf`.

Problèmes courants

Si vous le configurez `ldap_id_mapping = False`, le démarrage du service SSSD échouera parfois. La raison de cet échec est due au fait que les modifications UIDs ne sont pas prises en charge. Nous vous recommandons de supprimer le cache SSSD chaque fois que vous passez du mappage d'ID aux attributs POSIX ou des attributs POSIX au mappage d'ID. Pour plus de détails sur le mappage des identifiants et les paramètres `ldap_id_mapping`, consultez la page de manuel `sssd-ldap (8)` sur la ligne de commande Linux.

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

```
As "root" (sudo or sudo -i) use the:
```

- zypper command for package management
- yast command for configuration management

```
Management and Config: https://www.suse.com/suse-in-the-cloud-basics
```

```
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
```

```
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
```

```
System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load:  0.01      Processes:            102
Usage of /:    18.6% of 7.69GB   Users logged in:     2
Memory usage:  16%          IP address for eth0: 10.24.34.1
Swap usage:    0%
```

Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Microsoft AD Active Directory AWS géré à l'aide de Winbind

Vous pouvez utiliser le service Winbind pour joindre manuellement vos instances Amazon EC2 Linux à un domaine Microsoft AD Active Directory AWS géré. Cela permet aux utilisateurs Active Directory locaux existants d'utiliser leurs informations d'identification Active Directory lorsqu'ils accèdent aux instances Linux jointes à votre annuaire Microsoft AD Active Directory AWS géré. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

Note

D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Joindre une instance Linux à votre répertoire Microsoft AD Active Directory AWS géré

Important

Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux/CENTOS/REDHAT

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance Linux est à jour.

```
sudo yum -y update
```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec :

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Ouvrez le fichier de configuration d'origine `[/etc/samba/smb.conf]` dans un éditeur de texte.

```
sudo vim /etc/samba/smb.conf
```

Renseignez les informations relatives à votre environnement de domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes [/etc/hosts] dans un éditeur de texte.

```
sudo vim /etc/hosts
```

Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

Si vous n'avez pas indiqué votre adresse IP dans le fichier /etc/hosts, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine :

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Cette erreur signifie que la jonction a réussi, mais que la commande [net ads] n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à Active Directory à l'aide de l'utilitaire net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Un compte du *example.com* domaine doté de privilèges de connexion au domaine.

À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo authconfig --enablewinbind --enablewinbindauth --enablemkhomedir --update
```

- 10 Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier `/etc/ssh/sshd_config`.

- a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

- c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

11. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

```
## Adding Domain Users/Groups.  
%domainname\\AWS\\ Delegated\\ Administrators ALL=(ALL:ALL) ALL  
%domainname\\groupname ALL=(ALL:ALL) ALL  
domainname\\username ALL=(ALL:ALL) ALL  
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL  
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

SUSE

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance SUSE Linux 15 est à jour.
 - a. Connectez le référentiel de packages.

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

b. Mettre à jour SUSE.

```
sudo zypper update -y
```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

```
sudo zypper in -y samba samba-winbind
```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec :

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Ouvrez le fichier de configuration d'origine `[/etc/samba/smb.conf]` dans un éditeur de texte.

```
sudo vim /etc/samba/smb.conf
```

Renseignez les informations relatives à l'environnement de votre domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes `[/etc/hosts]` dans un éditeur de texte.

```
sudo vim /etc/hosts
```

Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

 Note

Si vous n'avez pas indiqué votre adresse IP dans le fichier `/etc/hosts`, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine :

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Cette erreur signifie que la jonction a réussi, mais que la commande `[net ads]` n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à l'annuaire avec la commande suivante.

```
sudo net ads join -U join_account@example.com
```

join_account

Le AMAccount nom s du *example.com* domaine doté de privilèges de jonction de domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo pam-config --add --winbind --mkhomedir
```

10. Ouvrez le fichier de configuration Name Service Switch `[/etc/nsswitch.conf]` dans un éditeur de texte.

```
vim /etc/nsswitch.conf
```

Ajoutez la directive Winbind comme indiqué ci-dessous.


```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11 Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier `/etc/ssh/sshd_config`.

- a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vim /etc/ssh/sshd_config
```

- b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

- c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

12 Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste `sudoers` en effectuant les étapes suivantes :

- a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

- b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

```
## Adding Domain Users/Groups.
%domainname\\AWS\\ Delegated\\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP de serveur DNS des serveurs DNS fournis par Directory Service. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance Linux est à jour.

```
sudo apt-get -y upgrade
```

4. Installez les paquets Samba/Winbind obligatoires sur votre instance Linux.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Faites une sauvegarde du fichier `smb.conf` principal afin de pouvoir y revenir en cas d'échec.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Ouvrez le fichier de configuration d'origine `[/etc/samba/smb.conf]` dans un éditeur de texte.

```
sudo vim /etc/samba/smb.conf
```

Renseignez les informations relatives à l'environnement de votre domaine Active Directory comme indiqué dans l'exemple ci-dessous :

```
[global]
workgroup = example
security = ads
realm = example.com
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
```

```
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Ouvrez le fichier d'hôtes [/etc/hosts] dans un éditeur de texte.

```
sudo vim /etc/hosts
```

Ajoutez l'adresse IP privée de votre instance Linux comme suit :

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

Si vous n'avez pas indiqué votre adresse IP dans le fichier /etc/hosts, le message d'erreur DNS suivant peut s'afficher lorsque vous joignez l'instance au domaine :

No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER

Cette erreur signifie que la jonction a réussi, mais que la commande [net ads] n'a pas pu consigner l'enregistrement DNS dans le DNS.

8. Joignez l'instance Linux à Active Directory à l'aide de l'utilitaire net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Un compte du *example.com* domaine doté de privilèges de connexion au domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
Enter join_account@example.com's password:
```

```
Using short domain name -- example  
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifiez le fichier de configuration PAM, utilisez la commande ci-dessous pour ajouter les entrées nécessaires à l'authentification Winbind :

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Ouvrez le fichier de configuration Name Service Switch [/etc/nsswitch.conf] dans un éditeur de texte.

```
vim /etc/nsswitch.conf
```

Ajoutez la directive Winbind comme indiqué ci-dessous.

```
passwd: compat winbind  
group:  compat winbind  
shadow: compat winbind
```

11. Définissez le service SSH pour permettre l'authentification du mot de passe en modifiant le fichier /etc/ssh/sshd_config.

- a. Ouvrez le fichier /etc/ssh/sshd_config dans un éditeur de texte.

```
sudo vim /etc/ssh/sshd_config
```

- b. Définissez le paramètre PasswordAuthentication sur yes.

```
PasswordAuthentication yes
```

- c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

12. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez des privilèges racine pour un groupe ou un utilisateur de domaine à la liste sudoers en effectuant les étapes suivantes :

- a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

- b. Ajoutez les groupes ou utilisateurs requis à partir de votre domaine approuvé ou d'approbation comme suit, puis enregistrez-les.

```
## Adding Domain Users/Groups.  
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL  
%domainname\\groupname ALL=(ALL:ALL) ALL  
domainname\\username ALL=(ALL:ALL) ALL  
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL  
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com  
johndoe@example.com's password:  
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)
```

As "root" (sudo or sudo -i) use the:

- zypper command for package management
- yast command for configuration management

Management and Config: <https://www.suse.com/suse-in-the-cloud-basics>

Documentation: <https://www.suse.com/documentation/sles-15/>

Forum: <https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud>

Have a lot of fun...

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Sat Apr 18 22:03:35 UTC 2020

System load:  0.01               Processes:            102
Usage of /:   18.6% of 7.69GB    Users logged in:     2
Memory usage: 16%               IP address for eth0: 10.24.34.1
Swap usage:   0%
```

Joindre une instance Amazon EC2 Mac à votre annuaire Microsoft AD Active Directory AWS géré

Cette procédure joint manuellement une instance Amazon EC2 Mac à votre répertoire Microsoft AD Active Directory AWS géré.

Prérequis

- Les instances Amazon EC2 Mac nécessitent des hôtes [Amazon EC2 Dedicated Hosts](#). Vous devez allouer un hôte dédié et lancer une instance sur l'hôte. Pour plus d'informations, consultez [Lancer une instance Mac](#) dans le guide de EC2 l'utilisateur Amazon.
- Nous vous recommandons de créer un ensemble d'options DHCP pour votre répertoire Microsoft AD Active Directory AWS géré. Cela permettra à toutes les instances de votre Amazon VPC de pointer vers le domaine spécifié et aux serveurs DNS de résoudre leurs noms de domaine. Pour plus d'informations, consultez [Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD](#).

 Note

Le tarif des hôtes dédiés varie en fonction de l'option de paiement que vous sélectionnez. Pour plus d'informations, consultez la section [Tarification et facturation](#) dans le guide de EC2 l'utilisateur Amazon.

Rejoindre manuellement une instance Mac

1. Utilisez la commande SSH suivante pour vous connecter à votre instance Mac. Pour plus d'informations sur la connexion à votre instance Mac, consultez la section [Se connecter à votre instance Mac](#).

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

2. Une fois connecté à votre instance Mac, créez un mot de passe pour le *ec2-user* compte à l'aide de la commande suivante :

```
sudo passwd ec2-user
```

3. Lorsque vous y êtes invité sur la ligne de commande, entrez un mot de passe pour le *ec2-user* compte. Vous pouvez mettre à jour votre système d'exploitation et vos logiciels en suivant la procédure décrite dans [Mettre à jour le système d'exploitation et le logiciel](#) dans le guide de EC2 l'utilisateur Amazon.
4. Utilisez la *dsconfigad* commande suivante pour joindre votre instance Mac au domaine AWS Managed Microsoft AD Active Directory. Assurez-vous de remplacer le nom de domaine, le nom de l'ordinateur et l'unité organisationnelle par les informations de votre domaine AWS Managed Microsoft AD Active Directory. Pour plus d'informations, voir [Configuration de l'accès au domaine dans Directory Utility sur Mac sur](#) le site Web d'Apple.

 Warning

Le nom de l'ordinateur ne doit pas contenir de tiret. Les traits d'union peuvent empêcher la liaison avec le répertoire AWS Microsoft AD Active Directory géré.

```
sudo dsconfigad -add domainName -computer computerName -username Username -  
ou "Your-AWS-Delegated-Organizational-Unit"
```

L'exemple suivant montre à quoi doit ressembler la commande lorsque vous rejoignez un utilisateur administratif sur une instance Mac **myec2mac01** associée au **example.com** domaine :

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -  
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Utilisez la commande suivante pour ajouter les administrateurs AWS délégués à l'utilisateur administratif sur votre instance Mac :

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators"
```

6. Utilisez la commande suivante pour confirmer que la jointure du domaine AWS Managed Microsoft AD Active Directory a réussi :

```
dsconfigad -show
```

Vous avez joint avec succès votre instance Mac à votre annuaire Microsoft AD Active Directory AWS géré. Vous pouvez désormais vous connecter à votre instance Mac à l'aide de vos informations d'identification Microsoft AD Active Directory AWS gérées.

Lorsque vous vous connectez pour la première fois à votre instance Mac, vous devriez avoir la possibilité de vous connecter en tant qu'utilisateur « Autre ». À ce stade, vous pouvez utiliser vos informations d'identification de domaine Active Directory pour vous connecter à l'instance Mac. Si le message « Autre » ne s'affiche pas sur l'écran de connexion après avoir effectué ces étapes, connectez-vous en tant qu'utilisateur ec2, puis déconnectez-vous.

Pour vous connecter à l'aide de l'interface utilisateur graphique avec un utilisateur de domaine, suivez les étapes décrites dans la [section Connexion à l'interface utilisateur graphique \(GUI\) de votre instance](#) dans le guide de EC2 l'utilisateur Amazon.

Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD

Pour associer un ordinateur à votre compte Microsoft AD AWS géré, vous devez disposer d'un compte doté des privilèges nécessaires pour associer des ordinateurs à l'annuaire.

Avec AWS Directory Service for Microsoft Active Directory, les membres des groupes Admins et AWS Delegated Server Administrators disposent de ces privilèges.

Cependant, en tant que bonne pratique, vous devez utiliser un compte disposant uniquement des privilèges minimum nécessaires. La procédure suivante montre comment créer un nouveau groupe appelé **Joiners** et déléguer les privilèges à ce groupe qui sont nécessaires pour joindre des ordinateurs à l'annuaire.

Vous devez effectuer cette procédure sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

Pour déléguer les privilèges d'adhésion pour AWS Managed Microsoft AD

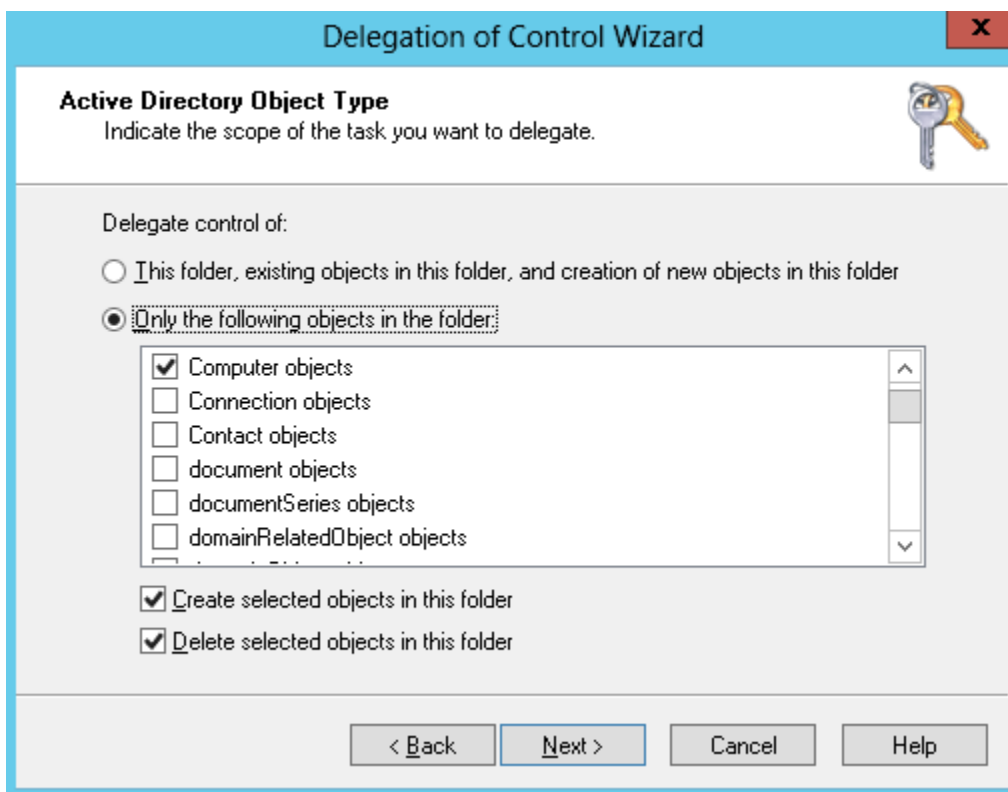
1. Ouvrez Utilisateurs et ordinateurs Active Directory et sélectionnez l'unité d'organisation ayant votre nom NetBIOS dans l'arborescence de navigation, puis sélectionnez l'unité d'organisation Utilisateurs.

Important

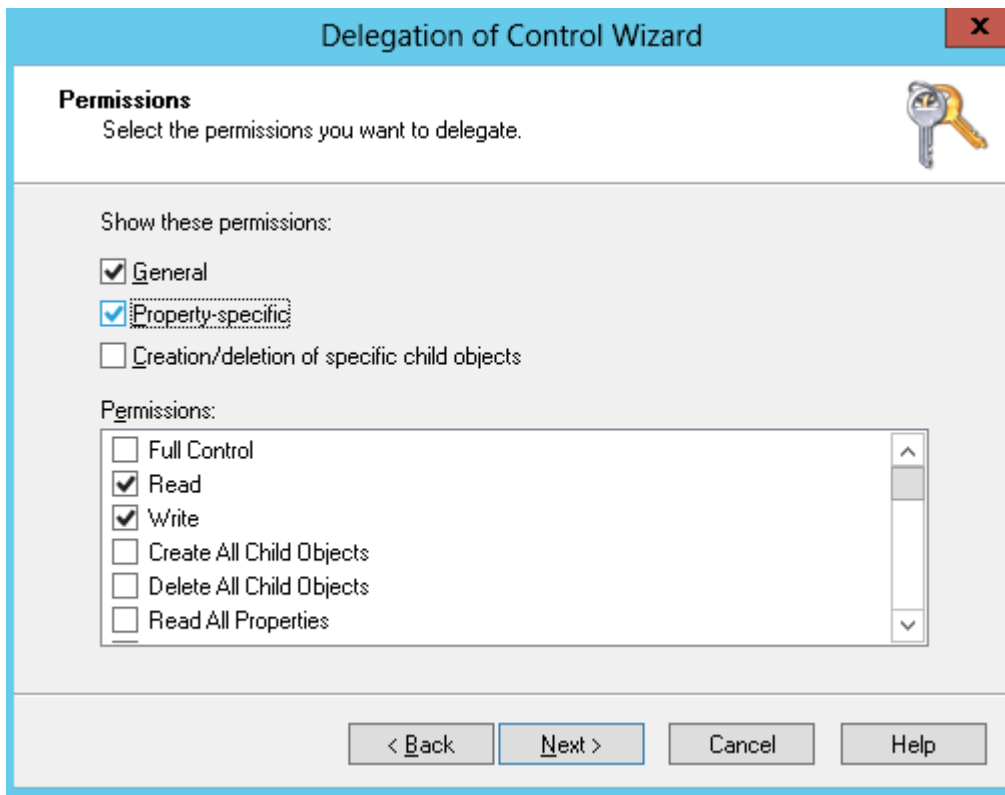
Lorsque vous lancez un service d' AWS annuaire pour Microsoft Active Directory, il AWS crée une unité organisationnelle (UO) qui contient tous les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine est détenue et gérée par AWS. Vous ne pouvez pas apporter des modifications à la racine du domaine lui-même, par conséquent, vous devez créer le groupe **Joiners** au sein de l'unité d'organisation qui détient votre nom NetBIOS.

2. Ouvrez le menu contextuel (clic droit) pour Utilisateurs, choisissez Nouveau, puis choisissez Groupe.
3. Dans la zone Nouvel objet - groupe, saisissez ce qui suit et choisissez OK.
 - Pour Nom du groupe, tapez **Joiners**.

- Pour Étendue du groupe, choisissez Global.
 - Pour Type de groupe, choisissez Sécurité.
4. Dans l'arborescence de navigation, sélectionnez le conteneur Ordinateurs sous votre nom NetBIOS. A partir du menu Action, choisissez Déléguer le contrôle.
 5. Sur la page Delegation of Control Wizard, choisissez Next, puis choisissez Add.
 6. Dans la zone Select Users, Computers, or Groups, saisissez Joiners, puis choisissez OK. Si vous trouvez plusieurs objets, sélectionnez le groupe Joiners créé précédemment. Choisissez Suivant.
 7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
 8. Sélectionnez Only the following objects in the folder, puis Computer objects.
 9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.



10. Sélectionnez Lecture et Ecriture, puis choisissez Suivant.



11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis choisissez Terminer.
12. Créez un utilisateur avec un mot de passe fort et ajoutez-le au groupe Joiners. Cet utilisateur doit figurer dans le conteneur Utilisateurs qui est sous votre nom NetBIOS. L'utilisateur aura alors les privilèges nécessaires pour connecter les instances à l'annuaire.

Création ou modification d'un ensemble d'options DHCP pour AWS Managed Microsoft AD

AWS vous recommande de créer un ensemble d'options DHCP pour votre Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. Cela permet à toutes les instances de ce VPC de pointer vers le domaine spécifié, et aux serveurs DNS de résoudre leurs noms de domaine.

Pour en savoir plus sur les jeux d'options DHCP, veuillez consulter la section [DHCP options sets](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.

2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, saisissez les valeurs suivantes pour votre annuaire :

Nom

Une balise facultative pour le jeu d'options.

Nom de domaine

Nom complet de votre annuaire, par exemple corp.example.com.

Serveurs de noms de domaine

Les adresses IP des serveurs DNS du répertoire AWS que vous avez fourni.

 Note

Vous pouvez trouver ces adresses en accédant au volet de navigation de la [console AWS Directory Service](#), en sélectionnant Directories (Annuaire), puis en choisissant l'ID d'annuaire correct.

Serveurs NTP

Laissez ce champ vide.

Serveur de nom NetBIOS

Laissez ce champ vide.

Type de nœud NetBIOS

Laissez ce champ vide.

4. Choisissez Créer un jeu d'options DHCP. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
5. Notez l'ID du nouveau jeu d'options DHCP (dopt-xxxxxxxx). Vous l'utilisez pour associer le nouveau jeu d'options à votre VPC.

Pour modifier le jeu d'options DHCP associé à un VPC

Vous ne pouvez pas modifier un jeu d'options DHCP après l'avoir créé. Si vous voulez que votre VPC utilise un jeu différent d'options DHCP, vous devez créer un nouveau jeu et l'associer à votre VPC. Vous pouvez également configurer votre VPC pour ne pas utiliser d'options DHCP du tout.

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, sélectionnez Vos VPCs.
3. Sélectionnez le VPC, puis choisissez Actions, Modifier les paramètres du VPC.
4. Pour le jeu d'options DHCP, sélectionnez-en un ou choisissez No DHCP options set (Aucun jeu d'option DHCP), puis sélectionnez Save (Enregistrer).

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la ligne de commande, consultez ce qui suit :

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Gestion des utilisateurs et des groupes dans AWS Managed Microsoft AD

Vous pouvez gérer les utilisateurs et les groupes dans AWS Managed Microsoft AD. Vous créez un utilisateur pour représenter une personne ou une entité pouvant accéder à votre annuaire. Vous pouvez également créer un groupe pour accorder ou refuser des autorisations à plusieurs utilisateurs à la fois. Vous pouvez ajouter non seulement des utilisateurs à un groupe, mais également des groupes à un groupe. Lorsque vous ajoutez un utilisateur à un groupe, celui-ci hérite des rôles et des autorisations attribués au groupe. Lorsque vous ajoutez un groupe à un groupe, les groupes partagent une relation parent-enfant, dans laquelle le groupe enfant hérite des rôles et des autorisations attribués au groupe parent. Vous pouvez également copier les adhésions d'un utilisateur à un groupe dans un autre utilisateur.

Vous pouvez gérer les utilisateurs et les groupes à [the section called “Données du service de répertoire”](#) l'aide des méthodes suivantes :

- [AWS Management Console](#)
- [AWS CLI](#)

- [AWS API de données du Service d'annuaire](#)
- [AWS Tools for Windows PowerShell](#)

Pour une démonstration de la CLI AWS Directory Service Data, regardez la YouTube vidéo suivante.

[Gérer les utilisateurs et les groupes dans AWS Managed Microsoft AD à l'aide de CRUD APIs](#)

Vous pouvez également utiliser une instance [jointe à un domaine](#).

Gérez les utilisateurs et les groupes à l'aide du AWS Management Console

Vous pouvez gérer les utilisateurs et les groupes à l'AWS Management Console aide des données du service de AWS répertoire. Directory Service Data est une extension Directory Service qui vous permet d'effectuer des tâches de gestion d'objets intégrées. Certaines de ces tâches incluent la création d'utilisateurs et de groupes et l'ajout d'utilisateurs à des groupes ainsi que de groupes à un groupe.

Pour plus d'informations, voir [Gérer les utilisateurs et les groupes Microsoft AD AWS gérés avec le AWS Management Console](#).

Note

Pour utiliser cette fonctionnalité, elle doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes](#).

Vous ne pouvez gérer les utilisateurs et les groupes qu'AWS Management Console à l'aide du menu principal Région AWS de votre annuaire. Pour plus d'informations, voir [Régions principales et régions supplémentaires](#).

Vous devez disposer des autorisations IAM nécessaires pour utiliser AWS Directory Service Data. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

Gérez les utilisateurs et les groupes à l'aide du AWS CLI

Vous pouvez gérer les utilisateurs et les groupes AWS CLI via l'[API AWS Directory Service Data](#). Directory Service Data est une extension Directory Service qui vous permet d'effectuer des tâches de gestion d'objets intégrées à l'aide de l'espace de ds-data noms. Certaines de ces tâches incluent la création d'utilisateurs et de groupes et l'ajout d'utilisateurs à des groupes ainsi que de groupes à un groupe.

Création d'un utilisateur à l'aide de la CLI AWS Directory Service Data

Voici un exemple de AWS CLI commande qui utilise l'espace de ds-data noms pour créer un utilisateur.

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
region your-Primary-Region-name
```

Note

Pour l'utiliser AWS CLI, il faut l'activer. Pour de plus amples informations, veuillez consulter [Activation ou désactivation de la gestion des utilisateurs et des groupes ou des données du service de AWS répertoire](#).

Vous pouvez uniquement gérer les utilisateurs et les groupes à l'aide de la CLI AWS Directory Service Data à partir de l'interface de ligne Région AWS de commande principale de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).

Vous devez disposer des autorisations IAM nécessaires pour utiliser AWS Directory Service Data. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que. [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour de plus amples informations, veuillez consulter [Bonnes pratiques de sécurité dans IAM](#).

Pour plus d'informations, voir [Gérer les utilisateurs et les groupes Microsoft AD AWS gérés avec le AWS CLI](#).

Gérez les utilisateurs et les groupes avec Outils AWS pour PowerShell

[Outils AWS pour PowerShell](#) fournit deux modules distincts pour la gestion AWS Directory Service : `AWS.Tools.DirectoryService` (DS) et `AWS.Tools.DirectoryServiceData` (DSD). Lorsque vous travaillez avec AWS Directory Service, assurez-vous d'utiliser le module approprié pour l'opération prévue.

- Le `DirectoryService` module contient des applets de commande pour gérer la configuration et l'administration des services d'annuaire, notamment des applets de commande tels que `Enable-DSDirectoryDataAccess`, et `Disable-DSDirectoryDataAccess` `Reset-DSUserPassword`
- Le `DirectoryServiceData` module contient des applets de commande permettant d'effectuer des opérations dans un répertoire, spécifiquement axées sur la gestion des utilisateurs et des groupes. Ces applets de commande DSD incluent les opérations de gestion des utilisateurs (`New-DSDUser`, `Get-DSDUserUpdate-DSDUser`, et `Remove-DSDUser`), les opérations de gestion des groupes (`New-DSDGroup`, et `Get-DSDGroup`, `Remove-DSDGroup`) `Update-DSDGroup`, la gestion des membres des groupes (`Add-DSDGroupMember` et `Remove-DSDGroupMember`) et les fonctionnalités de recherche (`Search-DSDUser` et `Search-DSDGroup`)

Gérez les utilisateurs et les groupes avec une instance sur site ou une instance Amazon EC2

Si les données du AWS Directory Service ne conviennent pas à votre cas d'utilisation, nous vous recommandons de gérer les utilisateurs et les groupes à l'aide d'une EC2 instance ou d'une instance sur site.

Pour créer des utilisateurs et des groupes dans un Microsoft AD AWS géré, vous pouvez utiliser n'importe quelle instance (locale ou EC2) jointe à votre Microsoft AD AWS géré. Vous devez être connecté en tant qu'utilisateur autorisé à créer des utilisateurs et des groupes. Vous devrez également installer les outils Active Directory sur votre instance afin de pouvoir ajouter vos utilisateurs et groupes à l'aide de l'outil Utilisateurs et ordinateurs Active Directory.

- Vous pouvez déployer une EC2 instance préconfigurée avec des outils d'administration Active Directory préinstallés depuis la console de Directory Service gestion. Pour de plus amples informations, veuillez consulter [Lancement d'une instance d'administration d'annuaire dans votre annuaire Microsoft AD Active Directory AWS géré](#).

- Si vous devez déployer une EC2 instance autogérée avec des outils d'administration et installer les outils nécessaires, consultez [Étape 3 : Déployer une EC2 instance Amazon pour gérer votre annuaire Microsoft AD Active Directory AWS géré.](#)

Rubriques

- [Gérez les utilisateurs et les groupes Microsoft AD AWS gérés avec AWS Management Console AWS CLI, ou Outils AWS pour PowerShell](#)
- [Gérez les utilisateurs et les groupes avec une EC2 instance Amazon](#)

Gérez les utilisateurs et les groupes Microsoft AD AWS gérés avec AWS Management Console AWS CLI, ou Outils AWS pour PowerShell

Vous pouvez utiliser le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell pour gérer vos utilisateurs et groupes Microsoft AD AWS gérés avec [AWS Données du service de répertoire](#). La CLI AWS Directory Service Data utilise l'espace de ds-data noms. Pour plus d'informations sur le AWS CLI, consultez [Getting started with AWS CLI](#). Pour plus d'informations Outils AWS pour PowerShell, consultez le [guide de Outils AWS pour PowerShell l'utilisateur](#).

Consultez les procédures suivantes pour plus d'informations sur la création, l'affichage, la mise à jour et la suppression d'utilisateurs et de groupes Microsoft AD AWS gérés.

Procédures de gestion des utilisateurs et des groupes

- [Activation ou désactivation de la gestion des utilisateurs et des groupes ou des données du service de AWS répertoire](#)
- [Création d'un utilisateur Microsoft AD AWS géré](#)
- [Affichage et mise à jour d'un utilisateur Microsoft AD AWS géré](#)
- [Supprimer un utilisateur Microsoft AD AWS géré](#)
- [Désactivation d'un AWS utilisateur Microsoft AD géré](#)
- [Réinitialisation et activation du mot de AWS passe d'un utilisateur Microsoft AD géré](#)
- [Création d'un groupe Microsoft AD AWS géré](#)
- [Afficher et mettre à jour les détails d'un groupe Microsoft AD AWS géré](#)
- [Suppression d'un groupe Microsoft AD AWS géré](#)
- [Ajouter et supprimer des membres de AWS Managed Microsoft AD à des groupes et des groupes à des groupes](#)

- [Copier les appartenances AWS à un groupe Microsoft AD géré dans le AWS Management Console](#)

Activation ou désactivation de la gestion des utilisateurs et des groupes ou des données du service de AWS répertoire

Pour utiliser la gestion des utilisateurs et des groupes ou les données de AWS Directory Service, elles doivent être activées. Une fois activé, vous pouvez gérer les utilisateurs et les groupes à partir du AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Important

- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Pour obtenir la liste des régions qui prennent en charge les données de AWS Directory Service, consultez [Pris en charge Régions AWS pour les données du Directory Service](#).
- Les contrôles d'accès aux données de AWS Directory Service sont différents des contrôles d' Services AWS accès pour Amazon WorkSpaces, Amazon Quick Suite et Amazon WorkMail. Pour de plus amples informations, veuillez consulter [AWS autorisation d'application avec Directory Service Data](#).

Activation AWS des données du Directory Service

Utilisez la procédure suivante pour activer la gestion des utilisateurs et des groupes ou les données de service d' AWS annuaire pour un Microsoft AD AWS géré existant avec le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

AWS Management Console

Vous pouvez activer la gestion des utilisateurs et des groupes à l'aide du AWS Management Console.

Pour activer la gestion des utilisateurs et des groupes

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.

2. Sur la page des détails du répertoire, pour activer la gestion des utilisateurs et des groupes, sélectionnez Activer.
3. Dans la boîte de dialogue Activer la gestion des utilisateurs et des groupes, sélectionnez Activer.

AWS CLI

Ce qui suit décrit comment formater une demande qui active la CLI AWS Directory Service Data. Vous devez inclure votre numéro d'identification de répertoire dans votre demande.

Note

Les commandes enable AWS Directory Service Data CLI utilisent `aws ds`.

Pour activer la CLI AWS Directory Service Data

- Ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

Outils AWS pour PowerShell

Pour activer les données du service de répertoire à l'aide des outils pour PowerShell

- Ouvrez PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

Désactivation des données du AWS Directory Service

Utilisez la procédure suivante pour désactiver la gestion des utilisateurs et des groupes ou les données de service d' AWS annuaire pour un Microsoft AD AWS géré existant avec le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

AWS Management Console

Vous pouvez désactiver la gestion des utilisateurs et des groupes à l'aide du AWS Management Console.

Pour désactiver la gestion des utilisateurs et des groupes

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page des détails du répertoire, pour désactiver la gestion des utilisateurs et des groupes, sélectionnez Désactiver.
3. Dans la boîte de dialogue Désactiver la gestion des utilisateurs et des groupes, sélectionnez Désactiver.

AWS CLI

Ce qui suit décrit comment formater une demande qui désactive la CLI AWS Directory Service Data. Vous devez inclure votre numéro d'identification de répertoire dans votre demande.

Note

Les commandes disable AWS Directory Service Data CLI utilisent `aws ds`.

Pour désactiver la CLI AWS Directory Service Data

- Ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

Outils AWS pour PowerShell

Pour désactiver les données du Service d'annuaire à l'aide des outils pour PowerShell

- Ouvrez PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire par votre ID de répertoire Microsoft AD AWS géré :

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

Création d'un utilisateur Microsoft AD AWS géré

Utilisez la procédure suivante pour créer un nouvel utilisateur Microsoft AD AWS géré avec la gestion des utilisateurs et des groupes ou les données du service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou les données du service d'annuaire](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

AWS Management Console

Vous pouvez créer un nouveau compte utilisateur Microsoft AD AWS géré dans le AWS Management Console. Lorsque vous créez un nouveau compte utilisateur, vous spécifiez les détails du nouvel utilisateur et vous déterminez s'il convient d'ajouter le nouvel utilisateur à un groupe ou de copier les adhésions d'un autre utilisateur à un groupe dans le nouvel utilisateur.

Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

Pour créer un utilisateur Microsoft AD AWS géré avec AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.

2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Sur la page des détails du répertoire, dans la section Utilisateurs, choisissez Créer un compte utilisateur.
5. La page Spécifier les détails de l'utilisateur s'ouvre. Dans la section Informations obligatoires, entrez un nom d'utilisateur et un mot de passe. Les noms de connexion des utilisateurs doivent répondre aux conditions suivantes :
 - Doit être un nom de connexion unique
 - Peut comporter jusqu'à 20 caractères
 - Ne peut contenir que des caractères alphanumériques
 - ~!@#\$\$%^&* _-+=`|()\{}[]:;'"<>,.?/
 - Le mot de passe doit respecter les exigences de votre politique en matière de mots de passe. Consultez votre AWS administrateur pour plus d'informations.

 Warning

Le nom de connexion de l'utilisateur ne peut pas être modifié une fois l'utilisateur créé.

- a. (Facultatif) Dans la section Informations principales, vous pouvez saisir le prénom et le nom de famille de l'utilisateur. Vous pouvez également saisir un nom d'affichage et une description pour l'utilisateur.
- b. (Facultatif) Dans la section Méthodes de contact, vous pouvez saisir l'adresse e-mail et les numéros de téléphone de l'utilisateur.
- c. (Facultatif) Dans la section Informations relatives au poste, vous pouvez saisir un département, un responsable, un bureau et une entreprise pour l'utilisateur.
- d. (Facultatif) Dans la section Adresse, vous pouvez saisir l'adresse de l'utilisateur.
- e. (Facultatif) Dans la section Paramètres du compte, vous pouvez saisir des notes, une langue préférée et le nom principal du service pour l'utilisateur.

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

6. Choisissez Next une fois que vous avez fourni les informations du compte utilisateur.
7. Sur la page facultative Ajouter des utilisateurs aux groupes, vous pouvez ajouter l'utilisateur à un nouveau groupe ou à un groupe existant. Vous pouvez également copier l'appartenance au groupe d'un utilisateur existant vers le nouvel utilisateur. Si vous ne souhaitez pas ajouter d'utilisateur à un groupe, choisissez Next. Passez à l'étape 12 pour poursuivre cette procédure.
8. (Facultatif) Pour créer un nouveau groupe, voir [Créer un groupe Microsoft AD AWS géré](#).
9. (Facultatif) Pour ajouter un nouvel utilisateur à un groupe existant :
 - Sélectionnez le groupe auquel vous souhaitez ajouter le nouvel utilisateur dans la section Groupes. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche.
10. (Facultatif) Pour copier l'appartenance au groupe d'un utilisateur existant vers un nouvel utilisateur :
 - a. Choisissez l'onglet Copier l'appartenance au groupe depuis l'utilisateur. Pour rechercher un utilisateur appartenant à un groupe que vous souhaitez copier, entrez le nom de connexion de l'utilisateur dans le champ de recherche sous la section Utilisateurs.
 - b. Dans la section Groupes sélectionnés, sélectionnez les groupes dont le nouvel utilisateur doit devenir membre.
11. Choisissez Next lorsque vous êtes prêt à créer le nouveau compte utilisateur.
12. Sur la page Réviser et créer un utilisateur, passez en revue tous les choix que vous avez faits. Choisissez Create user (Créer un utilisateur).
13. Une fois l'utilisateur configuré, vous êtes redirigé vers la page de détails du nouvel utilisateur. Une bannière apparaît indiquant que l'utilisateur a été créé avec succès.

 Important

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à créer un utilisateur, suivez les instructions du message d'erreur pour demander à votre administrateur de vous accorder l'accès.

AWS CLI

Ce qui suit décrit comment formater une demande qui crée un nouveau compte utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data. Vous devez inclure votre numéro d'identification de répertoire et un nom de connexion utilisateur dans votre demande. Vous pouvez également inclure d'autres attributs, tels qu'un nom d'affichage utilisateur dans l'DisplayNameattribut. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

Pour créer un utilisateur Microsoft AD AWS géré avec AWS CLI

- Ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, le nom d'utilisateur et le nom d'affichage par votre ID d'annuaire Microsoft AD AWS géré et les informations d'identification souhaitées :

```
aws ds-data create-user \  
  --directory-id d-1234567890 \  
  --sam-account-name "jane.doe" \  
  --other-attributes '{  
    "DisplayName" : { "S": "jane.doe"},  
    "Department":{ "S": "Legal"}  
  }'
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui crée un nouveau compte utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell. Vous devez inclure votre numéro d'identification de répertoire et un nom de connexion utilisateur dans votre demande. Vous pouvez également inclure d'autres attributs, tels qu'un nom d'affichage utilisateur dans l'DisplayNameattribut. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

Pour créer un utilisateur Microsoft AD AWS géré à l'aide des outils pour PowerShell

- Ouvrez et exécutez la commande suivantePowerShell, en remplaçant l'ID de répertoire, le nom d'utilisateur et le nom d'affichage par votre ID d'annuaire Microsoft AD AWS géré et les informations d'identification souhaitées :

```
New-DSDUser `
```



```
-DirectoryId d-1234567890 `
-SAMAccountName "jane.doe" `
-OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'jane.doe' }
    Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'Legal' }
}
```

Affichage et mise à jour d'un utilisateur Microsoft AD AWS géré

Utilisez la procédure suivante pour afficher ou mettre à jour les informations d'un utilisateur Microsoft AD AWS géré avec la gestion des utilisateurs et des groupes ou les données du service de AWS répertoire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Afficher les informations relatives AWS à un utilisateur de Managed Microsoft AD

Vous pouvez consulter les informations d'un utilisateur dans le AWS Management Console ou AWS CLI. Les informations de l'utilisateur incluent les informations de profil et de compte ainsi que l'adhésion au groupe.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou les données du service d'annuaire.](#)
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires.](#)
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.](#) Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM.](#)
- [Création d'un utilisateur Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez consulter les informations relatives AWS à un utilisateur de Managed Microsoft AD dans le AWS Management Console.

Pour consulter les informations relatives AWS à un utilisateur géré de Microsoft AD et à son compte à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Utilisateurs. L'onglet affiche la liste des utilisateurs de votre répertoire.
5. Sélectionnez un utilisateur. Vous êtes dirigé vers l'écran Détails de l'utilisateur. L'écran Détails de l'utilisateur affiche les informations suivantes :
 - Groupes dont l'utilisateur est membre (appartenances à des groupes)
 - Détails du profil (tels que les informations principales telles que le nom de connexion de l'utilisateur, le prénom, le nom de famille, etc.)
 - Paramètres du compte (tels que les informations du compte telles que le nom principal de l'utilisateur, le nom principal du service, le nom distinctif, etc.)
 - Statut du compte

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

AWS CLI

Avec le AWS CLI, vous pouvez consulter les informations d'un utilisateur, notamment les informations de profil et de compte et les adhésions à des groupes.

Pour consulter le profil et les détails du compte d'un utilisateur Microsoft AD AWS géré à l'aide du AWS CLI

Ce qui suit décrit comment afficher les informations d'un utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

- Pour consulter les informations d'un utilisateur, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID d'annuaire Microsoft AD AWS géré et votre nom d'utilisateur :

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Pour consulter les appartenances à un groupe d'utilisateurs

Ce qui suit décrit comment afficher l'appartenance au groupe d'un utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

- Pour consulter les appartenances à un groupe d'utilisateurs, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID d'annuaire Microsoft AD AWS géré et votre nom d'utilisateur :

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

Outils AWS pour PowerShell

Avec Outils pour PowerShell, vous pouvez consulter les informations d'un utilisateur, notamment les informations de profil et de compte, ainsi que les adhésions à des groupes.

Pour consulter le profil et les détails du compte d'un utilisateur Microsoft AD AWS géré à l'aide des outils pour PowerShell

Ce qui suit décrit comment afficher les informations d'un utilisateur Microsoft AD AWS géré à l'aide des outils pour PowerShell.

- Pour consulter les informations d'un utilisateur, ouvrez le et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID d'annuaire Microsoft AD AWS géré et votre nom d'utilisateur :

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Pour consulter les appartenances à un groupe d'utilisateurs

Ce qui suit décrit comment afficher l'appartenance à un groupe d'un utilisateur Microsoft AD AWS géré à l'aide des outils pour PowerShell.

- Pour consulter les appartenances à un groupe d'utilisateurs, ouvrez le et exécutez la commande suivantePowerShell, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID d'annuaire Microsoft AD AWS géré et votre nom d'utilisateur :

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName  
"jane.doe").Groups
```

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

Mettre à jour les informations d'un utilisateur de AWS Managed Microsoft AD

Utilisez la procédure suivante pour mettre à jour un utilisateur Microsoft AD AWS géré en utilisant la gestion des utilisateurs et des groupes ou les données du service d' AWS annuaire dans l'un ou l'autre des AWS CLI fichiers AWS Management Console, Outils AWS pour PowerShell.

 Note

La longueur minimale de l'attribut est de 1.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou les données du service d'annuaire](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer

à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

- [Création d'un utilisateur Microsoft AD AWS géré](#).

AWS Management Console

Vous pouvez mettre à jour les informations d'un utilisateur de AWS Managed Microsoft AD dans le AWS Management Console.

Pour mettre à jour les informations d'un utilisateur de AWS Managed Microsoft AD à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Utilisateurs. L'onglet affiche la liste des utilisateurs de votre répertoire.
5. Sélectionnez un utilisateur. Pour rechercher un utilisateur, entrez son nom de connexion dans le champ de recherche situé dans la section Utilisateurs. Vous êtes dirigé vers l'écran Détails de l'utilisateur.
6. Pour modifier les groupes dont l'utilisateur est membre, choisissez Groupes. Dans cet onglet, vous pouvez ajouter et supprimer l'utilisateur des groupes. Pour plus d'informations, voir [Ajouter un membre Microsoft AD AWS géré à un groupe](#).
7. Pour modifier les détails du profil de l'utilisateur, choisissez Profil, puis Modifier. Vous pouvez également choisir Actions, puis Modifier l'utilisateur. Effectuez et passez en revue vos mises à jour, puis choisissez Enregistrer.

Warning

Le nom de connexion de l'utilisateur ne peut pas être modifié une fois l'utilisateur créé.

8. Pour modifier les paramètres du compte de l'utilisateur, choisissez Paramètres du compte utilisateur. Vous pouvez également choisir Actions, puis Modifier l'utilisateur. Effectuez et passez en revue vos mises à jour, puis choisissez Enregistrer.

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

AWS CLI

Ce qui suit décrit comment formater une demande qui met à jour les informations d'un utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Lorsque vous mettez à jour le compte d'un utilisateur, vous devez inclure votre numéro d'identification de répertoire et votre nom de connexion utilisateur. Vous devez également inclure le type de mise à jour et l'attribut que vous souhaitez mettre à jour dans votre demande, par exemple un nom de famille d'utilisateur avec le Surname paramètre. Pour plus d'informations, consultez la section [Attributs des données du AWS Directory Service](#).

- Pour mettre à jour les informations d'un utilisateur, ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire, le nom d'utilisateur, le type d'utilisateur et la valeur d'attribut par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur, le type d'utilisateur et la valeur d'attribut souhaités :

```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
update-type "REPLACE" --surname "Doe"
```

Note

Lorsque vous supprimez des attributs utilisateur à l'aide de la commande [update-user CLI](#), vous devez spécifier l'attribut et la valeur exacte à supprimer. Pour déterminer les attributs utilisateur, utilisez la commande [describe-user](#).

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui met à jour les informations d'un utilisateur de AWS Managed Microsoft AD avec Outils AWS pour PowerShell.

Lorsque vous mettez à jour le compte d'un utilisateur, vous devez inclure votre numéro d'identification de répertoire et votre nom de connexion utilisateur. Vous devez également inclure le type de mise à jour et l'attribut que vous souhaitez mettre à jour dans votre demande, par exemple un nom de famille d'utilisateur avec le Surname paramètre. Pour plus d'informations, consultez la section [Attributs des données du AWS Directory Service](#).

- Pour mettre à jour les informations d'un utilisateur, ouvrez le PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire, le nom d'utilisateur, le type d'utilisateur et la valeur d'attribut par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur, le type d'utilisateur et la valeur d'attribut souhaités :

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType  
"REPLACE" -Surname "Doe"
```

Pour plus d'informations sur les attributs utilisateur, consultez [AWS Attributs des données du service de répertoire](#) la [Microsoftdocumentation](#).

Supprimer un utilisateur Microsoft AD AWS géré

Utilisez la procédure suivante pour supprimer un utilisateur Microsoft AD AWS géré avec des données de gestion des utilisateurs et des groupes ou des données de service d' AWS annuaire dans l'un ou l'autre des AWS CLI fichiers AWS Management Console, Outils AWS pour PowerShell.

Important

Lorsque vous supprimez le compte d'un utilisateur d'un annuaire, toutes les informations le concernant sont supprimées, y compris les autorisations dont dispose l'utilisateur pour accéder à son compte et à ses applications.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)

- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou les données du service d'annuaire](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Création d'un utilisateur Microsoft AD AWS géré](#).

AWS Management Console

Vous pouvez supprimer un compte utilisateur Microsoft AD AWS géré dans le AWS Management Console.

Pour supprimer un compte utilisateur Microsoft AD AWS géré avec AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Utilisateurs. L'onglet affiche la liste des utilisateurs de votre répertoire.
5. Choisissez l'utilisateur dont vous souhaitez supprimer le compte. Pour rechercher un utilisateur, entrez son nom de connexion dans le champ de recherche situé dans la section Utilisateurs. Vous êtes dirigé vers l'écran Détails de l'utilisateur.
6. Choisissez Actions. Choisissez ensuite Supprimer le compte utilisateur, puis Supprimer à nouveau le compte utilisateur.

AWS CLI

Ce qui suit décrit comment formater une demande qui supprime le compte d'un utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Pour supprimer un compte utilisateur Microsoft AD AWS géré avec AWS CLI

- Ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID de répertoire Microsoft AD AWS géré et votre nom d'utilisateur :

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui supprime le compte d'un utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell.

Pour supprimer un compte utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell

- Ouvrez PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID de répertoire Microsoft AD AWS géré et votre nom d'utilisateur :

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Désactivation d'un AWS utilisateur Microsoft AD géré

Utilisez la procédure suivante pour désactiver un utilisateur Microsoft AD AWS géré avec des données de gestion des utilisateurs et des groupes ou des données de service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Important

Lorsque vous désactivez le compte d'un utilisateur, celui-ci perd toute autorisation d'accès à son compte et à ses applications.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou les données du service d'annuaire.](#)
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires.](#)
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.](#) Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM.](#)
- [Création d'un utilisateur Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez désactiver un compte utilisateur Microsoft AD AWS géré dans le AWS Management Console.

Pour désactiver un compte utilisateur Microsoft AD AWS géré avec AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Utilisateurs. L'onglet affiche la liste des utilisateurs de votre répertoire.
5. Choisissez l'utilisateur dont vous souhaitez désactiver le compte. Vous êtes dirigé vers l'écran Détails de l'utilisateur.
6. Choisissez Actions. Choisissez ensuite Désactiver le compte utilisateur, puis Désactiver à nouveau le compte utilisateur.

 Note

Pour réactiver le compte de votre utilisateur, vous devez réinitialiser son mot de passe. Pour de plus amples informations, veuillez consulter [Réinitialisation et activation du mot de AWS passe d'un utilisateur Microsoft AD géré](#).

AWS CLI

Ce qui suit décrit comment formater une demande qui désactive un compte utilisateur Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Pour désactiver un compte utilisateur Microsoft AD AWS géré avec AWS CLI

- Ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID de répertoire Microsoft AD AWS géré et votre nom d'utilisateur :

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

 Note

Pour réactiver votre compte utilisateur, vous devez réinitialiser le mot de passe de l'utilisateur. Pour de plus amples informations, veuillez consulter [Réinitialisation et activation du mot de AWS passe d'un utilisateur Microsoft AD géré](#).

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui désactive un compte utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell.

Pour désactiver un compte utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell

- Ouvrez PowerShell ; et exécutez la commande suivante en remplaçant l'ID de répertoire et le nom d'utilisateur par votre ID de répertoire Microsoft AD AWS géré et votre nom d'utilisateur :

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

 Note

Pour réactiver votre compte utilisateur, vous devez réinitialiser le mot de passe de l'utilisateur. Pour de plus amples informations, veuillez consulter [Réinitialisation et activation du mot de passe d'un utilisateur Microsoft AD géré](#).

Réinitialisation et activation du mot de passe d'un utilisateur Microsoft AD géré

Utilisez la procédure suivante pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré afin d'activer son compte avec la gestion des utilisateurs et des groupes ou les données du service de AWS répertoire dans l'un ou l'autre des AWS CLI fichiers AWS Management Console, Outils AWS pour PowerShell.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré](#).
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Création d'un utilisateur Microsoft AD AWS géré](#).

AWS Management Console

Vous pouvez réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré pour activer son compte dans le AWS Management Console. Vous pouvez effectuer cette tâche à partir de l'écran Répertoires ou de l'écran Détails des répertoires.

Annuaire

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez Actions, puis sélectionnez Réinitialiser le mot de passe utilisateur et activer le compte.
 - a. Sous Nom de connexion utilisateur, entrez le nom de connexion de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
 - b. Sous Nouveau mot de passe, entrez le nouveau mot de passe de l'utilisateur.
 - c. Sous Confirmer le mot de passe, entrez de nouveau le nouveau mot de passe de l'utilisateur.
4. Après avoir confirmé le nouveau mot de passe de l'utilisateur, choisissez Réinitialiser le mot de passe et activer le compte.

Détails de l'annuaire

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Utilisateurs. L'onglet affiche la liste des utilisateurs de votre répertoire.
5. Sélectionnez l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
6. Choisissez Actions, puis sélectionnez Réinitialiser le mot de passe utilisateur et activer le compte.
 - a. Sous Nouveau mot de passe, entrez le nouveau mot de passe de l'utilisateur.
 - b. Sous Confirmer le mot de passe, entrez de nouveau le nouveau mot de passe de l'utilisateur.

- Après avoir confirmé le nouveau mot de passe de l'utilisateur, choisissez Réinitialiser le mot de passe et activer le compte.

AWS CLI

Vous pouvez réinitialiser le mot de passe d'un utilisateur de AWS Managed Microsoft AD pour activer son compte avec la CLI AWS Directory Service Data.

Note

La commande de réinitialisation du mot de passe de l'utilisateur utilise `aws ds`.

Pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré à l'aide du AWS CLI

- Pour réinitialiser le mot de passe d'un utilisateur, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, le nom d'utilisateur et le mot de passe par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur et les informations d'identification souhaitées :

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "your-password"
```

Outils AWS pour PowerShell

Vous pouvez réinitialiser le mot de passe d'un utilisateur de AWS Managed Microsoft AD pour activer son compte avec Outils AWS pour PowerShell.

Pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré avec Outils AWS pour PowerShell

- Pour réinitialiser le mot de passe d'un utilisateur, ouvrez le et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire, le nom d'utilisateur et le mot de passe par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur et les informations d'identification souhaitées :

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword  
"your-password"
```

Création d'un groupe Microsoft AD AWS géré

Utilisez la procédure suivante pour créer un groupe Microsoft AD AWS géré avec des données de gestion des utilisateurs et des groupes ou des données de service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

AWS Management Console

Vous pouvez créer un nouveau groupe Microsoft AD AWS géré dans le AWS Management Console. Lorsque vous créez un nouveau groupe, vous spécifiez les détails du groupe et déterminez le [type et la portée du groupe](#). Vous avez également la possibilité d'ajouter des utilisateurs et des groupes d'enfants à votre nouveau groupe ou d'ajouter votre nouveau groupe à un groupe de parents.

Pour créer un groupe Microsoft AD AWS géré avec AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.

2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez le groupe. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez Créer un groupe. Vous êtes dirigé vers une procédure qui vous permet de terminer la création de votre nouveau groupe.
6. La page Spécifier les détails du groupe s'ouvre. Entrez un nom de groupe. Les noms de groupes doivent répondre aux conditions suivantes :
 - Doit être un nom de groupe unique
 - Peut comporter jusqu'à 64 caractères
 - Ne peut contenir que des caractères alphanumériques
 - ~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/

 Warning

Le nom du groupe ne peut pas être modifié une fois le groupe créé.

7. Choisissez le type de groupe parmi les suivants :
 - Sécurité
 - Distribution
 - Pour en savoir plus, veuillez consulter la section [the section called "Type de groupe"](#).
8. Choisissez l'étendue du groupe parmi les options suivantes :
 - Domaine local
 - Universel
 - Solution internationale
 - Vous pouvez activer Comparer les étendues pour afficher un graphique des similitudes et des différences entre les étendues de groupe. Pour en savoir plus, veuillez consulter la section [the section called "Étendue du groupe"](#).
9. Après avoir fourni les informations principales et les méthodes de contact, choisissez Next.

10. La page Ajouter des utilisateurs au groupe - Facultatif s'ouvre et vous pouvez ajouter des utilisateurs au nouveau groupe. Pour trouver un utilisateur à ajouter au groupe, entrez son nom de connexion dans le champ de recherche de la section Utilisateurs. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe, puis cliquez sur Suivant.
11. La page Ajouter des groupes d'enfants - Facultatif s'ouvre et vous pouvez ajouter des groupes existants au nouveau groupe. Les groupes existants deviennent des groupes enfants du groupe nouvellement créé. Lorsque vous ajoutez un groupe enfant à votre groupe, celui-ci devient le groupe parent et le groupe enfant hérite de tous les rôles et autorisations de votre groupe. Pour trouver des groupes à ajouter, entrez le nom du groupe dans le champ de recherche de la section Ajouter des groupes d'enfants. Sélectionnez les groupes d'enfants que vous souhaitez ajouter au nouveau groupe, puis cliquez sur Suivant.
12. La page Ajouter des groupes parents - Facultatif s'ouvre et vous pouvez ajouter le nouveau groupe aux groupes existants. Le nouveau groupe devient le groupe parent des groupes existants. Lorsque vous ajoutez votre groupe à un groupe parent, celui-ci devient le groupe enfant et hérite de tous les rôles et autorisations du groupe parent. Pour trouver des groupes à ajouter, entrez le nom du groupe dans le champ de recherche sous la section Ajouter des groupes parents. Sélectionnez les groupes parents que vous souhaitez ajouter au nouveau groupe, puis cliquez sur Suivant.
13. Sur la page Réviser et créer un groupe, passez en revue vos choix, puis choisissez Créer un groupe.

AWS CLI

Ce qui suit décrit comment formater une demande qui crée un groupe Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data. Lorsque vous créez un nouveau groupe, vous devez inclure votre numéro d'identification de répertoire et un nom de groupe. Vous pouvez également ajouter d'autres attributs, tels qu'un nom d'affichage de groupe avec l'attribut `DisplayName`. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

Pour créer un groupe Microsoft AD AWS géré avec AWS CLI

- Ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID du répertoire, le nom d'utilisateur et le nom d'affichage du groupe par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur et le nom d'affichage du groupe souhaité :

```
aws ds-data create-group \  
  --directory-id d-1234567890 \  
  --sam-account-name "your-group-name" \  
  --other-attributes '{  
    "DisplayName": { "S": "myGroupDisplayName"}  
    "Description":{ "S": "myGroupDescription"}  
  }'
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui crée un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell. Lorsque vous créez un nouveau groupe, vous devez inclure votre numéro d'identification de répertoire et un nom de groupe. Vous pouvez également ajouter d'autres attributs, tels qu'un nom d'affichage de groupe avec l'AttributeNameattribut. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

Pour créer un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell

- Ouvrez et exécutez la commande suivantePowerShell, en remplaçant l'ID du répertoire, le nom d'utilisateur et le nom d'affichage du groupe par votre ID d'annuaire Microsoft AD AWS géré, votre nom d'utilisateur et le nom d'affichage du groupe souhaité :

```
New-DSDGroup `   
  -DirectoryId d-1234567890 `   
  -SAMAccountName "your-group-name" `   
  -OtherAttribute @{  
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =   
'myGroupDisplayName' }   
    Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =   
'myGroupDescription' }   
  }
```

Afficher et mettre à jour les détails d'un groupe Microsoft AD AWS géré

Utilisez la procédure suivante pour afficher ou mettre à jour les détails d'un groupe Microsoft AD AWS géré avec la gestion des utilisateurs et des groupes ou les données du service de AWS répertoire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Afficher les détails d'un groupe Microsoft AD AWS géré

Vous pouvez consulter ou mettre à jour les détails d'un groupe dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data.](#)
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires.](#)
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.](#) Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM.](#)
- [Création d'un groupe Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez consulter les détails d'un groupe Microsoft AD AWS géré dans le AWS Management Console.

Pour consulter les détails du groupe AWS Managed Microsoft AD à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez le groupe. L'onglet affiche la liste des groupes de votre Région AWS.

5. Choisissez un groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe. L'écran des détails du groupe affiche les informations suivantes :
 - L'onglet Membres répertorie les utilisateurs et les groupes d'enfants membres de votre groupe.
 - L'onglet Groupes de parents répertorie les groupes de parents dont votre groupe est membre.
 - L'onglet Propriétés répertorie les propriétés du groupe (telles que les informations principales telles que le nom du groupe, le nom d'affichage du groupe, etc.).

AWS CLI

Vous pouvez consulter les détails d'un groupe Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Pour consulter les détails d'un groupe Microsoft AD AWS géré à l'aide du AWS CLI

Ce qui suit décrit comment afficher les détails d'un groupe Microsoft AD AWS géré à l'aide du AWS CLI.

- Pour afficher les détails d'un groupe, ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom du groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom du groupe :

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

Pour afficher les membres d'un groupe Microsoft AD AWS géré à l'aide du AWS CLI

Ce qui suit décrit comment afficher les membres d'un groupe Microsoft AD AWS géré avec le AWS CLI.

- Pour afficher les détails d'un groupe, ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom du groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom du groupe :

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

Outils AWS pour PowerShell

Vous pouvez consulter les détails d'un groupe Microsoft AD AWS géré à l'aide de Outils AWS pour PowerShell.

Pour consulter les détails d'un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell

Ce qui suit décrit comment afficher les détails d'un groupe Microsoft AD AWS géré à l'aide des outils pour PowerShell.

- Pour afficher les détails d'un groupe, ouvrez le PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom du groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom du groupe :

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Pour afficher les membres d'un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell

Ce qui suit décrit comment afficher les membres d'un groupe Microsoft AD AWS géré à l'aide des outils pour PowerShell.

- Pour afficher les détails d'un groupe, ouvrez le PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom du groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom du groupe :

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-name") .Members
```

Mettre à jour les informations d'un groupe Microsoft AD AWS géré

Utilisez la procédure suivante pour mettre à jour les informations d'un groupe Microsoft AD AWS géré avec la gestion des utilisateurs et des groupes ou les données du service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Création d'un groupe Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez mettre à jour les informations d'un groupe à l'aide du AWS Management Console. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#)

Pour mettre à jour les informations d'un groupe Microsoft AD AWS géré à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez le groupe. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe.

6. Pour modifier les utilisateurs et les groupes d'enfants membres de votre groupe, sélectionnez Membres. Dans cet onglet, vous pouvez ajouter et supprimer des utilisateurs et des groupes d'enfants de votre groupe. Pour de plus amples informations, veuillez consulter [Ajouter et supprimer des membres dans des groupes et des groupes dans des groupes](#).
7. Pour modifier les groupes de parents dont votre groupe est membre, choisissez Groupes de parents. Dans cet onglet, vous pouvez ajouter et supprimer votre groupe des groupes parents. Pour de plus amples informations, veuillez consulter [Ajouter et supprimer des membres dans des groupes et des groupes dans des groupes](#).
8. Pour modifier les propriétés de votre groupe, choisissez Propriétés, puis Modifier. Vous pouvez également choisir Actions, puis Modifier le groupe. Effectuez et passez en revue vos mises à jour, puis choisissez Enregistrer.

AWS CLI

Ce qui suit décrit comment formater une demande qui met à jour les détails d'un groupe Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Lorsque vous mettez à jour un groupe, vous devez inclure votre numéro d'identification de répertoire et le nom du groupe. Vous devez également inclure le type de mise à jour et l'attribut que vous souhaitez mettre à jour dans votre demande, par exemple une adresse e-mail de groupe avec le EmailAddress paramètre. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

- Pour mettre à jour les informations d'un groupe Microsoft AD AWS géré à l'aide du AWS CLI

Pour mettre à jour les informations d'un groupe, ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID de répertoire, le nom du groupe, le type de mise à jour et l'attribut par votre ID d'annuaire Microsoft AD AWS géré, le nom du groupe, le type de mise à jour et l'attribut souhaités :

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui met à jour les détails d'un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell.

Lorsque vous mettez à jour un groupe, vous devez inclure votre numéro d'identification de répertoire et le nom du groupe. Vous devez également inclure le type de mise à jour et l'attribut que vous souhaitez mettre à jour dans votre demande, par exemple une adresse e-mail de groupe avec le `EmailAddress` paramètre. Pour plus d'informations, consultez [AWS Attributs des données du service de répertoire](#) et [Type de groupe et étendue du groupe](#).

- Pour mettre à jour les informations d'un groupe Microsoft AD AWS géré avec Outils AWS pour PowerShell

Pour mettre à jour les informations d'un groupe, ouvrez le PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire, le nom du groupe, le type de mise à jour et l'attribut par votre ID d'annuaire Microsoft AD AWS géré, le nom du groupe, le type de mise à jour et l'attribut souhaités :

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -  
UpdateType "REPLACE" -GroupScope "global"
```

Suppression d'un groupe Microsoft AD AWS géré

Utilisez la procédure suivante pour supprimer un groupe Microsoft AD AWS géré avec des données de gestion des utilisateurs et des groupes ou des données de service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Important

Lorsque vous supprimez un groupe, toutes les informations le concernant sont supprimées, y compris les autorisations dont les membres du groupe héritent.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré](#).
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).

- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Créez un groupe Microsoft AD AWS géré](#).

AWS Management Console

Vous pouvez supprimer un groupe Microsoft AD AWS géré dans le AWS Management Console.

Pour supprimer un groupe Microsoft AD AWS géré à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez le groupe. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez le groupe que vous souhaitez supprimer. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe.
6. Choisissez Supprimer un groupe. Une boîte de dialogue apparaît dans laquelle vous pouvez sélectionner Confirmer pour supprimer le groupe.

AWS CLI

Ce qui suit décrit comment formater une demande qui supprime un groupe Microsoft AD AWS géré à l'aide de la CLI AWS Directory Service Data.

Pour supprimer un groupe Microsoft AD AWS géré à l'aide du AWS CLI

- Ouvrez le AWS CLI et exécutez la commande suivante, en remplaçant l'ID du répertoire et le nom du groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom de groupe :

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui supprime un groupe Microsoft AD AWS géré avec le Outils AWS pour PowerShell.

Pour supprimer un groupe Microsoft AD AWS géré à l'aide du Outils AWS pour PowerShell

- Ouvrez PowerShell et exécutez la commande suivante, en remplaçant l'ID de répertoire et le nom de groupe par votre ID d'annuaire Microsoft AD AWS géré et le nom de groupe :

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Ajouter et supprimer des membres de AWS Managed Microsoft AD à des groupes et des groupes à des groupes

Avec l'[API AWS Directory Service Data](#), un membre peut être un utilisateur, un groupe ou un ordinateur. Un utilisateur représente une personne ou une entité qui peut accéder à votre annuaire. Les groupes vous permettent d'accorder ou de refuser des autorisations à plusieurs utilisateurs à la fois.

Utilisez les procédures suivantes pour ajouter ou supprimer un utilisateur Microsoft AD AWS géré dans un groupe ou un groupe dans un autre groupe avec des données de gestion des utilisateurs et des groupes ou des données de service d' AWS annuaire dans le AWS Management Console AWS CLI, ou Outils AWS pour PowerShell.

Ajouter un utilisateur à un groupe

Utilisez la procédure suivante pour ajouter un utilisateur Microsoft AD AWS géré à un groupe dont la gestion des utilisateurs et des groupes ou les données du service d' AWS annuaire se trouvent soit dans le AWS Management Console AWS CLI, soit Outils AWS pour PowerShell.

⚠ Important

Lorsque vous ajoutez un utilisateur Microsoft AD AWS géré à un groupe, l'utilisateur hérite des rôles et des autorisations attribués au groupe. Ces rôles et autorisations font partie des appartenances aux groupes de l'utilisateur.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data.](#)
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires.](#)
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.](#) Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess.](#) Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM.](#)
- [Créez un utilisateur Microsoft AD AWS géré.](#)
- [Créez un groupe Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez ajouter un membre de AWS Managed Microsoft AD à un groupe avec le AWS Management Console.

Pour ajouter un utilisateur Microsoft AD AWS géré à un groupe avec AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.

3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Groupes. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Vous êtes dirigé vers l'écran des détails du groupe.
6. Choisissez Membres. L'onglet affiche une liste des utilisateurs et des groupes d'enfants par type de membre dans votre groupe.
7. Sous l'onglet Membres, choisissez Ajouter un membre.
8. Sous Membres, sélectionnez l'utilisateur que vous souhaitez ajouter à votre groupe, puis choisissez Ajouter un membre au groupe. Pour rechercher des membres, entrez le nom de connexion des utilisateurs et le nom du groupe pour les groupes dans le champ de recherche de la section Membres.

AWS CLI

Ce qui suit décrit comment formater une demande qui ajoute un membre de AWS Managed Microsoft AD à un groupe à l'aide de la CLI AWS Directory Service Data.

Pour ajouter un utilisateur Microsoft AD AWS géré à un groupe avec AWS CLI

- Pour ajouter un utilisateur à un groupe, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré et les noms de groupe et de membre :

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui ajoute un membre Microsoft AD AWS géré à un groupe avec Outils AWS pour PowerShell.

Pour ajouter un utilisateur Microsoft AD AWS géré à un groupe avec Outils AWS pour PowerShell

- Pour ajouter un utilisateur à un groupe, ouvrez le et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré et les noms de groupe et de membre :


```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -  
MemberName "jane.doe"
```

Supprimer un utilisateur d'un groupe

Avec l'[API AWS Directory Service Data](#), un membre peut être un utilisateur, un groupe ou un ordinateur. Un utilisateur représente une personne ou une entité qui peut accéder à votre annuaire. Les groupes vous permettent d'accorder ou de refuser des autorisations à plusieurs utilisateurs à la fois.

Utilisez la procédure suivante pour supprimer un utilisateur Microsoft AD AWS géré d'un groupe dont la gestion des utilisateurs et des groupes ou les données du service d' AWS annuaire se trouvent soit dans le AWS Management Console AWS CLI, soit Outils AWS pour PowerShell.

Important

Lorsque vous supprimez un utilisateur Microsoft AD AWS géré d'un groupe, il perd l'accès aux rôles et aux autorisations attribués au groupe. Ces rôles et autorisations font partie des adhésions au groupe.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Créez un utilisateur Microsoft AD AWS géré.](#)

- [Créez un groupe Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez supprimer un membre Microsoft AD AWS géré d'un groupe avec le AWS Management Console.

Pour supprimer un utilisateur Microsoft AD AWS géré d'un groupe doté du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe.
6. Choisissez Membres. L'onglet affiche une liste des utilisateurs et des groupes d'enfants par type de membre dans votre groupe.
7. Sélectionnez l'utilisateur que vous souhaitez supprimer de votre groupe, puis choisissez Supprimer. Pour rechercher des utilisateurs, entrez le nom de connexion de l'utilisateur dans le champ de recherche sous la section Membres.
8. Confirmez que vous souhaitez supprimer l'utilisateur de votre groupe, puis choisissez de nouveau Supprimer.

AWS CLI

Ce qui suit décrit comment formater une demande qui supprime un membre de AWS Managed Microsoft AD d'un groupe à l'aide de la CLI AWS Directory Service Data.

Pour supprimer un utilisateur Microsoft AD AWS géré d'un groupe avec AWS CLI

- Pour supprimer un utilisateur d'un groupe, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui supprime un membre Microsoft AD AWS géré d'un groupe avec Outils AWS pour PowerShell.

Pour supprimer un utilisateur Microsoft AD AWS géré d'un groupe avec Outils AWS pour PowerShell

- Pour supprimer un utilisateur d'un groupe, ouvrez le et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

Ajouter un groupe à un groupe

Lorsque vous ajoutez un groupe Microsoft AD AWS géré à un autre groupe, les groupes partagent une relation parent-enfant. Le groupe d'enfants a accès aux rôles et aux autorisations attribués au groupe parent. Vous pouvez ajouter un groupe d'enfants à votre groupe et votre groupe à un groupe de parents.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data](#).
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser

des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).

- [Créez un groupe Microsoft AD AWS géré](#).

AWS Management Console

Vous pouvez ajouter un groupe Microsoft AD AWS géré à un groupe avec le AWS Management Console.

Pour ajouter un groupe d'enfants à votre groupe à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe.
6. Choisissez Membres. L'onglet affiche une liste des utilisateurs et des groupes d'enfants par type de membre dans votre groupe.
7. Choisissez Ajouter un membre.
8. Sous Membres, sélectionnez le ou les groupes d'enfants que vous souhaitez ajouter à votre groupe, puis choisissez Ajouter un membre au groupe.

Pour ajouter un groupe parent à un groupe doté du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.

4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes. Vous êtes dirigé vers l'écran des détails du groupe.
6. Choisissez Groupes de parents. L'onglet affiche la liste des groupes dont votre groupe est membre.
7. Choisissez Ajouter des groupes de parents.
8. Sous Groupes, sélectionnez le ou les groupes auxquels vous souhaitez ajouter votre groupe, puis choisissez à nouveau Ajouter des groupes parents.

AWS CLI

Ce qui suit décrit comment formater une demande qui ajoute un groupe Microsoft AD AWS géré à un groupe à l'aide de la CLI AWS Directory Service Data.

Pour ajouter un groupe d'enfants à votre groupe à l'aide du AWS CLI

- Pour ajouter un groupe enfant à un groupe parent, ouvrez le et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui ajoute un groupe Microsoft AD AWS géré à un groupe avec Outils AWS pour PowerShell.

Pour ajouter un groupe d'enfants à votre groupe avec Outils AWS pour PowerShell

- Pour ajouter un groupe enfant à un groupe parent, ouvrez le et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Supprimer un groupe d'un groupe

Lorsque vous supprimez un groupe Microsoft AD AWS géré d'un autre groupe, les groupes ne partagent plus de relation parent-enfant. Le groupe enfant perd l'accès aux rôles et aux autorisations attribués au groupe parent. Vous pouvez supprimer un groupe d'enfants de votre groupe et votre groupe d'un groupe de parents.

Avant de commencer l'une ou l'autre des procédures, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data.](#)
- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires.](#)
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions.](#) Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM.](#)
- [Créez un groupe Microsoft AD AWS géré.](#)

AWS Management Console

Vous pouvez supprimer un groupe Microsoft AD AWS géré vers un groupe doté du AWS Management Console.

Pour supprimer un groupe d'enfants de votre groupe à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.

4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Vous êtes dirigé vers l'écran des détails du groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes.
6. Choisissez Membres. L'onglet affiche une liste des utilisateurs et des groupes d'enfants par type de membre dans votre groupe.
7. Sélectionnez le ou les groupes d'enfants que vous souhaitez supprimer de votre groupe, puis choisissez Supprimer.
8. Confirmez le ou les groupes d'enfants que vous souhaitez supprimer de votre groupe, puis choisissez de nouveau Supprimer.

Pour supprimer votre groupe d'un groupe parent à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez un groupe. Vous êtes dirigé vers l'écran des détails du groupe. Pour rechercher des groupes, entrez le nom du groupe dans le champ de recherche sous la section Groupes.
6. Choisissez Groupes de parents. L'onglet affiche la liste des groupes dont votre groupe est membre.
7. Sélectionnez le groupe parent dont vous souhaitez supprimer votre groupe, puis choisissez Supprimer les groupes parents.
8. Confirmez le groupe parent dont vous souhaitez supprimer votre groupe, puis choisissez à nouveau Supprimer les groupes parents.

AWS CLI

Ce qui suit décrit comment formater une demande qui supprime un groupe Microsoft AD AWS géré vers un groupe à l'aide de la CLI AWS Directory Service Data.

- Pour supprimer un groupe d'enfants d'un groupe de parents à l'aide du AWS CLI

Pour ajouter et supprimer un groupe enfant d'un groupe parent, ouvrez et exécutez la commande suivante AWS CLI, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

Outils AWS pour PowerShell

Ce qui suit décrit comment formater une demande qui supprime un groupe Microsoft AD AWS géré vers un groupe avec Outils AWS pour PowerShell.

- Pour supprimer un groupe d'enfants d'un groupe de parents avec Outils AWS pour PowerShell

Pour ajouter et supprimer un groupe enfant d'un groupe parent, ouvrez et exécutez la commande suivante PowerShell, en remplaçant l'ID de répertoire, les noms de groupe et de membre par votre ID d'annuaire Microsoft AD AWS géré, les noms de groupe et de membre :

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Copier les appartenances AWS à un groupe Microsoft AD géré dans le AWS Management Console

Vous pouvez copier les adhésions à des groupes d'un utilisateur de AWS Managed Microsoft AD vers un autre utilisateur dans le AWS Management Console. Les appartenances à un groupe sont les rôles et les autorisations dont un utilisateur hérite lorsque vous l'ajoutez à un groupe.

Avant de commencer cette procédure, vous devez effectuer les opérations suivantes :

- [Création de votre AWS compte Microsoft AD géré.](#)
- Pour utiliser la gestion des utilisateurs et des groupes ou la CLI AWS Directory Service Data, celle-ci doit être activée. Pour plus d'informations, voir [Activer la gestion des utilisateurs et des groupes ou Directory Service Data.](#)

- Vous ne pouvez activer cette fonctionnalité qu'à partir du serveur principal Région AWS de votre annuaire. Pour plus d'informations, voir Régions [principales et régions supplémentaires](#).
- Vous devez disposer des autorisations IAM nécessaires pour utiliser les données du service de AWS répertoire. Pour de plus amples informations, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#). Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, vous pouvez utiliser des politiques AWS gérées telles que [AWS politique gérée : AWSDirectoryServiceDataFullAccess](#) ou [AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess](#). Pour plus d'informations, consultez [Bonnes pratiques de sécurité dans IAM](#).
- [Créez un groupe Microsoft AD AWS géré](#).

Pour copier les appartenances à des groupes Microsoft AD AWS gérés à l'aide du AWS Management Console

1. Ouvrez la Directory Service console à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Dans le volet de navigation, choisissez Active Directory, puis Directories. Vous êtes dirigé vers l'écran Répertoires où vous pouvez consulter la liste des répertoires de votre Région AWS.
3. Choisissez un répertoire. Vous êtes dirigé vers l'écran des détails du répertoire.
4. Choisissez Groupes. L'onglet affiche la liste des groupes de votre Région AWS.
5. Choisissez l'utilisateur dont vous souhaitez copier l'appartenance au groupe sur le compte. Pour rechercher un utilisateur, entrez son nom de connexion dans le champ de recherche situé dans la section Utilisateurs. Vous êtes dirigé vers l'écran Détails de l'utilisateur.
6. Choisissez Copier toutes les adhésions au groupe. Vous êtes dirigé vers une procédure dans laquelle vous pouvez spécifier les groupes que vous souhaitez copier.
 - a. Pour Verify groups to copy, sous Groupes à copier, sélectionnez les groupes avec des rôles et des autorisations que vous souhaitez copier, puis choisissez Next.
 - b. Pour Sélectionner le compte de destination, sous Type de compte, choisissez Compte utilisateur existant pour copier les adhésions à un groupe dans un compte utilisateur existant. Vous pouvez également choisir Nouveau compte utilisateur pour créer un nouvel utilisateur et copier les adhésions aux groupes dans le nouveau compte utilisateur. Pour trouver un groupe, entrez le nom du groupe dans le champ de recherche sous la section Groupes sélectionnés.

- i. (Facultatif) Si vous choisissez Compte utilisateur existant, sélectionnez les comptes de destination dans lesquels vous souhaitez copier les rôles et les autorisations, puis cliquez sur Suivant.
- ii. (Facultatif) Si vous choisissez Nouveau compte utilisateur, suivez la procédure, puis choisissez Suivant. Pour plus d'informations sur la création d'un utilisateur, consultez [Création d'un utilisateur](#).
- c. Pour Réviser et copier les adhésions à un groupe, passez en revue vos choix, puis choisissez Copier l'adhésion au groupe.

Gérez les utilisateurs et les groupes avec une EC2 instance Amazon

Cette section inclut les procédures de gestion des utilisateurs et des groupes avec une EC2 instance Amazon jointe à votre AWS Managed Microsoft AD.

Nous vous recommandons de gérer les utilisateurs et les groupes avec une EC2 instance Amazon si l'API Directory Service Data ne prend pas en charge votre cas d'utilisation. Pour plus d'informations, consultez le manuel [AWS Directory Service Data API Reference](#).

Note

Avant de terminer l'une des procédures décrites dans les rubriques suivantes, vous devez installer les outils d'administration Active Directory. Pour plus d'informations, voir [Installer les outils d'administration Active Directory](#).

Rubriques

- [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#)
- [Création d'un utilisateur Microsoft AD AWS géré](#)
- [Supprimer le compte d'un utilisateur avec une EC2 instance Amazon](#)
- [Réinitialisation d'un AWS mot de passe utilisateur Microsoft AD géré](#)
- [Création d'un groupe Microsoft AD AWS géré](#)
- [Ajouter un utilisateur Microsoft AD AWS géré à un groupe](#)

Installation des outils d'administration Active Directory pour Microsoft AD AWS géré

Vous pouvez gérer votre annuaire Microsoft AD Active Directory AWS géré à l'aide de Active Directory Domain Services and Active Directory Lightweight Directory Services Tools. Pour les utiliser Active Directory Domain Services and Active Directory Lightweight Directory Services Tools, vous devez les installer. Les procédures suivantes vous expliquent comment installer ces outils sur une instance Amazon EC2 Windows Server ou à l'aide d'une PowerShell commande. Vous pouvez également lancer une EC2 instance d'administration d'annuaire sur laquelle ces outils sont déjà installés.

EC2 Windows Server instance

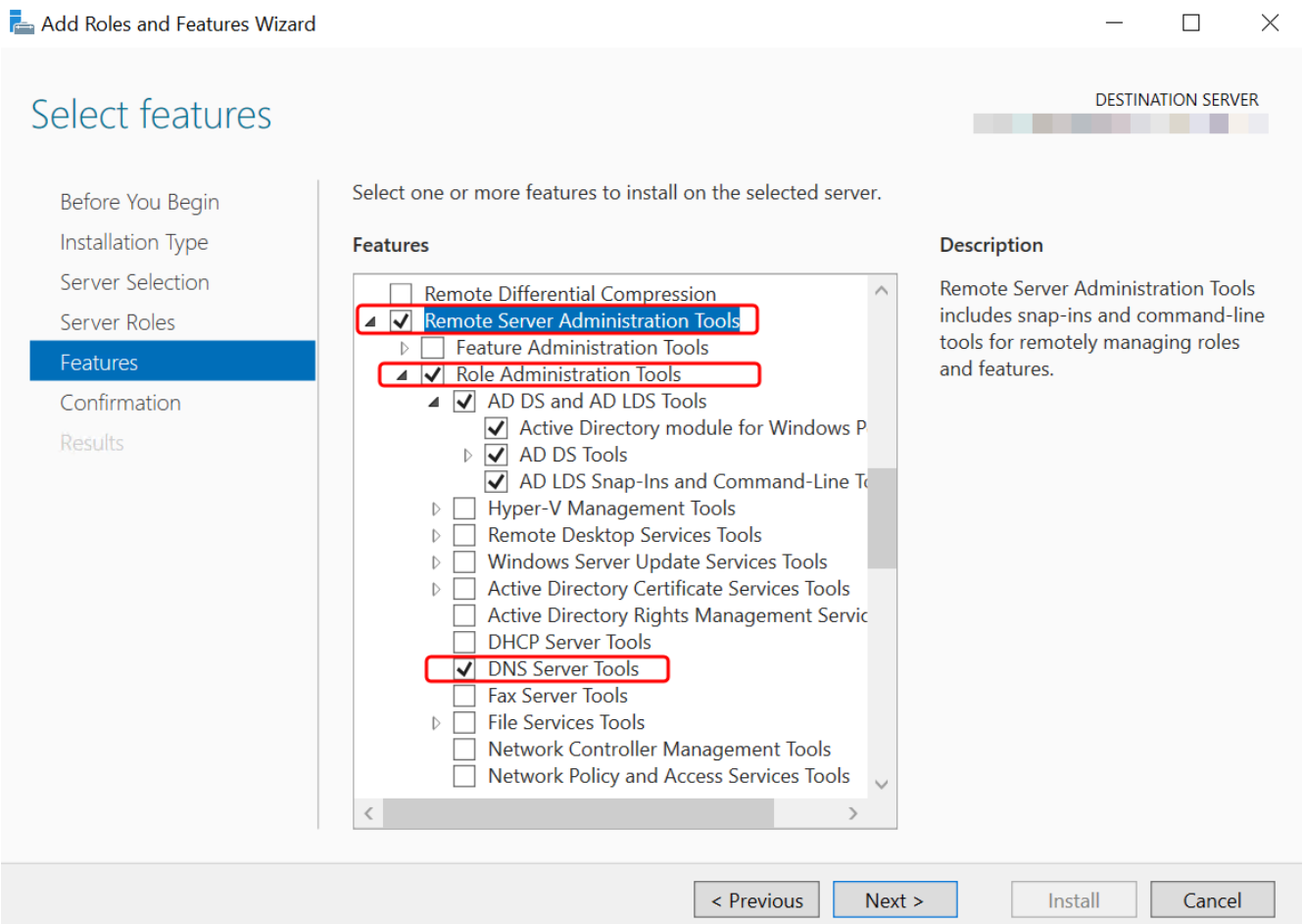
Avant de commencer cette procédure, effectuez les opérations suivantes :

1. Créez un répertoire Microsoft AD Active Directory AWS géré. Pour de plus amples informations, veuillez consulter [Création de votre AWS compte Microsoft AD géré](#).
2. Lancez et joignez une instance EC2 Windows Server à votre répertoire Microsoft AD Active Directory AWS géré. L' EC2 instance a besoin des politiques suivantes pour créer des utilisateurs et des groupes : **AmazonSSMManagedInstanceCore** et **AmazonSSMDirectoryServiceAccess**. Pour plus d'informations, consultez [Lancement d'une instance d'administration d'annuaire dans votre annuaire Microsoft AD Active Directory AWS géré](#) et [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).
3. Vous aurez besoin des informations d'identification de votre administrateur de domaine Active Directory. Ces informations d'identification ont été créées lors de la création de AWS Managed Microsoft AD. Si vous avez suivi la procédure décrite dans [Création de votre AWS compte Microsoft AD géré](#), votre nom d'utilisateur d'administrateur inclut votre nom NetBIOS, **corp** \admin

Installation des outils d'administration Active Directory sur une instance EC2 Windows de serveur

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la EC2 console Amazon, choisissez Instances, sélectionnez l'instance Windows Server, puis sélectionnez Connect.
3. Dans la page Se connecter à l'instance, sélectionnez Client RDP.
4. Dans l'onglet Client RDP, sélectionnez Télécharger le fichier Bureau à distance, puis choisissez Obtenir le passe pour récupérer votre mot de passe.

5. Dans le champ Obtenir le mot de passe Windows, sélectionnez Chargement du fichier de clé privée. Choisissez le fichier de clé privée .pem associé à l'instance Windows Server. Après avoir chargé le fichier de clé privée, sélectionnez Déchiffrer le mot de passe.
6. Dans la boîte de dialogue de sécurité Windows, copiez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter. Le nom d'utilisateur peut être dans les formats suivants : **NetBIOS-Name\admin** ou **DNS-Name\admin**. Par exemple, **corp\admin** ce serait le nom d'utilisateur si vous avez suivi la procédure dans [Création de votre AWS compte Microsoft AD géré](#).
7. Une fois connecté à l'instance Windows Server, ouvrez le Gestionnaire de serveur dans le menu Démarrer en choisissant Gestionnaire de serveur.
8. Dans le tableau de bord du Gestionnaire de serveur, choisissez Ajouter des rôles et des fonctionnalités.
9. Dans l'Assistant Ajout de rôles et de fonctionnalités, choisissez Type d'installation, sélectionnez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
10. Sous Sélection de serveur, vérifiez que le serveur local est sélectionné, puis choisissez Fonctionnalités dans le volet de navigation de gauche.
11. Dans l'arborescence Fonctionnalités, sélectionnez et ouvrez Outils d'administration de serveur distant, Outils d'administration de rôles et Outils AD DS et AD LDS. Lorsque les outils AD DS et AD LDS sont sélectionnés, le module Active Directory pour, les outils AD DSPowerShell, les composants logiciels enfichables et les outils de ligne de commande AD LDS sont sélectionnés. Faites défiler la page vers le bas et sélectionnez Outils du serveur DNS, puis cliquez sur Suivant.



12. Passez en revue les informations, puis choisissez Installer. Lorsque l'installation des fonctionnalités est terminée, les outils Active Directory Domain Services et Active Directory Lightweight Directory Services sont disponibles sur l'écran Démarrer dans le dossier Outils d'administration.

PowerShell

Vous pouvez installer les outils d'administration Active Directory à l'aide de PowerShell. Par exemple, vous pouvez installer les outils d'administration à distance Active Directory à partir d'une PowerShell invite en utilisant `Install-WindowsFeature RSAT-ADDS`. Pour plus d'informations, consultez [Install- WindowsFeature](#) sur le site Web de Microsoft.

Directory administration instance

Vous pouvez lancer une EC2 instance d'administration d'annuaire dans AWS Management Console laquelle les services de domaine Active Directory et les outils Active Directory Lightweight Directory Services sont déjà installés en suivant les procédures décrites

dans [Lancement d'une instance d'administration d'annuaire dans votre annuaire Microsoft AD Active Directory AWS géré](#).

Création d'un utilisateur Microsoft AD AWS géré

Vous pouvez créer des utilisateurs Microsoft AD AWS gérés à l'aide des outils d'administration Active Directory et PowerShell. Avant de créer un utilisateur avec les outils d'administration Active Directory, vous devez effectuer la procédure dans [Installation des outils d'administration Active Directory pour Microsoft AD AWS géré](#).

Active Directory Administration Tools

Utilisez la procédure suivante pour créer un utilisateur Microsoft AD AWS géré avec les outils d'administration Active Directory.

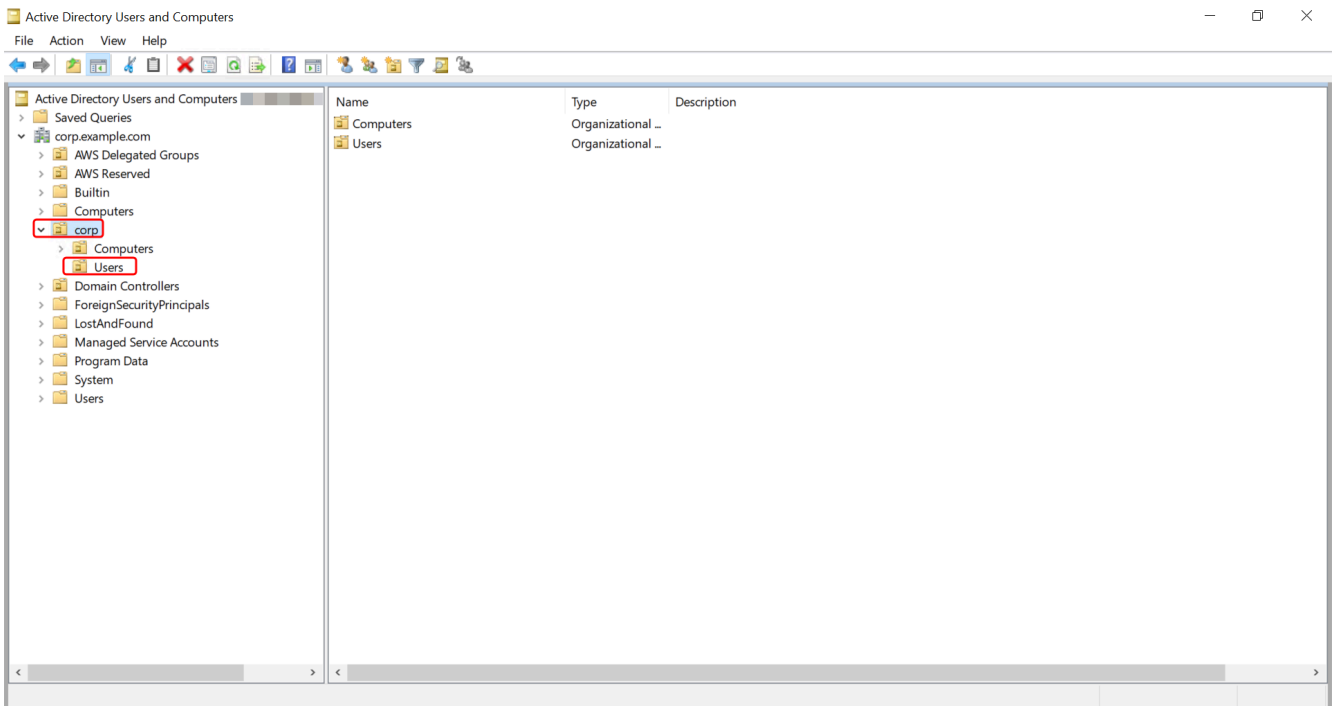
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous le nom NetBIOS de votre répertoire ou dans laquelle vous souhaitez enregistrer votre utilisateur (par exemple, **corp\Users**). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).



4. Dans le menu Action, choisissez Nouveau, puis sélectionnez Utilisateur pour ouvrir l'assistant de création d'utilisateurs.
5. Sur la première page de l'assistant, entrez les valeurs des champs suivants, puis sélectionnez Suivant.
 - Prénom
 - Nom
 - Nom de connexion de l'utilisateur
6. Sur la deuxième page de l'assistant, entrez un mot de passe temporaire dans Mot de passe et Confirmer le mot de passe. Assurez-vous que l'utilisateur doit modifier le mot de passe lors de sa prochaine connexion. Aucune autre option ne doit être sélectionnée. Choisissez Suivant.
7. Sur la troisième page de l'assistant Nouvel utilisateur, vérifiez que les informations du nouvel utilisateur sont correctes, puis choisissez Terminer. Le nouvel utilisateur s'affiche dans le dossier Utilisateurs.

PowerShell

Utilisez la procédure suivante pour créer un utilisateur Microsoft AD AWS géré avec PowerShell.

1. Connectez-vous à l'instance jointe à votre domaine Active Directory en tant qu'administrateur Active Directory.
2. Ouvrir PowerShell.
3. Tapez la commande suivante en remplaçant le nom **jane.doe** d'utilisateur par le nom d'utilisateur de l'utilisateur que vous souhaitez créer. Vous serez invité PowerShell à fournir un mot de passe pour le nouvel utilisateur. Pour plus d'informations sur les exigences relatives à la complexité des mots de passe Active Directory, consultez [Microsoftla documentation](#). Pour plus d'informations sur la ADUser commande New-, consultez [Microsoftla documentation](#).

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -  
AsSecureString 'Password')
```

Supprimer le compte d'un utilisateur avec une EC2 instance Amazon

Vous pouvez utiliser la procédure suivante pour supprimer un utilisateur possédant une EC2 instance Amazon jointe à votre AWS Managed Microsoft AD.

Note

Avant de terminer cette procédure, vous devez installer les outils d'administration Active Directory. Pour plus d'informations, voir [Installer les outils d'administration Active Directory](#).

Pour supprimer un utilisateur

1. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration de Windows.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```


2. Dans l'arborescence du répertoire, sélectionnez l'unité d'organisation contenant l'utilisateur que vous souhaitez supprimer (par exemple, Corp\Users).
3. Sélectionnez l'utilisateur que vous souhaitez supprimer. Dans le menu Action, sélectionnez Supprimer.
4. Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'utilisateur. Choisissez Oui pour supprimer l'utilisateur.

Les utilisateurs supprimés sont stockés temporairement dans la corbeille AD. Pour plus d'informations sur la corbeille AD, veuillez consulter [The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting](#) (français non garanti) sur le blog Ask the Directory Services Team de Microsoft.

Réinitialisation d'un AWS mot de passe utilisateur Microsoft AD géré

Les utilisateurs doivent respecter les politiques de mot de passe définies dans Active Directory. Parfois, cela peut prendre le dessus sur les utilisateurs, y compris l'administrateur Active Directory, et ils oublient leur mot de passe. Dans ce cas, vous pouvez rapidement réinitialiser le mot de passe de l'utilisateur en Directory Service indiquant s'il réside dans AWS Managed Microsoft AD.

Vous devez être connecté en tant qu'utilisateur avec les autorisations nécessaires pour réinitialiser les mots de passe. Pour plus d'informations sur les autorisations, consultez [Vue d'ensemble de la gestion des autorisations d'accès à vos Directory Service ressources](#).

Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de votre Active Directory, sauf dans les cas suivants :

- Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de l'unité organisationnelle (UO) en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre Active Directory. Par exemple, si vous avez suivi la procédure indiquée dans [Création de votre AWS compte Microsoft AD géré](#) votre NetBIOS, le nom serait CORP et les mots de passe des utilisateurs que vous pourriez réinitialiser seraient membres de l' Corp/Users UO.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur en dehors de l'unité d'organisation en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre Active Directory. Par exemple, vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur dans l'unité d'organisation AWS réservée. Pour plus d'informations sur la structure de l'unité organisationnelle de AWS Managed Microsoft AD, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).

Pour plus d'informations sur la façon dont les politiques de mot de passe sont appliquées lorsqu'un mot de passe est réinitialisé dans AWS Managed Microsoft AD, consultez [Comment les politiques relatives aux mots de passe sont appliquées](#).

Vous pouvez utiliser l'un des outils suivants pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré :

- AWS Management Console
- AWS CLI
- PowerShell

AWS Management Console

Utilisez la procédure suivante pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré avec le AWS Management Console.

1. Dans le volet de navigation de la [Directory Service console](#), sous Active Directory, choisissez Directories, puis sélectionnez Active Directory dans la liste où vous souhaitez réinitialiser un mot de passe utilisateur.
2. Sur la page des détails de l'annuaire, choisissez Actions, puis Réinitialiser le mot de passe utilisateur.
3. Dans la boîte de dialogue Réinitialiser le mot de passe utilisateur, dans Nom d'utilisateur, tapez le nom d'utilisateur de l'utilisateur dont le mot de passe doit être modifié.
4. Entrez un mot de passe dans Nouveau mot de passe et Confirmer le mot de passe, puis choisissez Réinitialiser le mot de passe.

AWS CLI

Utilisez la procédure suivante pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré avec le AWS CLI.

1. Pour installer le AWS CLI, voir [Installer ou mettre à jour la dernière version du AWS CLI](#).
2. Ouvrez le AWS CLI.
3. Tapez la commande suivante et remplacez l'ID de répertoire, le nom d'utilisateur **jane.doe** et le mot de passe **P@ssw0rd** par votre ID Active Directory et les informations d'identification souhaitées. Consultez [reset-user-password](#) la référence des AWS CLI commandes pour plus d'informations.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

PowerShell

Utilisez la procédure suivante pour réinitialiser le mot de passe d'un utilisateur Microsoft AD AWS géré avec le PowerShell.

1. Connectez-vous à l'instance jointe à votre domaine Active Directory en tant qu'administrateur Active Directory.
2. Ouvrir PowerShell.
3. Tapez la commande suivante en remplaçant le nom d'utilisateur **jane.doe**, l'ID de répertoire et le mot de passe **P@ssw0rd** par votre ID Active Directory et les informations d'identification souhaitées. Consultez l'[applet de commande Reset- DSUser Password](#) pour plus d'informations.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword "P@ssw0rd"
```

Création d'un groupe Microsoft AD AWS géré

Vous pouvez créer des groupes dans votre AWS Managed Microsoft AD. Utilisez la procédure suivante pour créer un groupe de sécurité avec une EC2 instance Amazon jointe à votre répertoire AWS Managed Microsoft AD. Avant de créer des groupes de sécurité, vous devez suivre les procédures décrites dans la section [Installation des outils d'administration Active Directory](#).

Active Directory Administration Tools

Utilisez les procédures suivantes pour créer un groupe Microsoft AD AWS géré à l'aide des outils d'administration Active Directory.

Pour créer un groupe

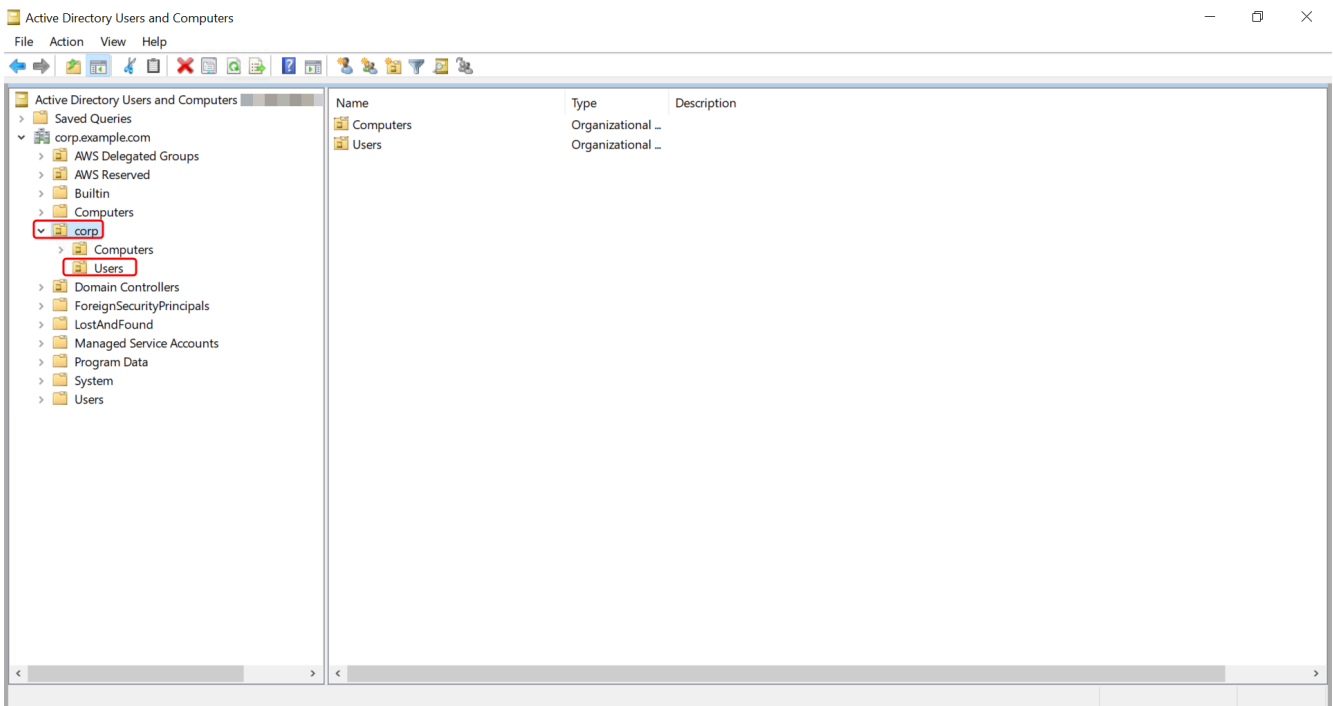
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous souhaitez stocker votre groupe (par exemple, Corp\Users). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré.](#)



4. Dans le menu Action, cliquez sur Nouveau, puis sur Groupe pour ouvrir l'assistant de création de nouveaux groupes.
5. Tapez le nom du groupe dans Nom du groupe, sélectionnez une étendue de groupe qui répond à vos besoins, puis sélectionnez Sécurité pour le type de groupe. Pour plus d'informations sur l'étendue des groupes Active Directory et les groupes de sécurité, veuillez consulter la section [Groupes de sécurité Active Directory](#) dans la documentation de Microsoft Windows Server.
6. Cliquez sur OK. Le nouveau groupe de sécurité apparaîtra dans le dossier Utilisateurs.

PowerShell

Vous pouvez utiliser des PowerShell commandes pour créer des groupes. Pour plus d'informations, consultez la section [Nouveautés ADGroup](#) dans la PowerShell documentation de Windows Server 2022.

Ajouter un utilisateur Microsoft AD AWS géré à un groupe

Vous pouvez ajouter des utilisateurs Microsoft AD AWS gérés à un groupe. Utilisez la procédure suivante pour ajouter un utilisateur à un groupe de sécurité avec une EC2 instance Amazon jointe à votre répertoire AWS Managed Microsoft AD.

Active Directory Administration Tools

Pour ajouter un utilisateur à un groupe

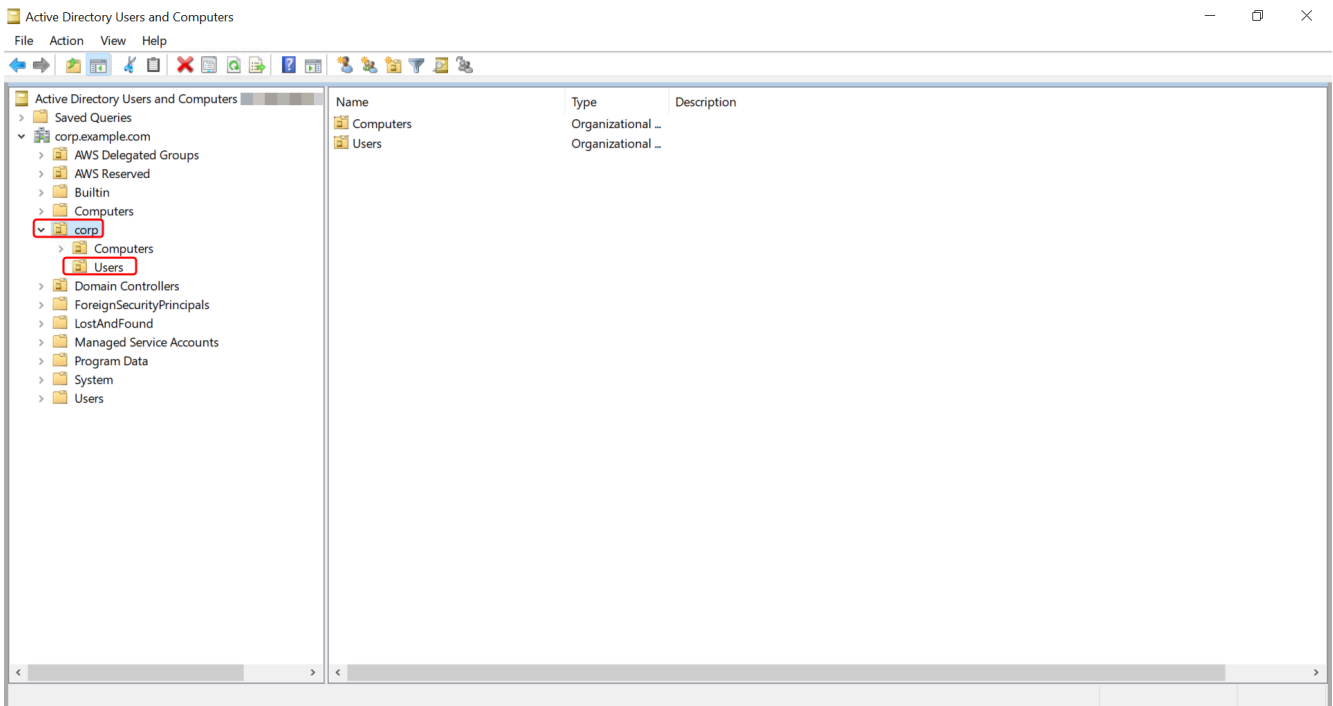
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence de l'annuaire, sélectionnez l'unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous avez enregistré votre groupe, puis sélectionnez le groupe auquel vous souhaitez ajouter un utilisateur en tant que membre.



4. Dans le menu Action, cliquez sur Propriétés pour ouvrir la boîte de dialogue des propriétés du groupe.
5. Sélectionnez l'onglet Membres, puis cliquez sur Ajouter.
6. Pour Entrez les noms des objets à sélectionner, tapez le nom d'utilisateur que vous souhaitez ajouter et cliquez sur OK. Le nom sera affiché dans la liste Membres. Cliquez à nouveau sur OK pour mettre à jour les membres du groupe.
7. Vérifiez que l'utilisateur est désormais membre du groupe en le sélectionnant dans le dossier Utilisateurs et en cliquant sur Propriétés dans le menu Action pour ouvrir la boîte de dialogue des propriétés. Sélectionnez l'onglet Membre de. Le nom du groupe doit apparaître dans la liste des groupes auxquels appartient l'utilisateur.

AWS Données du service de répertoire

AWS Directory Service Data est une extension de AWS Directory Service. Vous pouvez créer, lire, mettre à jour des utilisateurs, des groupes et des adhésions Active Directory (AD) à partir d'un service d' AWS annuaire pour Microsoft Active Directory sans déployer d'instances de gestion AD dédiées sur une EC2 instance Amazon. Vous pouvez également effectuer des tâches de gestion d'objets intégrées dans des annuaires sans aucune connectivité réseau directe. Cela simplifie le provisionnement et la gestion des accès pour réaliser des déploiements entièrement automatisés. Pour plus d'informations, consultez le manuel [AWS Directory Service Data API Reference](#).

Directory Service Data prend en charge les opérations d'écriture des utilisateurs `CreateUser` et des groupes `CreateGroup`, comme et au sein du AWS Managed Microsoft AD intégré à votre unité organisationnelle (UO). Directory Service Data prend en charge les opérations de lecture, de type `ListUsers` et `ListGroups`, sur tous les utilisateurs, groupes et appartenances à des groupes au sein de AWS Managed Microsoft AD et dans les domaines approuvés. Directory Service Data prend en charge l'ajout et la suppression de membres de groupes dans les groupes de votre unité d'organisation et de l' AWS unité d'organisation Delegated Groups. Vous pouvez ainsi déléguer des autorisations en ajoutant des utilisateurs à des objets de groupe délégués spécifiques. Pour de plus amples informations, veuillez consulter [Gestion des utilisateurs et des groupes dans AWS Managed Microsoft AD](#).

 Note

Les données du service de répertoire ne sont disponibles que dans votre région principale. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

Rubriques

- [Réplication et cohérence](#)
- [AWS Attributs des données du service de répertoire](#)
- [Type de groupe et étendue du groupe](#)

Réplication et cohérence

L'API Directory Service Data se connecte à vos contrôleurs de domaine Microsoft AD AWS gérés pour effectuer des opérations sur les objets d'annuaire sous-jacents. Active Directory est une plateforme finalement cohérente, et la réplication se produit en permanence entre les contrôleurs de domaine d' Directory Service annuaire. Par défaut, chaque Directory Service répertoire est créé avec deux contrôleurs de domaine.

Directory Service Data tente de maintenir une expérience cohérente en utilisant le même contrôleur de domaine pour toutes les demandes. Si un contrôleur de domaine n'est pas disponible, Directory Service Data bascule vers un autre contrôleur de domaine. Au cours de ces événements, vous remarquerez peut-être une certaine cohérence entre les contrôleurs de domaine lorsque les objets sont répliqués entre les contrôleurs de domaine.

Les limites du répertoire varient selon l'édition de AWS Managed Microsoft AD :

- Édition standard — Supporte 8 transactions par seconde pour les opérations de lecture et 4 TPS pour les opérations d'écriture par répertoire.
- Édition Enterprise : prend en charge 16 transactions par seconde pour les opérations de lecture et 8 TPS pour les opérations d'écriture par répertoire.

 Note

Il existe une limite de 10 demandes simultanées pour les éditions Standard et Enterprise.

- Compte AWS— Prend en charge un total de 100 transactions par seconde pour les opérations de Directory Service Data dans tous les annuaires.

AWS Attributs des données du service de répertoire

Cette rubrique décrit comment utiliser les attributs dans le [AWS Directory Service Data API Reference](#).

Attributs de demande

Les attributs suivants doivent être définis dans les paramètres du corps de la demande. Pour un exemple de définition de ces attributs, consultez le [CreateGroup](#) manuel AWS Directory Service Data API Reference.

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
DistinguishedName	distinguishedName	Nom unique	Aucune	ReadOnly	Utilisateur, Groupe	Chaîne	Non

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
EmailAddress	courrier	Adresse e-mail	EmailAddress	Créable	Utilisateur	Chaîne	Oui
Enabled	Aucune	Activées	Activées	Mutable	Utilisateur	Booléen	Non
GivenName	givenName	Prénom	GivenName	Créable	Utilisateur	Chaîne	Oui
GroupScope	Portée du groupe	Étendue du groupe	Aucune	Créable	Groupe	Enum	Non
GroupType	Type de groupe	Type de groupe	Aucune	Créable	Groupe	Enum	Non
SamAccountName	sAMAccountName	Nom de connexion de l'utilisateur	sAMAccountName	Créable	Utilisateur, Groupe	Chaîne	Oui
SID	ID de l'objet	Identifiant de sécurité (SID) de l'utilisateur/du groupe	SID	ReadOnly	Utilisateur, Groupe	Chaîne	Non
Nom	sn	Nom	Surname	Créable	Utilisateur	Chaîne	Oui

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
UserPrincipalName	userPrincipalName	Nom principal de l'utilisateur	UserPrincipalName	ReadOnly	Utilisateur	Chaîne	Non

Autres attributs

Les attributs suivants doivent être définis dans les paramètres du corps de la demande `OtherAttributes` et ne doivent pas être mappés à ceux-ci. Lorsque vous définissez d'autres attributs dans vos demandes, vous devez spécifier le nom de l'attribut, le type de données et la valeur de chaque attribut. Pour un exemple de définition de ces attributs, consultez le [CreateUser](#) manuel AWS Directory Service Data API Reference.

Note

Les noms de ces attributs ne distinguent pas les majuscules et minuscules lorsqu'ils sont fournis en entrée et sont l'équivalent du nom d'affichage LDAP.

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
Assistant	assistant	Assistant	Aucune	ReadOnly	Utilisateur	Chaîne	Non

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
Cn	cn	Nom commun	Aucune	ReadOnly	Utilisateur, Groupe	Chaîne	Non
Co	co	Pays/région	Pays	Mutable	Utilisateur	Chaîne	Non
L'entreprise	company	Société	Société	Créable	Utilisateur	Chaîne	Non
Département	department	Département	Département	Créable	Utilisateur	Chaîne	Non
Description	description	Description	Description	Créable	Utilisateur, Groupe	Chaîne	Non
DirectReports	Rapports directs	Rapports directs	Aucune	ReadOnly	Utilisateur	Set de cordes	Non
DisplayName	displayName	Nom d'affichage	DisplayName	Créable	Utilisateur, Groupe	Chaîne	Oui
Facsimile Telephone Number	facsimile Telephone Number	Fax	Fax	Créable	Utilisateur, Groupe	Chaîne	Non
HomePhone	Téléphone domestique	Numéro de téléphone personnel	HomePhone	Créable	Utilisateur	Chaîne	Non

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
Info (Infos)	info	Remarques	Aucune	Mutable	Utilisateur, Groupe	Chaîne	Non
Initiales	initiales	Initials	Initials	Mutable	Utilisateur	Chaîne	Non
IpPhone	téléphone IP	Téléphone IP	Aucune	Mutable	Utilisateur	Chaîne	Non
L	I	Ville	Ville	Créable	Utilisateur	Chaîne	Oui
Gérant	manager	Responsable	Responsable	Mutable	Utilisateur	Chaîne	Non
Courrier	courrier	Adresse e-mail	EmailAddress	Mutable	Groupe	Chaîne	Oui
Applications mobiles	mobile	Numéro de téléphone portable	MobilePhone	Mutable	Utilisateur	Chaîne	Non
ObjectClass	Classe d'objet	Utilisateur/groupe	Aucune	ReadOnly	Groupe	Chaîne	Non
Guide de l'objet	Guide de l'objet	Identifiant unique global (GUID)	Aucune	ReadOnly	Utilisateur, Groupe	Chaîne	Non

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
Téléavertisseur	téléavertisseur	Téléavertisseur	Aucune	Mutable	Utilisateur	Chaîne	Non
PhysicalDeliveryOfficeName	physicalDeliveryOfficeNom	Bureau	Aucune	Créable	Utilisateur	Chaîne	Oui
PostalCode	Code postal	Code postal/Zip	PostalCode	Créable	Utilisateur	Chaîne	Non
PreferredLanguage	Langue préférée	Langue préférée	Aucune	Mutable	Utilisateur	Chaîne	Non
ProxyAddresses	Adresses proxy	Adresse du proxy	Aucune	ReadOnly	Utilisateur, Groupe	Chaîne à valeurs multiples	Oui
ServicePrincipalName	servicePrincipalName	Nom principal du service	ServicePrincipalName	Mutable	Utilisateur	Chaîne à valeurs multiples	Non
St.	saint	État/province	État	Créable	Utilisateur	Chaîne	Non
StreetAddress	Adresse de rue	Adresse de rue	StreetAddress	Créable	Utilisateur	Chaîne	Non
TelephoneNumber	Numéro de téléphone	Numéro de téléphone	OfficePhone	Créable	Utilisateur	Chaîne	Non

Nom de l'attribut Directory Service Data	Nom d'affichage LDAP	AWS Management Console	PowerShell alias	Type d'accès	Type d'objet	Valeur d'attribut	Peut faire l'objet d'une recherche
Titre	title	Titre de la tâche	Title	Mutable	Utilisateur	Chaîne	Non
WhenChanged	En cas de modification	Dernière mise à jour	Aucune	ReadOnly	Utilisateur, Groupe	Chaîne	Non
WWWHomePage	à WWHome Page	URL de la page d'accueil	à WWHome Page	Mutable	Utilisateur, Groupe	Chaîne	Non

Type de groupe et étendue du groupe

Dans AWS Managed Microsoft AD, les groupes possèdent à la fois un type de groupe et une étendue de groupe. Consultez les sections suivantes pour plus d'informations sur chacune d'elles.

Rubriques

- [Type de groupe](#)
- [Étendue du groupe](#)

Type de groupe

Le type de groupe détermine les ressources partagées au sein d'Active Directory auxquelles les membres du groupe peuvent accéder. Il existe deux types de groupes :

- **Sécurité** : vous pouvez attribuer des autorisations à ces groupes afin que les membres du groupe puissent accéder aux ressources Active Directory partagées.
- **Distribution** : vous pouvez utiliser ce type pour créer des listes de distribution par e-mail. Ces membres du groupe ne peuvent pas accéder aux ressources partagées Active Directory.

Il n'y a aucune limite lors du passage d'un type de groupe à un autre.

Pour plus d'informations sur les types de groupes, consultez [la documentation Microsoft](#).

Étendue du groupe

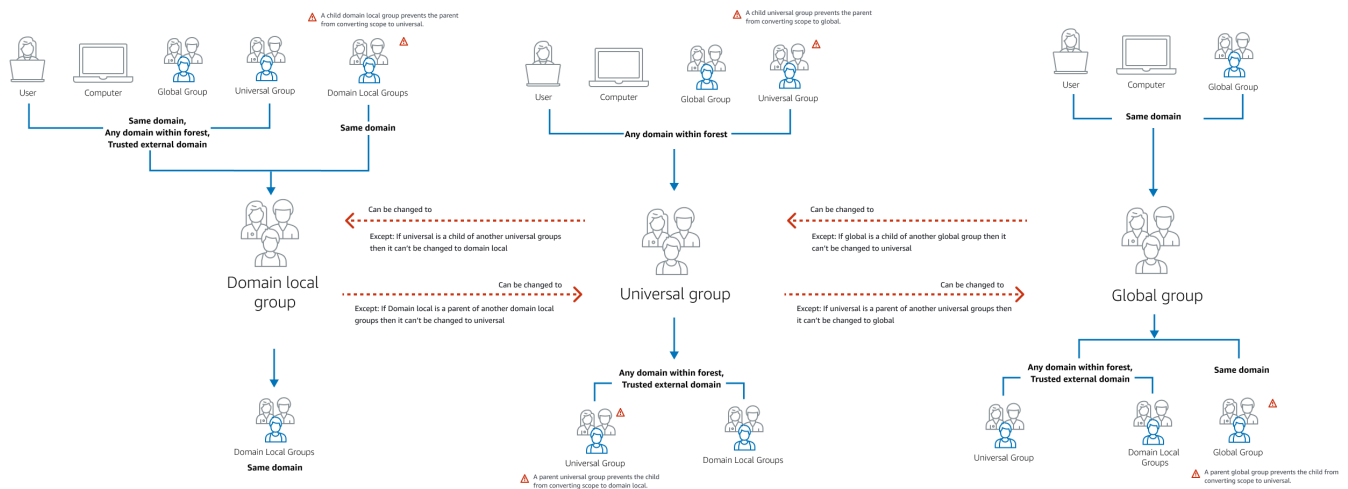
L'étendue du groupe détermine la façon dont les membres du groupe sont définis par rapport à l'arborescence ou à la forêt du domaine. Il existe trois champs d'application de groupe :

- **Domaine local** : pour attribuer des autorisations aux membres du groupe situés dans le même domaine.
- **Universel** : pour attribuer des autorisations aux membres du groupe situés dans n'importe quel domaine.
- **Global** : pour attribuer des autorisations aux membres du groupe situés dans n'importe quel domaine ou forêt.

Il existe des limites lors de la modification de l'étendue d'un groupe. La liste et le schéma suivants décrivent ces limites.

- Modification de l'étendue du groupe de domaine local à universel - Oui
 - À moins que le groupe local de domaines ne soit le parent d'un autre groupe local de domaines.
- Modification de l'étendue du groupe de Universal à Domain Local - Oui
 - À moins que le groupe universel ne soit un groupe enfant d'un autre groupe universel.
- Modification de la portée du groupe de Universal à Global - Oui
 - À moins que le groupe universel ne soit le parent d'un autre groupe universel.
- Modification de l'étendue du groupe de Global à Universal - Oui
 - À moins que le groupe mondial ne soit un enfant d'un autre groupe mondial.

Pour plus d'informations sur les étendues de groupe, consultez [Microsoft la documentation](#).



Connecter votre Microsoft AD AWS géré à Microsoft Entra Connect Sync

Ce didacticiel vous explique les étapes nécessaires à l'installation [Microsoft Entra Connect Sync](#) pour vous synchroniser avec votre [Microsoft Entra ID](#) AWS Managed Microsoft AD.

Dans ce didacticiel, vous allez effectuer les opérations suivantes :

1. Créez un utilisateur de domaine Microsoft AD AWS géré.
2. Téléchargement Entra Connect Sync.
3. PowerShell à utiliser pour exécuter un script afin de fournir les autorisations appropriées à l'utilisateur nouvellement créé.
4. Installer Entra Connect Sync.

Prérequis

Vous aurez besoin des éléments suivants pour suivre ce didacticiel :

- Un Microsoft AD AWS géré. Pour de plus amples informations, veuillez consulter [the section called "Création de votre AWS compte Microsoft AD géré"](#).
- Une instance Amazon EC2 Windows Server jointe à votre AWS Managed Microsoft AD. Pour de plus amples informations, veuillez consulter [Rejoindre une instance Windows](#).

- Un EC2 Windows serveur Administration Tools sur lequel Active Directory est installé pour gérer votre Microsoft AD AWS géré. Pour de plus amples informations, veuillez consulter [the section called “Installation des outils d'administration AD”](#).

Création d'un utilisateur de domaine Active Directory

Ce didacticiel part du principe que vous disposez déjà d'une instance Microsoft AD AWS gérée ainsi que d'une instance de EC2 Windows serveur sur laquelle Active Directory Administration Tools est installé. Pour de plus amples informations, veuillez consulter [the section called “Installation des outils d'administration AD”](#).

1. Connectez-vous à l'instance sur laquelle Active Directory a Administration Tools été installé.
2. Créez un utilisateur de domaine Microsoft AD AWS géré. Cet utilisateur deviendra le Active Directory Directory Service (AD DS) Connector account pour Entra Connect Sync. Pour connaître les étapes détaillées de ce processus, voir [the section called “Création d'un utilisateur”](#).

Télécharger Entra Connect Sync

- Téléchargez Entra Connect Sync depuis le [Microsoftsite Web](#) sur l' EC2 instance qui est l'administrateur Microsoft AD AWS géré.

Warning

Ne l'ouvrez pas ou ne Entra Connect Sync l'exécutez pas à ce stade. Les prochaines étapes fourniront les autorisations nécessaires à l'utilisateur de votre domaine créé à l'étape 1.

Exécuter PowerShell le script

- [Ouvrez PowerShell en tant qu'administrateur](#) et exécutez le script suivant.

Pendant l'exécution du script, il vous sera demandé de saisir le [AMAccountnom s du](#) nouvel utilisateur de domaine créé à l'étape 1.

Note

Consultez ce qui suit pour plus d'informations sur l'exécution du script :

- Vous pouvez enregistrer le script avec l'ps1extension dans un dossier tel que **temp**. Vous pouvez ensuite utiliser la PowerShell commande suivante pour charger le script :

```
import-module "c:\temp\entra.ps1"
```

- Après avoir chargé le script, vous pouvez utiliser la commande suivante pour définir les autorisations nécessaires pour exécuter le script, en *Entra_Service_Account_Name* remplaçant par le nom de votre compte de Entra service :

```
Set-EntraConnectSvcPerms -ServiceAccountName Entra_Service_Account_Name
```

```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig\AdSyncConfig.psm1"
```

```
try {  
    # Attempt to import the module  
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."  
    Import-Module $modulePath -ErrorAction Stop  
    Write-Host -ForegroundColor Green "Success!"  
}  
catch {  
    # Display the exception message  
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"  
}
```

```
Function Set-EntraConnectSvcPerms {  
    [CmdletBinding()]  
    Param (  
        [String]$ServiceAccountName  
    )  
  
    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator  
  
    Try {  
        $Domain = Get-ADDomain -ErrorAction Stop  
    } Catch [System.Exception] {  
        Write-Output "Failed to get AD domain information $_"  
    }  
}
```

```

$BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
$Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

Try {
    $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
}

Try {
    $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
Stop | Select-Object -ExpandProperty 'DistinguishedName'
} Catch [System.Exception] {
    Write-Output "Failed to get service account DN $_"
}

Foreach ($OU in $OUs) {
    try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
$ADConnectorAccountDN -ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

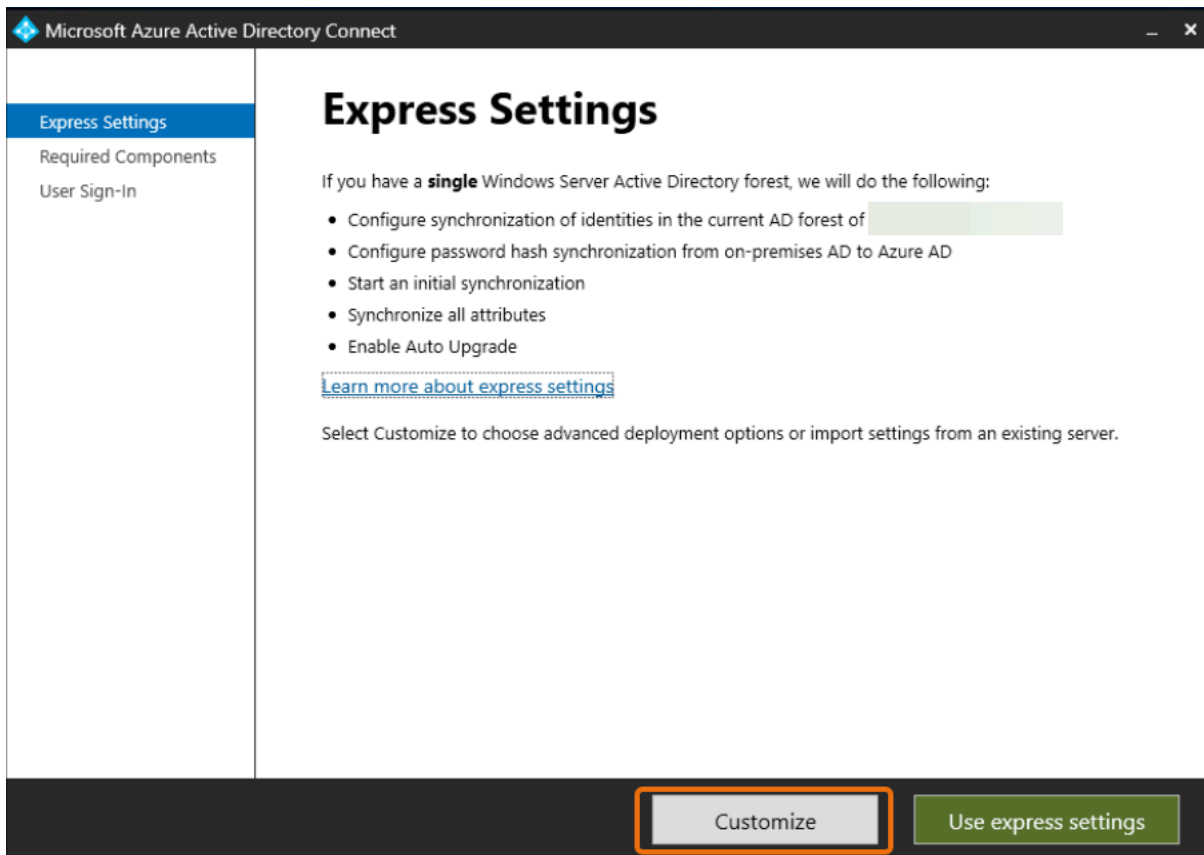
        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
$ADConnectorAccountDN on OU $OU : $_"
    }
}
}

```

Installer Entra Connect Sync

1. Une fois le script terminé, vous pouvez exécuter le fichier de configuration téléchargé Microsoft Entra Connect (anciennement connu sous le nom de fichier Azure Active Directory Connect).

2. Une Microsoft Azure Active Directory Connect fenêtre s'ouvre après l'exécution du fichier de configuration de l'étape précédente. Dans la fenêtre Express Settings, sélectionnez Personnaliser.



3. Dans la fenêtre Installer les composants requis, cochez la case Utiliser un compte de service existant. Dans NOM DU COMPTE DE SERVICE et MOT DE PASSE DU COMPTE DE SERVICE, entrez le AD DS Connector account nom et le mot de passe de l'utilisateur que vous avez créé à l'étape 1. Par exemple, si votre AD DS Connector account nom est entra, le nom du compte sera corp\entra. Sélectionnez ensuite Installer.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ?

☐ Specify a custom installation location

☐ Use an existing SQL Server

☒ Use an existing service account

☐ Managed Service Account

☒ Domain Account

SERVICE ACCOUNT NAME

corp\entra

SERVICE ACCOUNT PASSWORD

.....

☐ Specify custom sync groups

☐ Import synchronization settings ?

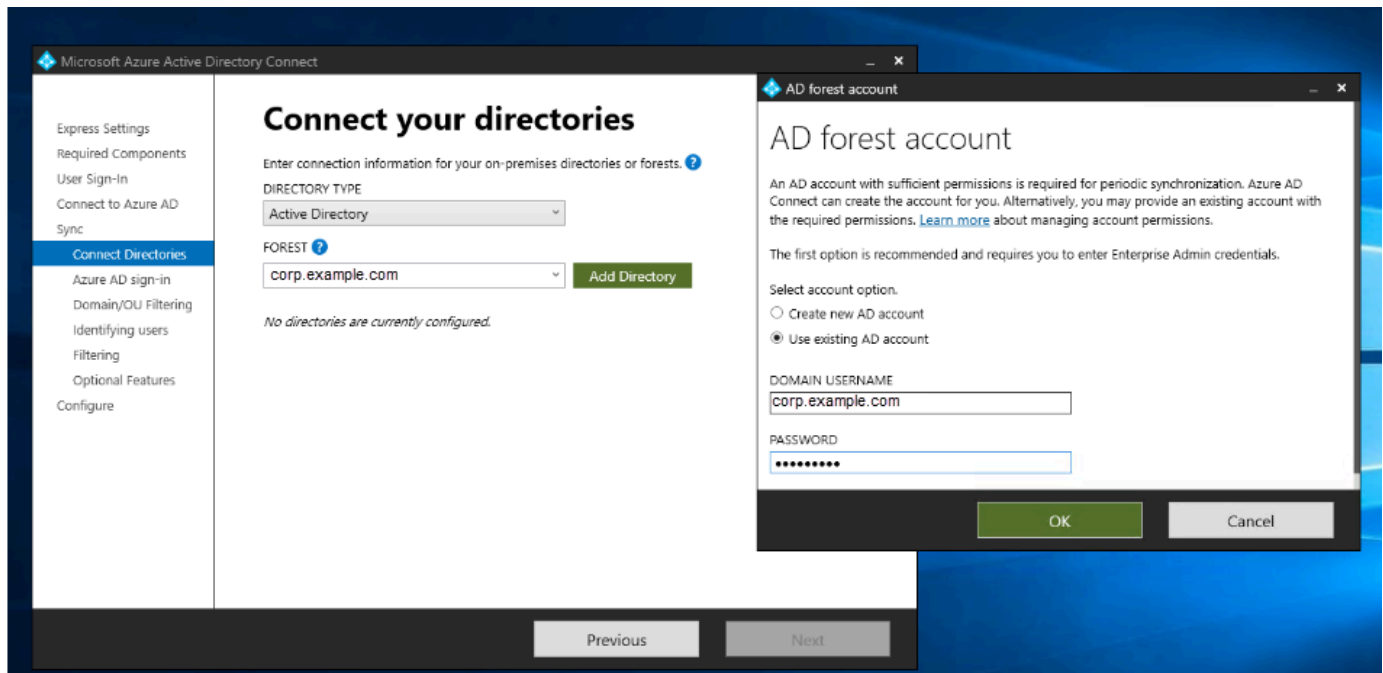
Previous Install

4. Dans la fenêtre de connexion de l'utilisateur, sélectionnez l'une des options suivantes :
 - a. [Authentification directe : cette option vous permet de vous connecter à votre Active Directory à l'aide de votre nom d'utilisateur et de votre mot de passe.](#)
 - b. Ne pas configurer : cela vous permet d'utiliser la connexion fédérée avec Microsoft Entra (anciennement connue sous le nom de Azure Active Directory (AzureAD)) ou Office 365.

Sélectionnez ensuite Next.

5. Dans la Azure fenêtre Connect to, entrez votre nom d'utilisateur et votre mot de passe d'[administrateur global](#), Entra ID puis sélectionnez Next.
6. Dans la fenêtre Connect your directories, choisissez Active Directory pour DIRECTORY TYPE. Choisissez la forêt pour votre AWS Managed Microsoft AD for FOREST. Sélectionnez ensuite Ajouter un répertoire.

- Une fenêtre contextuelle s'affiche pour vous demander les options de votre compte. Sélectionnez Utiliser un compte AD existant. Entrez le AD DS Connector account nom d'utilisateur et le mot de passe créés à l'étape 1, puis sélectionnez OK. Sélectionnez ensuite Next.



- Dans la fenêtre de Azure ADconnexion, sélectionnez Continuer sans associer tous les suffixes UPN aux domaines vérifiés, uniquement si aucun domaine personnalisé vérifié n'y a été ajouté. Entra ID Sélectionnez ensuite Next.
- Dans la fenêtre de filtrage des domaines/OU, sélectionnez les options qui répondent à vos besoins. Pour plus d'informations, voir [Entra Connect Sync: Configurer le filtrage](#) dans Microsoft la documentation. Sélectionnez ensuite Next.
- Dans la fenêtre Identification des utilisateurs, filtrage et fonctionnalités facultatives, conservez les valeurs par défaut et sélectionnez Suivant.
- Dans la fenêtre Configurer, passez en revue les paramètres de configuration et sélectionnez Configurer. L'installation de Entra Connect Sync sera finalisée et les utilisateurs commenceront à se synchroniser avecMicrosoft Entra ID.

AWS Tutoriels de laboratoire de test Microsoft AD gérés

Cette section propose une série de didacticiels guidés destinés à vous aider à créer un environnement de laboratoire de test dans AWS le quel vous pourrez expérimenter avec AWS Managed Microsoft AD.

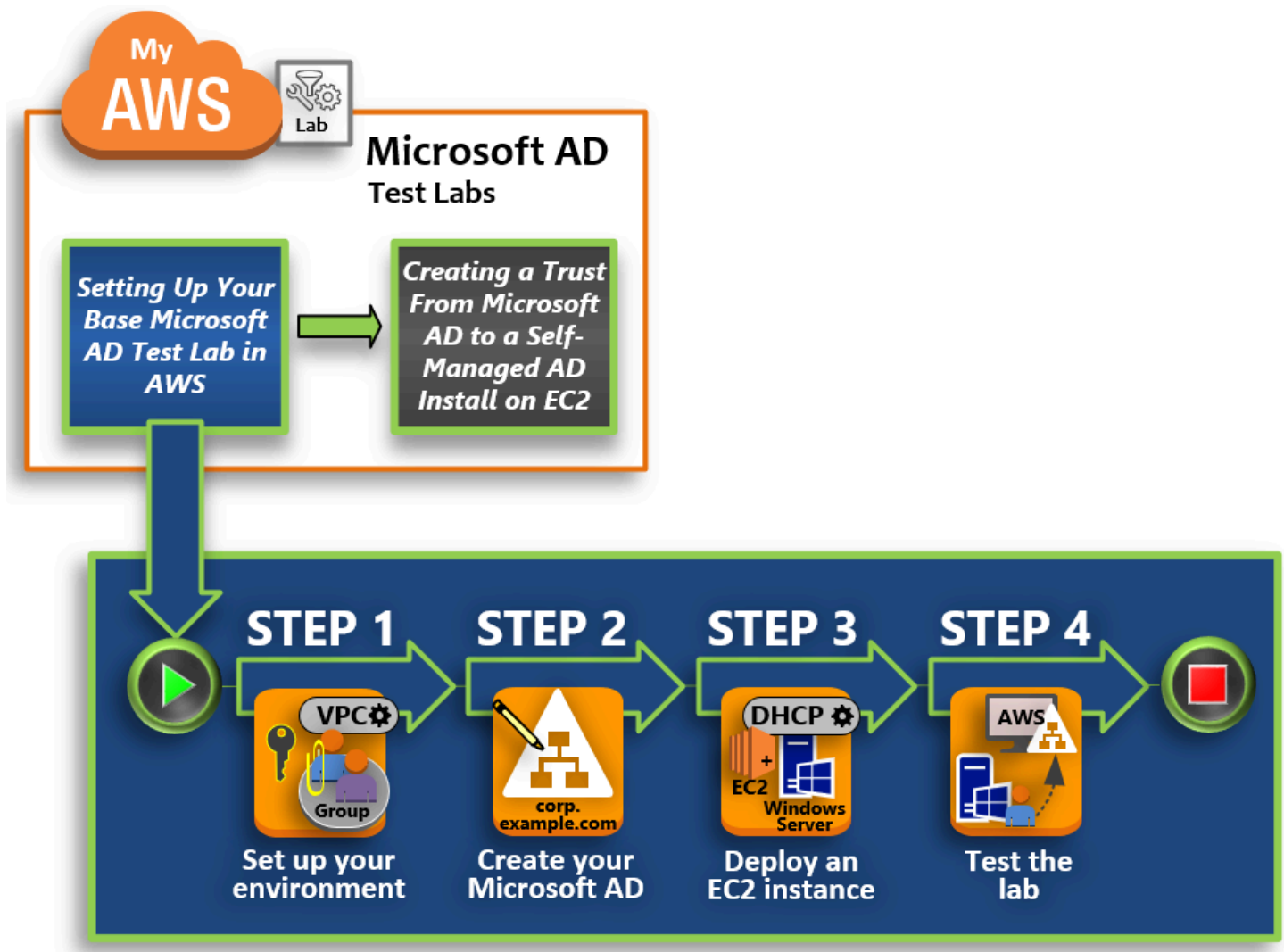
Rubriques

- [Tutoriel : Configuration de votre laboratoire de test Microsoft AD AWS géré de base dans AWS](#)
- [Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2](#)

Tutoriel : Configuration de votre laboratoire de test Microsoft AD AWS géré de base dans AWS

Ce didacticiel vous explique comment configurer votre AWS environnement pour préparer une nouvelle installation de AWS Managed Microsoft AD qui utilise une nouvelle EC2 instance Amazon exécutant Windows Server 2019. Il vous apprend ensuite à utiliser les outils d'administration Active Directory classiques pour gérer votre environnement Microsoft AD AWS géré à partir de votre instance EC2 Windows. À la fin du didacticiel, vous aurez défini les conditions requises pour le réseau et configuré une nouvelle forêt Microsoft AD AWS gérée.

Comme le montre l'illustration suivante, l'atelier que vous créez à partir de ce didacticiel est l'élément de base de l'apprentissage pratique de AWS Managed Microsoft AD. Vous pourrez ensuite ajouter des didacticiels facultatifs pour améliorer votre expérience pratique. Cette série de didacticiels est idéale pour toute personne qui débute avec AWS Managed Microsoft AD et qui souhaite bénéficier d'un environnement de test à des fins d'évaluation. Ce didacticiel vous prendra environ 1 heure.



Étape 1 : Configuration de votre AWS environnement pour AWS Managed Microsoft AD Active Directory

Une fois que vous avez terminé vos tâches prérequis, vous créez et configurez un Amazon VPC dans votre EC2 instance.

Étape 2 : Création de votre répertoire Microsoft AD Active Directory AWS géré

Au cours de cette étape, vous configurez AWS Managed Microsoft AD AWS pour la première fois.

Étape 3 : Déployer une EC2 instance Amazon pour gérer votre annuaire Microsoft AD Active Directory AWS géré

Ici, vous allez passer en revue les différentes tâches post-déploiement nécessaires pour que les ordinateurs clients puissent se connecter à votre nouveau domaine et y configurer un nouveau système Windows Server. EC2

Étape 4 : vérifier que l'atelier de test de base est opérationnel

Enfin, en tant qu'administrateur, vous vérifiez que vous pouvez vous connecter et vous connecter à AWS Managed Microsoft AD depuis votre système Windows Server EC2. Une fois que vous aurez confirmé que le laboratoire est opérationnel, vous pourrez continuer d'ajouter d'autres modules guides de votre atelier de test.

Prérequis

Si vous prévoyez de suivre uniquement les étapes de l'interface utilisateur décrites dans ce didacticiel pour créer votre atelier de test, vous pouvez ignorer cette section préalable et passer directement à l'étape 1. Toutefois, si vous prévoyez d'utiliser des AWS CLI commandes ou des AWS Tools for Windows PowerShell modules pour créer votre environnement de laboratoire de test, vous devez d'abord configurer les éléments suivants :

- Utilisateur IAM avec l'accès et la clé d'accès secrète — Un utilisateur IAM avec une clé d'accès est requis si vous souhaitez utiliser les modules AWS CLI or AWS Tools for Windows PowerShell . Si vous n'avez pas de clé d'accès, veuillez consulter la section [Creating, modifying, and viewing access keys \(AWS Management Console\)](#) (français non garanti).
- AWS Command Line Interface (facultatif) — Téléchargez et [installez AWS CLI le sous Windows](#). Une fois installé, ouvrez l'invite de commande ou PowerShell la fenêtre, puis tapez `aws configure`. Notez que vous avez besoin de la clé d'accès et de la clé secrète pour effectuer la configuration. Référez-vous au premier prérequis pour savoir comment procéder. Vous devrez renseigner les informations suivantes :
 - AWS ID de clé d'accès [Aucun] : AKIAIOSFODNN7EXAMPLE
 - AWS clé d'accès secrète [Aucune] : wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
 - Default Region name [None] : us-west-2
 - Default output format [None] : json
- AWS Tools for Windows PowerShell(facultatif) — Téléchargez et installez la dernière version AWS Tools for Windows PowerShell du formulaire <https://aws.amazon.com/powershell/>, puis exécutez la commande suivante. Notez que vous avez besoin de votre clé d'accès et de votre clé secrète pour effectuer la configuration. Référez-vous au premier prérequis pour savoir comment procéder.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey  
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Étape 1 : Configuration de votre AWS environnement pour AWS Managed Microsoft AD Active Directory

Avant de pouvoir créer AWS Managed Microsoft AD dans votre laboratoire de AWS test, vous devez d'abord configurer votre paire de EC2 clés Amazon afin que toutes les données de connexion soient cryptées.

Création d'une paire de clés

Si vous possédez déjà une paire de clés, vous pouvez ignorer cette étape. Pour plus d'informations sur les paires de EC2 clés Amazon, consultez la section [Créer des paires de clés](#).

Création d'une paire de clés

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Réseau et sécurité, choisissez Paires de clés, puis sélectionnez Créer une paire de clés.
3. Pour Key pair name (Nom de la paire de clés), saisissez **AWS-DS-KP**. Pour Key pair file format (Format de fichier de la paire de clés), sélectionnez pem, puis choisissez Create (Créer).
4. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Le nom de fichier est le nom que vous avez spécifié lorsque vous avez créé votre paire de clés, suivi de l'extension .pem. Enregistrez le fichier de clé privée en lieu sûr.

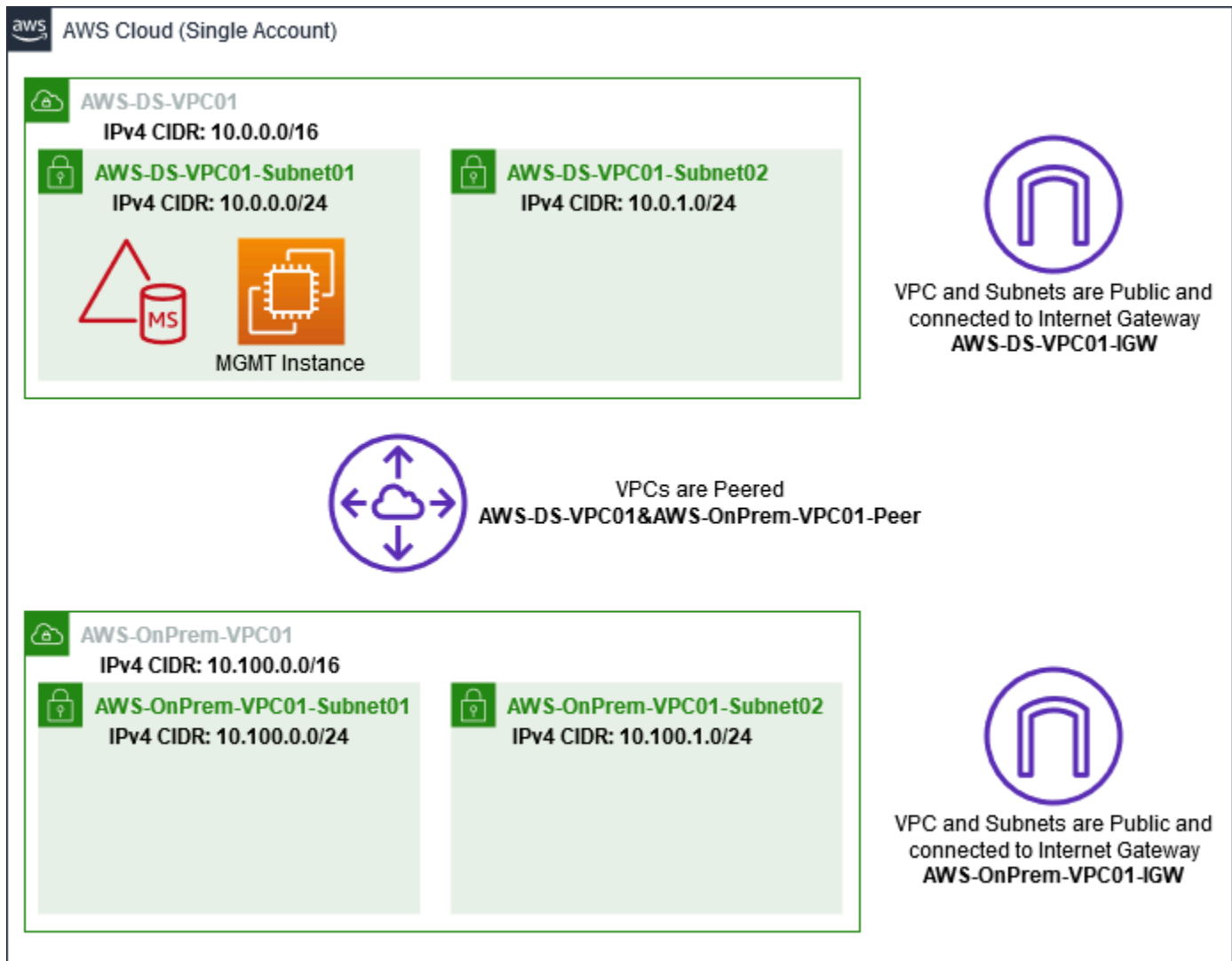
Important

C'est votre seule occasion d'enregistrer le fichier de clé privée. Vous devez indiquer le nom de votre paire de clés quand vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous déchiffrez le mot de passe de l'instance.

Créez, configurez et associez deux Amazon VPCs

Comme le montre l'illustration suivante, à la fin de ce processus en plusieurs étapes, vous aurez créé et configuré deux sous-réseaux publics VPCs, deux sous-réseaux publics par VPC, une passerelle Internet par VPC et une connexion VPC Peering entre les. VPCs Nous avons choisi d'utiliser des réseaux publics VPCs et des sous-réseaux pour des raisons de simplicité et de coût. Pour les charges de travail de production, nous vous recommandons d'utiliser le mode privé VPCs. Pour de

plus amples informations sur l'amélioration de la sécurité VPC, veuillez consulter [Security in Amazon Virtual Private Cloud](#) (français non garanti).



Tous les AWS CLI PowerShell exemples utilisent les informations VPC ci-dessous et sont intégrés dans us-west-2. Vous pouvez choisir n'importe quelle [région prise en charge](#) pour créer votre environnement. Pour de plus amples informations, veuillez consulter [What is Amazon VPC?](#) (français non garanti).

Étape 1 : Créez deux VPCs

Au cours de cette étape, vous devez en créer deux VPCs dans le même compte en utilisant les paramètres spécifiés dans le tableau suivant. AWS Managed Microsoft AD prend en charge l'utilisation de comptes distincts avec [Partagez votre Microsoft AD AWS géré](#) cette fonctionnalité. Le premier VPC sera utilisé pour Managed AWS Microsoft AD. Le deuxième VPC sera utilisé pour des

ressources qui pourront servir plus tard dans [Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2](#).

Informations sur les VPC Active Directory gérés	Informations sur le VPC sur site
Nom du tag : AWS-DS-VPC01	Balise de nom : AWS- OnPrem -VPC01
IPv4 Bloc CIDR : 10.0.0.0/16	IPv4 Bloc CIDR : 10.100.0.0/16
IPv6 Bloc CIDR : aucun bloc IPv6 CIDR	IPv6 Bloc CIDR : aucun bloc IPv6 CIDR
Location : Par défaut	Location : Par défaut

Pour obtenir des instructions détaillées, veuillez consulter [Creating a VPC](#) (français non garanti).

Étape 2 : Créer deux sous-réseaux par VPC

Après avoir créé le, VPCs vous devez créer deux sous-réseaux par VPC en utilisant les paramètres spécifiés dans le tableau suivant. Pour ce laboratoire de test, chaque sous-réseau sera de type /24. Cela permet d'émettre jusqu'à 256 adresses par sous-réseau. Chaque sous-réseau doit être un dans une zone de disponibilité distincte. Mettre chaque sous-réseau dans une zone de disponibilité distincte est un des [Conditions préalables à la création d'un Microsoft AWS AD géré](#).

Informations sur le sous-réseau AWS-DS-VP C01 :	AWS- Informations sur le OnPrem sous-réseau -VPC01
Balise de nom : AWS-DS-VPC01-subnet01	Balise de nom : AWS- OnPrem -vPC01-subnet01
VPC : vpc-xxxxxxxxxxxxxxxx-DS-VPC01 AWS	VPC : AWS vpc-xxxxxxxxxxxxxxxx - -VPC01 OnPrem
Zone de disponibilité : us-west-2a	Zone de disponibilité : us-west-2a
IPv4 Bloc CIDR : 10.0.0.0/24	IPv4 Bloc CIDR : 10.100.0.0/24
Balise de nom : AWS-DS-VPC01-subnet02	Tag de nom : AWS- OnPrem -vPC01-subnet02
VPC : vpc-xxxxxxxxxxxxxxxx-DS-VPC01 AWS	VPC : AWS vpc-xxxxxxxxxxxxxxxx - -VPC01 OnPrem

Informations sur le sous-réseau AWS-DS-VP C01 :	AWS- Informations sur le OnPrem sous-réseau -VPC01
Zone de disponibilité : us-west-2b	Zone de disponibilité : us-west-2b
IPv4 Bloc CIDR : 10.0.1.0/24	IPv4 Bloc CIDR : 10.100.1.0/24

Pour obtenir des instructions détaillées, veuillez consulter [Creating a subnet in your VPC](#) (français non garanti).

Étape 3 : Créez et connectez une passerelle Internet Gateway à votre VPCs

Comme nous utilisons le mode public, VPCs vous devrez créer et associer une passerelle Internet à votre compte VPCs en utilisant les paramètres spécifiés dans le tableau suivant. Cela vous permettra de vous connecter à vos EC2 instances et de les gérer.

Informations sur la passerelle Internet AWS-DS-VPC01	AWS- OnPrem -Informations sur la passerelle Internet Gateway VPC01
Nom du tag : AWS-DS-VPC01-IGW	Porte-nom : AWS- OnPrem -VPC01-IGW
VPC : vpc-xxxxxxxxxxxxxxxx-DS-VPC01 AWS	VPC : AWS vpc-xxxxxxxxxxxxxxxx - -VPC01 OnPrem

Pour obtenir des instructions détaillées, veuillez consulter [Internet gateways](#) (français non garanti).

Étape 4 : Configuration d'une connexion d'appairage VPC entre AWS-DS-VPC01 et -VPC01 AWS OnPrem

Comme vous en avez déjà créé deux VPCs auparavant, vous devrez les mettre en réseau à l'aide de l'appairage VPC en utilisant les paramètres spécifiés dans le tableau suivant. Bien qu'il existe de nombreuses façons de vous connecter VPCs, ce didacticiel utilisera le peering VPC. AWS [Managed Microsoft AD prend en charge de nombreuses solutions pour vous connecter VPCs, notamment le peering VPC, Transit Gateway et VPN.](#)

Étiquette nominative de connexion d'appairage : AWS-DS-VPC01& -AWS-VPC01-Peer OnPrem

VPC (demandeur) : vpc-xxxxxxxxxxxxxxxx -DS-VPC01 AWS

Compte : Mon compte

Région : Cette région

VPC (Accepter) : vpc-xxxxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Pour obtenir des instructions sur la création d'une connexion d'appairage de VPC avec un autre VPC depuis votre compte, veuillez consulter [Creating a VPC peering connection with another VPC in your account](#) (français non garanti).

Étape 5 : ajouter deux routes à la table de routage principale de chaque VPC

Pour que les passerelles Internet et la connexion d'appairage VPC créées au cours des étapes précédentes soient fonctionnelles, vous devez mettre à jour la table de routage principale des VPCs deux à l'aide des paramètres spécifiés dans le tableau suivant. Vous allez ajouter deux routes : 0.0.0.0/0, qui desservira toutes les destinations non explicitement connues de la table de routage et 10.0.0.0/16 ou 10.100.0.0/16, qui desservira chaque VPC via la connexion d'appairage de VPC établie ci-dessus.

Vous pouvez facilement trouver la bonne table de routage pour chaque VPC en filtrant sur le nom du VPC (AWS-DS-VPC01 ou - -VPC01). AWS OnPrem

Informations sur la route 1 AWS-DS-VP C01	Informations sur la route 2 AWS-DS-VP C01	AWS- Informations OnPrem sur la route 1 -VPC01	AWS- Informations OnPrem sur la route 2 -VPC01
Destination : 0.0.0.0/0	Destination : 10.100.0.0/16	Destination : 0.0.0.0/0	Destination : 10.0.0.0/16
Cible : igw-xxxxx xxxxxxxxxxxxx -DS- VPC01-IGW AWS	Cible : pcx-xxxxx xxxxxxxxxxxxxxxxxxx - DS-VPC01& - AWS- VPC01-peer AWS OnPrem	Cible : AWS igw- xxxxxxxxxxxxxxxxxxx - OnPrem-VPC01	Cible : pcx-xxxxx xxxxxxxxxxxxxxxxxxx - DS-VPC01& - AWS- VPC01-peer AWS OnPrem

Pour obtenir des instructions sur l'ajout de routes à une table de routage de VPC, veuillez consulter [Adding and removing routes from a route table](#) (français non garanti).

Création de groupes de sécurité pour les EC2 instances Amazon

Par défaut, AWS Managed Microsoft AD crée un groupe de sécurité pour gérer le trafic entre ses contrôleurs de domaine. Dans cette section, vous devrez créer 2 groupes de sécurité (un pour chaque VPC) qui seront utilisés pour gérer le trafic au sein de votre VPC pour vos EC2 instances à l'aide des paramètres spécifiés dans les tableaux suivants. Vous allez également ajouter une règle qui autorise le trafic entrant RDP (3389) entrant depuis n'importe où et pour tous les types de trafic entrant depuis le VPC local. Pour plus d'informations, consultez les [groupes EC2 de sécurité Amazon pour les instances Windows](#).

Informations sur le groupe de sécurité AWS-DS-VPC01 :

Nom du groupe de sécurité : AWS DS Test Lab Security Group

Description : Groupe de sécurité AWS DS Test Lab

VPC : vpc-xxxxxxxxxxxxxxxx-DS-VPC01 AWS

Règles entrantes du groupe de sécurité pour AWS-DS-VPC01

Type	Protocole	Plage de ports	Source	Type de trafic
Destination	TCP	3389	Mon IP	Bureau à distance
Tout le trafic	Tous	Tous	10.0.0.0/16	Tout le trafic du VPC local

Règles de sortie du groupe de sécurité pour AWS-DS-VPC01

Type	Protocole	Plage de ports	Destination	Type de trafic
Tout le trafic	Tous	Tous	0.0.0.0/0	Tout le trafic

AWS- Informations OnPrem sur le groupe de sécurité -VPC01 :

Nom du groupe de sécurité : AWS OnPrem Test Lab Security Group.

Description : Groupe de sécurité du laboratoire de AWS OnPrem test.

VPC : AWS vpc-xxxxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Règles entrantes du groupe de sécurité pour AWS- -VPC01 OnPrem

Type	Protocole	Plage de ports	Source	Type de trafic
Destination	TCP	3389	Mon IP	Bureau à distance
Destination	TCP	53	10.0.0.0/16	DNS
Destination	TCP	88	10.0.0.0/16	Kerberos
Destination	TCP	389	10.0.0.0/16	LDAP
Destination	TCP	464	10.0.0.0/16	Mot de passe Kerberos (modification/définition)
Destination	TCP	445	10.0.0.0/16	SMB / CIFS
Destination	TCP	135	10.0.0.0/16	Réplication
Destination	TCP	636	10.0.0.0/16	LDAP SSL
Destination	TCP	49152 - 65535	10.0.0.0/16	RPC
Destination	TCP	3268 - 3269	10.0.0.0/16	LDAP GC & LDAP GC SSL
Règle UDP personnalisée	UDP	53	10.0.0.0/16	DNS

Type	Protocole	Plage de ports	Source	Type de trafic
Règle UDP personnalisée	UDP	88	10.0.0.0/16	Kerberos
Règle UDP personnalisée	UDP	123	10.0.0.0/16	Heure Windows
Règle UDP personnalisée	UDP	389	10.0.0.0/16	LDAP
Règle UDP personnalisée	UDP	464	10.0.0.0/16	Mot de passe Kerberos (modification/définition)
Tout le trafic	Tous	Tous	10.100.0.0/16	Tout le trafic du VPC local

Règles de sortie du groupe de sécurité pour AWS- -VPC01 OnPrem

Type	Protocole	Plage de ports	Destination	Type de trafic
Tout le trafic	Tous	Tous	0.0.0.0/0	Tout le trafic

Pour obtenir des instructions détaillées sur la création et l'ajout de règles à vos groupes de sécurité, veuillez consulter [Working with security groups](#) (français non garanti).

Étape 2 : Création de votre répertoire Microsoft AD Active Directory AWS géré

Vous pouvez créer votre annuaire selon trois méthodes différentes. Vous pouvez utiliser la AWS Management Console procédure (recommandée pour ce didacticiel) ou vous pouvez utiliser les AWS Tools for Windows PowerShell procédures AWS CLI ou pour créer votre répertoire.

Méthode 1 : pour créer votre répertoire Microsoft AD AWS géré (AWS Management Console)

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire, puis Configurer un annuaire.

2. Sur la page Sélectionner un type d'annuaire, choisissez AWS Managed Microsoft AD, puis Suivant.
3. Sur la page Enter directory information (Saisir les détails de l'annuaire), indiquez les informations suivantes, puis choisissez Next (Suivant).
 - Pour Edition (Édition), choisissez Standard Edition (Édition standard) ou Enterprise Edition (Édition d'entreprise). Pour plus d'informations sur les éditions, veuillez consulter [AWS Directory Service for Microsoft Active Directory Service](#) (français non garanti).
 - Pour Directory DNS name (Nom DNS de l'annuaire), tapez **corp.example.com**.
 - Pour Directory NetBIOS name (Nom NetBIOS de l'annuaire), saisissez **corp**.
 - Pour Directory description (Description de l'annuaire), saisissez **AWS DS Managed**.
 - Pour Mot de passe administrateur, saisissez le mot de passe que vous souhaitez utiliser pour ce compte, puis saisissez de nouveau le mot de passe dans le champ Confirmer le mot de passe. Ce compte Admin est automatiquement créé pendant le processus de création de l'annuaire. Le mot de passe ne peut pas contenir le terme admin. Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :
 - Lettres minuscules (a-z)
 - Lettres majuscules (A-Z)
 - Chiffres (0-9)
 - Caractères non alphanumériques (~!@#\$%^&*_-+=`|\\(){}[]:;'"<>,.?/)
4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).
 - Pour VPC, choisissez l'option qui commence par AWS-DS-VPC01 et qui se termine par (10.0.0.0/16).
 - Pour Subnets (Sous-réseaux), sélectionnez les sous-réseaux publics 10.0.0.0/24 et 10.0.1.0/24.
5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend entre 20 et 40 minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Méthode 2 : pour créer votre Microsoft AD AWS géré (PowerShell) (facultatif)

1. Ouvrir PowerShell.
2. Saisissez la commande suivante. Assurez-vous d'utiliser les valeurs fournies à l'étape 4 de la AWS Management Console procédure précédente.

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd  
-Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxx -  
VpcSettings_SubnetId subnet-xxxxxxx, subnet-xxxxxxx
```

Méthode 3 : pour créer votre Microsoft AD AWS géré (AWS CLI) (facultatif)

1. Ouvrez le AWS CLI.
2. Saisissez la commande suivante. Assurez-vous d'utiliser les valeurs fournies à l'étape 4 de la AWS Management Console procédure précédente.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --  
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-  
xxxxxxx,SubnetIds= subnet-xxxxxxx, subnet-xxxxxxx
```

Étape 3 : Déployer une EC2 instance Amazon pour gérer votre annuaire Microsoft AD Active Directory AWS géré

Pour cet atelier, nous utilisons des EC2 instances Amazon dotées d'adresses IP publiques afin de faciliter l'accès à l'instance de gestion où que vous soyez. Dans un environnement de production, vous pouvez utiliser des instances situées dans un VPC privé qui ne sont accessibles que via un VPN ou Direct Connect un lien. Il n'est pas nécessaire que l'instance possède une adresse IP publique.

Dans cette section, vous allez passer en revue les différentes tâches post-déploiement nécessaires pour que les ordinateurs clients puissent se connecter à votre domaine à l'aide de Windows Server sur votre nouvelle EC2 instance. Vous allez utiliser Windows Server dans l'étape suivante pour vérifier que votre atelier de test est opérationnel.

Facultatif : créez un ensemble d'options DHCP dans AWS-DS-VPC01 pour votre répertoire

Dans cette procédure facultative, vous configurez une étendue d'options DHCP afin que les EC2 instances de votre VPC utilisent automatiquement votre Microsoft AD AWS géré pour la résolution DNS. Pour plus d'informations, veuillez consulter [DHCP options sets](#) (français non garanti).

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, entrez les valeurs suivantes pour votre annuaire :
 - Pour Name (Nom), tapez **AWS DS DHCP**.
 - Pour Domain name (Nom de domaine), tapez **corp.example.com**.
 - Pour Domain name servers (Serveurs de noms de domaine), tapez les adresses IP des serveurs DNS de votre annuaire fourni par AWS .

 Note

Pour trouver ces adresses, rendez-vous sur la page Directory Service Répertoires, puis choisissez l'ID de répertoire applicable. Sur la page Détails, identifiez et utilisez IPs les informations affichées dans l'adresse DNS.

Pour trouver ces adresses, rendez-vous sur la page Directory Service Annuaire, puis choisissez l'ID de répertoire applicable. Choisissez ensuite Mettre à l'échelle et partager. Sous Contrôleurs de domaine, identifiez et utilisez IPs ceux qui sont affichés dans l'adresse IP.

- Ne renseignez aucune valeur dans les champs Serveurs NTP, Serveurs de noms NetBIOS et Type de nœud NetBIOS.
4. Choisissez Créer un jeu d'options DHCP, puis choisissez Fermer. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
 5. Notez l'ID du nouveau jeu d'options DHCP (dopt- **xxxxxxxx**). Vous en aurez besoin à la fin de cette procédure lorsque vous associerez le nouveau jeu d'options à votre VPC.

 Note

La jonction transparente de domaines fonctionne sans qu'il soit nécessaire de configurer un jeu d'options DHCP.

6. Dans le volet de navigation, sélectionnez Votre VPCs.
7. Dans la liste de VPCs, sélectionnez AWS DS VPC, choisissez Actions, puis choisissez Modifier le jeu d'options DHCP.
8. Sur la page Modifier le jeu d'options DHCP, sélectionnez les options que vous avez enregistrées à l'étape 5, puis choisissez Enregistrer.

Créez un rôle pour joindre des instances Windows à votre domaine Microsoft AD AWS géré

Utilisez cette procédure pour configurer un rôle qui joint une instance Amazon EC2 Windows à un domaine. Pour de plus amples informations, veuillez consulter [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).

Pour configurer EC2 l'association d'instances Windows à votre domaine

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
4. Immédiatement sous Choisissez le service qui utilisera ce rôle, choisissez EC2, puis cliquez sur Suivant : Autorisations.
5. Sur la page Stratégie d'autorisations attachée, procédez comme suit :
 - Cochez la case à côté de la politique SSManaged InstanceCore gérée par Amazon. Cette stratégie fournit les autorisations minimales nécessaires pour pouvoir utiliser le service Systems Manager.
 - Cochez la case à côté de la politique SSMDirectory ServiceAccess gérée par Amazon. La stratégie fournit les autorisations nécessaires pour joindre des instances à un domaine Active Directory géré par Directory Service.

Pour plus d'informations sur ces politiques gérées et sur les autres politiques que vous pouvez attacher à un profil d'instance IAM pour Systems Manager consultez [Création d'un profil d'instance IAM pour Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager . Pour plus d'informations sur les politiques gérées, veuillez consulter [AWS Managed policies](#) (français non garanti) dans le Guide de l'utilisateur IAM.

6. Sélectionnez Suivant : Étiquettes.
7. (Facultatif) Ajoutez une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès pour ce rôle, puis sélectionnez Suivant : Vérifier.
8. Dans Nom du rôle, entrez un nom pour le rôle qui décrit qu'il est utilisé pour joindre des instances à un domaine, tel que EC2DomainJoin.
9. (Facultatif) Pour Role description (Description du rôle), entrez une description.
10. Sélectionnez Créer un rôle. Le système vous renvoie à la page Rôles.

Créez une EC2 instance Amazon et rejoignez automatiquement le répertoire

Dans cette procédure, vous configurez un système Windows Server dans une EC2 instance qui pourra être utilisée ultérieurement pour administrer les utilisateurs, les groupes et les politiques dans Active Directory.

Pour créer une EC2 instance et rejoindre automatiquement le répertoire

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Launch Instances (Lancer les instances).
3. Sur la page Étape 1, à côté de Microsoft Windows Server 2019 Base - ami-,
xxxxxxxxxxxxxxxxxxxx choisissez Sélectionner.
4. Sur la page Step 2 (Étape 2), sélectionnez t3.micro (notez que vous pouvez choisir un type d'instance plus volumineux), puis cliquez sur Next: Configure Instance Details (Suivant : Configurer les détails de l'instance).
5. Sur la page Étape 3, procédez comme suit :
 - Pour Réseau, choisissez le VPC qui se termine par -DS-VPC01 (par exemple, AWS vpc- | -DS-VPC01). **xxxxxxxxxxxxxxxxxxxx** AWS

- Pour Sous-réseau, choisissez le sous-réseau public 1, qui doit être préconfiguré pour votre zone de disponibilité préférée (par exemple, subnet- **xxxxxxxxxxxxxxxxxx** | -DS-VPC01-subnet01 | AWS). *us-west-2a*
 - Pour Attribuer automatiquement l'adresse IP publique, choisissez Activer (si le sous-réseau n'est pas défini sur Activer par défaut).
 - Pour le répertoire de jointure de domaines, choisissez corp.example.com (d-). **xxxxxxxxxx**
 - Pour le rôle IAM, choisissez le nom dans lequel vous avez attribué votre rôle d'instance [Créez un rôle pour joindre des instances Windows à votre domaine Microsoft AD AWS géré](#), par exemple. EC2DomainJoin
 - Conservez les valeurs par défaut des autres paramètres.
 - Choisissez Next: Add Storage (Suivant : Ajouter le stockage).
6. Sur la page Étape 4, conservez les paramètres par défaut, puis choisissez Next: Add Tags.
 7. Sur la page Étape 5, choisissez Add Tag. Sous Key (Clé), saisissez **corp.example.com-mgmt**, puis choisissez Next: Configure Security Group (Suivant : Configurer le groupe de sécurité).
 8. Sur la page Étape 6, choisissez Sélectionner un groupe de sécurité existant, sélectionnez AWS DS Test Lab Security Group (que vous avez précédemment défini dans le [didacticiel de base](#)), puis choisissez Vérifier et lancer pour vérifier votre instance.
 9. Sur la page Étape 7, vérifiez la page, puis choisissez Lancer.
 10. Dans la boîte de dialogue Sélectionner une paire de clés existante ou créer une nouvelle paire de clés, procédez comme suit :
 - Choisissez Choisir une paire de clés existante.
 - Sous Sélectionner une paire de clés, choisissez AWS-DS-KP.
 - Cochez la case I acknowledge....
 - Choisissez Launch Instances (Démarrer les instances).
 11. Choisissez View Instances pour revenir à la EC2 console Amazon et consulter l'état du déploiement.

Installez les outils Active Directory sur votre EC2 instance

Vous pouvez choisir entre deux méthodes pour installer les outils de gestion de domaine Active Directory sur votre EC2 instance. Vous pouvez utiliser l'interface utilisateur du gestionnaire de serveur (recommandée pour ce didacticiel) ou PowerShell.

Pour installer les outils Active Directory sur votre EC2 instance (Gestionnaire de serveur)

1. Dans la EC2 console Amazon, choisissez Instances, sélectionnez l'instance que vous venez de créer, puis sélectionnez Connect.
2. Dans la boîte de dialogue Connect to your instance, choisissez Get Password pour récupérer votre mot de passe si ce n'est pas déjà fait, puis choisissez Download Remote Desktop File.
3. Dans la boîte de dialogue Windows Security (Sécurité Windows) saisissez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter (par exemple : **administrator**).
4. Dans le menu Démarrer, choisissez Server Manager.
5. Dans le Tableau de bord, choisissez Ajouter des rôles et des fonctionnalités.
6. Dans l'Assistant Ajouter des rôles et des fonctionnalités, choisissez Suivant.
7. Sur la page Sélectionner le type d'installation, choisissez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
8. Sur la page Sélectionner le serveur de destination, assurez-vous que le serveur local est sélectionné, puis choisissez Suivant.
9. Sur la page Sélectionner des rôles de serveur, cliquez sur Suivant.
10. Sur la page Sélectionner les fonctionnalités, procédez comme suit :
 - Cochez la case Gestion des stratégies de groupe.
 - Développez Outils d'administration de serveur distant, puis Outils d'administration de rôles.
 - Cochez la case Outils AD DS et AD LDS.
 - Cochez la case DNS Server Tools.
 - Choisissez Suivant.
11. Sur la page Confirmer les sélections d'installation, vérifiez les informations, puis cliquez sur Installer. Une fois l'installation des fonctionnalités terminée, les nouveaux outils ou composants suivants seront disponibles dans le dossier Outils d'administration Windows, via le menu Démarrer.

- Centre d'administration Active Directory
- Domaines et approbations Active Directory
- Module Active Directory pour PowerShell
- Sites et services Active Directory
- Utilisateurs et ordinateurs Active Directory
- ADSI Edit
- DNS
- Gestion des stratégies de groupe

Pour installer les outils Active Directory sur votre EC2 instance (PowerShell) (Facultatif)

1. Démarrer PowerShell.
2. Saisissez la commande suivante.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

Étape 4 : vérifier que l'atelier de test de base est opérationnel

Utilisez la procédure suivante pour vérifier que l'atelier de test a bien été configuré avant d'ajouter d'autres modules de guide pour votre atelier de test. Cette procédure permet de vérifier que votre serveur Windows est correctement configuré, qu'il peut se connecter au domaine corp.example.com et qu'il est utilisé pour administrer votre forêt AWS Microsoft AD gérée.

Pour vérifier que l'atelier de test est opérationnel

1. Déconnectez-vous de l' EC2 instance à laquelle vous étiez connecté en tant qu'administrateur local.
2. De retour dans la EC2 console Amazon, choisissez Instances dans le volet de navigation. Sélectionnez ensuite l'instance que vous avez créée. Choisissez Se connecter.
3. Dans la boîte de dialogue Connectez-vous à votre instance, choisissez Télécharger le fichier Bureau à distance.

4. Dans la boîte de dialogue Windows Security (Sécurité Windows), saisissez vos informations d'identification d'administrateur local pour que le domaine CORP puisse se connecter (par exemple, **corp\admin**).
5. Une fois connecté, dans le menu Démarrer, sous Outils d'administration Windows, choisissez Utilisateurs et ordinateurs Active Directory.
6. corp.example.com devrait s'afficher avec tous les comptes par défaut OUs et associés à un nouveau domaine. Sous Contrôleurs de domaine, notez les noms des contrôleurs de domaine qui ont été automatiquement créés lorsque vous avez créé votre AWS Managed Microsoft AD à l'étape 2 de ce didacticiel.

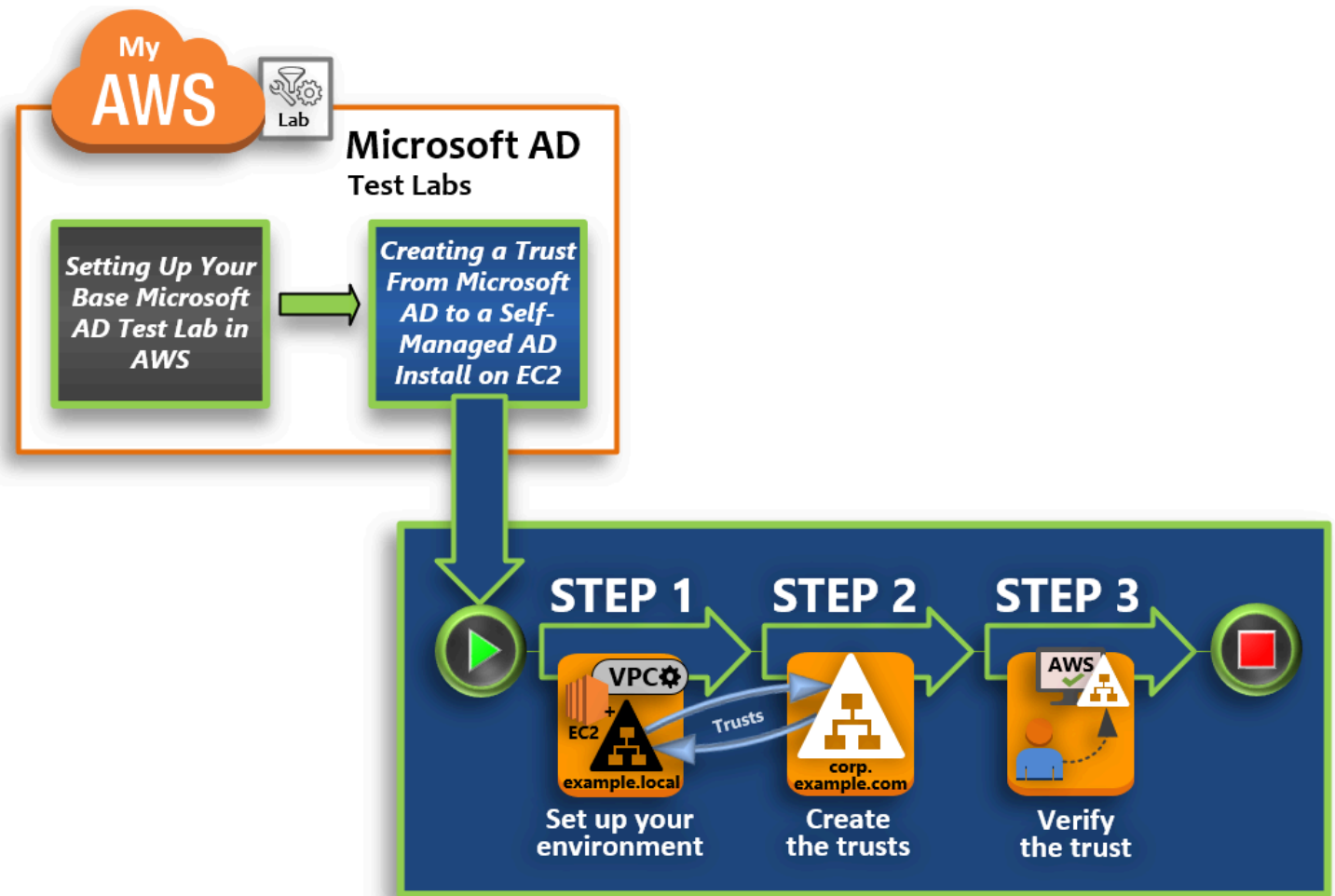
Félicitations ! Votre environnement de laboratoire de test de base Microsoft AD AWS géré est maintenant configuré. Vous pouvez commencer à ajouter le prochain atelier de test de la série.

Didacticiel suivant : [Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2](#)

Tutoriel : Création d'une relation de confiance entre AWS Managed Microsoft AD et une installation Active Directory autogérée sur Amazon EC2

Dans ce didacticiel, vous apprendrez à créer une relation de confiance entre la forêt AWS Directory Service for Microsoft Active Directory que vous avez créée dans le [didacticiel de base](#). Vous apprendrez également à créer une nouvelle forêt Active Directory native sur un serveur Windows dans Amazon EC2. Comme le montre l'illustration suivante, le laboratoire que vous créez à partir de ce didacticiel est le deuxième élément de base nécessaire pour configurer un laboratoire de test Microsoft AD AWS géré complet. Vous pouvez utiliser le laboratoire de test pour tester vos solutions basées sur AWS le cloud pur ou hybride.

Vous ne devez créer ce didacticiel qu'une seule fois. Après cela, vous pourrez ajouter des didacticiels facultatifs, si nécessaire, pour acquérir davantage d'expérience.



Étape 1 : configurer votre environnement pour les approbations

Avant de pouvoir établir des liens de confiance entre une nouvelle forêt Active Directory et la forêt Microsoft AD AWS gérée que vous avez créée dans le [didacticiel de base](#), vous devez préparer votre EC2 environnement Amazon. Pour ce faire, vous devez d'abord créer un serveur Windows Server 2019, promouvoir ce serveur en contrôleur de domaine, puis configurer votre VPC en conséquence.

Étape 2 : création des approbations

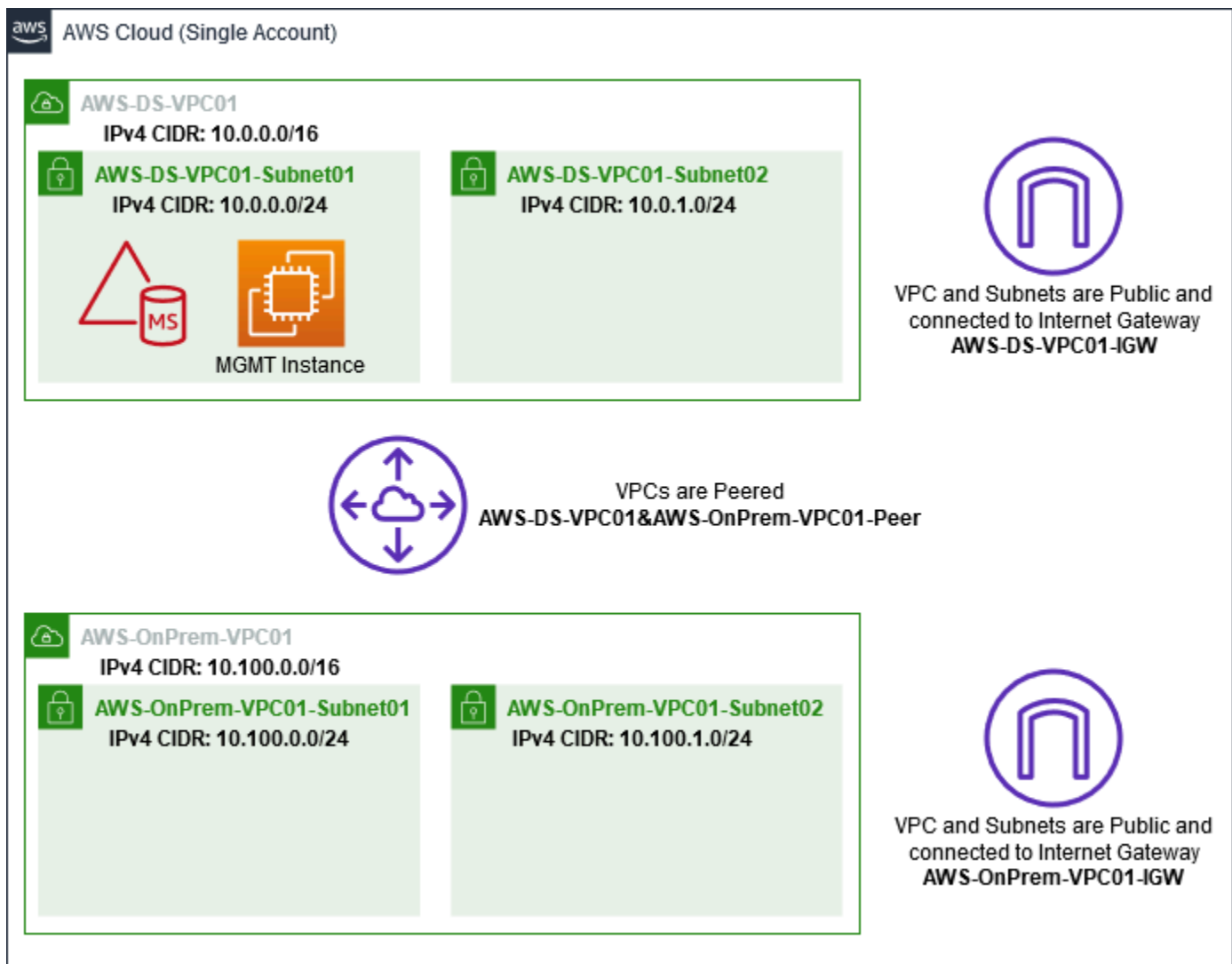
Au cours de cette étape, vous allez créer une relation de confiance bidirectionnelle entre votre forêt Active Directory nouvellement créée hébergée sur Amazon EC2 et votre forêt Microsoft AD AWS gérée dans AWS.

Étape 3 : vérification de l'approbation

Enfin, en tant qu'administrateur, vous utilisez la Directory Service console pour vérifier que les nouvelles approbations sont opérationnelles.

Étape 1 : configurer votre environnement pour les approbations

Dans cette section, vous allez configurer votre EC2 environnement Amazon, déployer votre nouvelle forêt et préparer votre VPC pour les approbations avec AWS



Création d'une EC2 instance Windows Server 2019

Utilisez la procédure suivante pour créer un serveur membre Windows Server 2019 sur Amazon EC2.

Pour créer une EC2 instance Windows Server 2019

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la EC2 console Amazon, choisissez Launch Instance.
3. Sur la page Étape 1, recherchez Microsoft Windows Server 2019 Base - ami-
xxxxxxxxxxxxxxxxxxxx dans la liste. Puis choisissez Sélectionner.

4. Sur la page Étape 2, sélectionnez t2.large, puis choisissez Suivant : Configurer les détails de l'instance.
5. Sur la page Étape 3, procédez comme suit :
 - [Pour Réseau, sélectionnez vpc- ~~xxxxxxxxxxxxxxxxxxxx~~ AWS- OnPrem -VPC01 \(que vous avez précédemment configuré dans le didacticiel de base\).](#)
 - Pour Sous-réseau, sélectionnez sous-réseau - ~~xxxxxxxxxxxxxxxxxxxx~~ | AWS- OnPrem - VPC01-Sous-réseau 01 | - -VPC01. AWS OnPrem
 - Dans la liste Attribuer automatiquement l'adresse IP publique, choisissez Activer (si le sous-réseau n'est pas défini sur Activer par défaut).
 - Conservez les valeurs par défaut des autres paramètres.
 - Choisissez Next: Add Storage (Suivant : Ajouter le stockage).
6. Sur la page Étape 4, conservez les paramètres par défaut, puis choisissez Next: Add Tags.
7. Sur la page Étape 5, choisissez Add Tag. Sous Under Key (Clé), saisissez **example.local-DC01**, puis choisissez Next: Configure Security Group (Suivant : Configurer le groupe de sécurité).
8. Sur la page Étape 6, choisissez Sélectionner un groupe de sécurité existant, sélectionnez AWS On-Prem Test Lab Security Group (que vous avez précédemment défini dans le [didacticiel de base](#)), puis choisissez Vérifier et lancer pour vérifier votre instance.
9. Sur la page Étape 7, vérifiez la page, puis choisissez Lancer.
10. Dans la boîte de dialogue Sélectionner une paire de clés existante ou créer une nouvelle paire de clés, procédez comme suit :
 - Choisissez Choisir une paire de clés existante.
 - Sous Sélectionner une paire de clés, choisissez AWS-DS-KP (que vous avez précédemment défini dans le [didacticiel de base](#)).
 - Cochez la case I acknowledge....
 - Choisissez Launch Instances (Démarrer les instances).
11. Choisissez View Instances pour revenir à la EC2 console Amazon et consulter l'état du déploiement.

Promouvoir votre serveur en contrôleur de domaine

Avant de pouvoir créer des approbations, vous devez générer et déployer le premier contrôleur de domaine pour une nouvelle forêt. Au cours de ce processus, vous configurez une nouvelle forêt Active Directory, installez DNS et définissez ce serveur afin qu'il utilise le serveur DNS local pour la résolution des noms. Vous devez redémarrer le serveur à la fin de cette procédure.

Note

Si vous souhaitez créer un contrôleur de domaine AWS qui se réplique avec votre réseau local, vous devez d'abord joindre manuellement l' EC2 instance à votre domaine local. Après cela, vous pourrez promouvoir le serveur en contrôleur de domaine.

Pour promouvoir votre serveur en contrôleur de domaine

1. Dans la EC2 console Amazon, choisissez Instances, sélectionnez l'instance que vous venez de créer, puis sélectionnez Connect.
2. Dans la boîte de dialogue Connectez-vous à votre instance, choisissez Télécharger le fichier Bureau à distance.
3. Dans la boîte de dialogue Windows Security (Sécurité Windows) saisissez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter (par exemple : **administrator**). Si vous n'avez pas encore le mot de passe de l'administrateur local, retournez sur la EC2 console Amazon, cliquez avec le bouton droit sur l'instance et choisissez Get Windows Password. Accédez à votre fichier AWS_DS_KP.pem ou votre clé .pem personnelle, puis choisissez Déchiffrer le mot de passe.
4. Dans le menu Démarrer, choisissez Server Manager.
5. Dans le Tableau de bord, choisissez Ajouter des rôles et des fonctionnalités.
6. Dans l'Assistant Ajouter des rôles et des fonctionnalités, choisissez Suivant.
7. Sur la page Sélectionner le type d'installation, choisissez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
8. Sur la page Sélectionner le serveur de destination, assurez-vous que le serveur local est sélectionné, puis choisissez Suivant.
9. Sur la page Sélectionner des rôles de serveurs, sélectionnez Services de domaine Active Directory. Dans la boîte de dialogue Assistant Ajouter des rôles et des fonctionnalités, vérifiez

que la case Inclure les outils de gestion (le cas échéant) est cochée. Cliquez sur Ajouter des fonctionnalités, puis sur Suivant.

10. Sur la page Sélectionner les fonctionnalités, choisissez Suivant.
11. Sur la page Services de domaine Active Directory, choisissez Suivant.
12. Sur la page Confirmer les sélections d'installation, choisissez Installer.
13. Une fois les fichiers binaires Active Directory installés, choisissez Fermer.
14. Lorsque le Gestionnaire de serveurs s'ouvre, recherchez un indicateur en haut de la page en regard de la mention Gérer. Lorsque cet indicateur devient jaune, le serveur est prêt à être promu.
15. Choisissez l'indicateur jaune, puis choisissez Promouvoir ce serveur en contrôleur de domaine.
16. Sur la page Configuration de déploiement, choisissez Ajouter une nouvelle forêt. Dans Root domain nam (Nom de domaine racine), saisissez **example.local**, puis choisissez Next (Suivant).
17. Sur la page Options du contrôleur de domaine, procédez comme suit :
 - Dans Niveau fonctionnel de la forêt et Niveau fonctionnel du domaine, choisissez Windows Server 2016.
 - Sous Spécifier les capacités du contrôleur de domaine, vérifiez que le serveur DNS et le catalogue global (GC) sont sélectionnés.
 - Saisissez et confirmez un mot de passe pour le mode de restauration des services d'annuaire (DSRM). Ensuite, sélectionnez Suivant.
18. Sur la page Options DNS, ignorez l'avertissement sur la délégation et choisissez Suivant.
19. Sur la page Options supplémentaires, assurez-vous que EXAMPLE est répertorié comme nom de NetBios domaine.
20. Sur la page Chemins, conservez les valeurs par défaut, puis choisissez Suivant.
21. Sur la page Vérifier les options, choisissez Suivant. Le serveur vérifie maintenant que toutes les conditions préalables requises pour le contrôleur de domaine sont remplies. Certains avertissements peuvent s'afficher, mais vous pouvez les ignorer sans risque.
22. Choisissez Installer. Une fois l'installation terminée, le serveur redémarre puis devient un contrôleur de domaine fonctionnel.

Configuration de votre VPC

Les trois procédures suivantes vous guident à travers les étapes de configuration de votre VPC pour établir une connectivité avec AWS.

Pour configurer vos règles sortantes VPC

1. [Dans la AWS Directory Service console, notez l'ID de répertoire Microsoft AD AWS géré pour corp.example.com que vous avez créé précédemment dans le didacticiel de base.](#)
2. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
3. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité).
4. Recherchez votre ID d'annuaire Microsoft AD AWS géré. Dans les résultats de la recherche, sélectionnez l'élément avec la description du groupe de sécurité AWS créé pour les contrôleurs d'**xxxxxx**annuaire D.

Note

Ce groupe de sécurité a été automatiquement créé lorsque vous avez créé votre annuaire.

5. Choisissez l'onglet Règles sortantes de ce groupe de sécurité. Choisissez Modifier, Ajouter une autre règle, puis ajoutez les valeurs suivantes :
 - Pour Type, sélectionnez Tout le trafic.
 - Pour Destination, tapez **0.0.0.0/0**.
 - Conservez les valeurs par défaut des autres paramètres.
 - Sélectionnez Save.

Pour vérifier que l'authentification préalable Kerberos est activée

1. Sur le contrôleur de domaine example.local, ouvrez le Gestionnaire de serveurs.
2. Dans le menu Tools, choisissez Active Directory Users and Computers.
3. Accédez à l'annuaire Utilisateurs, cliquez avec le bouton droit sur n'importe quel utilisateur et sélectionnez Propriétés, puis choisissez l'onglet Compte. Faites défiler la liste Options de compte vers le bas pour vérifier que l'option La pré-authentification Kerberos n'est pas nécessaire n'est pas cochée.

4. Effectuez les mêmes étapes pour le domaine corp.example.com de l'instance corp.example.com-mgmt.

Pour configurer des redirecteurs conditionnels DNS

 Note

Un redirecteur conditionnel est un serveur DNS sur un réseau qui est utilisé pour transférer des requêtes DNS en fonction du nom de domaine DNS dans la requête. Par exemple, un serveur DNS peut être configuré pour transférer toutes les requêtes qu'il reçoit pour des noms se terminant par widgets.example.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS.

1. Ouvrez la [AWS Directory Service console](#).
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sélectionnez l'ID de répertoire de votre AWS Managed Microsoft AD.
4. Prenez note du nom de domaine complet (FQDN), corp.example.com, et des adresses DNS de votre annuaire.
5. À présent, retournez sur votre contrôleur de domaine example.local, puis ouvrez le Gestionnaire de serveurs.
6. Dans le menu Tools, choisissez DNS.
7. Dans l'arborescence de la console, développez le serveur DNS du domaine pour lequel vous configurez l'approbation et accédez à Redirecteurs conditionnels.
8. Cliquez avec le bouton droit de la souris sur Redirecteurs conditionnels, puis choisissez Nouveau redirecteur conditionnel.
9. Pour le domaine DNS, saisissez **corp.example.com**.
10. Sous Adresses IP des serveurs principaux, choisissez <Cliquez ici pour ajouter... >, tapez la première adresse DNS de votre annuaire Microsoft AD AWS géré (dont vous avez pris note lors de la procédure précédente), puis appuyez sur Entrée. Répétez l'opération pour la seconde adresse DNS. Après avoir saisi les adresses DNS, il est possible que l'erreur « timeout » ou « Impossible à résoudre » s'affiche. Vous pouvez généralement ignorer ces erreurs.
11. Cochez la case Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit. Dans le menu déroulant, choisissez Tous les serveurs DNS de cette forêt, puis cliquez sur OK.

Étape 2 : création des approbations

Dans cette section, vous créez deux approbations de forêts. Une approbation est créée à partir du domaine Active Directory de votre EC2 instance et l'autre à partir de votre AWS Managed Microsoft AD in AWS.



Pour créer un lien de confiance entre votre EC2 domaine et votre Microsoft AD AWS géré

1. Connectez-vous à example.local.
2. Ouvrez le Gestionnaire de serveurs et choisissez DNS dans l'arborescence de la console. Prenez note de l' IPv4 adresse indiquée pour le serveur. Vous en aurez besoin au cours de la procédure suivante lors de la création d'un redirecteur conditionnel depuis corp.example.com vers l'annuaire example.local.
3. Dans le menu Outils, choisissez Domaines et approbations Active Directory.
4. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur example.local, puis choisissez Propriétés.
5. Dans l'onglet Approbations, choisissez Nouvelle approbation, puis Suivant.
6. Sur la page Trust Name (Nom d'approbation), saisissez **corp.example.com**, puis choisissez Next (Suivant).
7. Sur la page Type d'approbation, choisissez Approbation de forêt, puis Suivant.

Note

AWS Managed Microsoft AD prend également en charge les approbations externes. Toutefois, dans le cadre de ce didacticiel, vous allez créer une approbation de forêt bidirectionnelle.

8. Sur la page Direction d'approbation, choisissez Bidirectionnelle, puis Suivant.

 Note

Si vous décidez ultérieurement d'utiliser une approbation unidirectionnelle à la place, assurez-vous que les directions d'approbation sont correctement configurées (sortant sur le domaine d'approbation, entrant sur le domaine approuvé). Pour de plus amples informations générales, veuillez consulter [Understanding trust direction](#) (français non garanti) sur le site web de Microsoft.

9. Sur la page Sens d'approbation, choisissez Ce domaine uniquement, puis Suivant.
10. Sur la page Niveau d'authentification d'approbations sortantes, choisissez Authentification pour toutes les ressources de la forêt, puis Suivant.

 Note

Bien que Selective authentication (Authentification sélective) soit une option, pour la simplicité de ce didacticiel, nous vous recommandons de ne pas l'activer ici. Lorsqu'elle est configurée, elle restreint l'accès sur une approbation externe ou de forêt aux seuls utilisateurs d'un domaine ou d'une forêt approuvé ayant reçu explicitement des autorisations d'authentification sur des objets informatiques (ordinateurs de ressources) résidant dans le domaine ou la forêt d'approbation. Pour de plus amples informations, veuillez consulter [Configuring selective authentication settings](#) (français non garanti).

11. Sur la page Mot de passe d'approbation, saisissez le mot de passe d'approbation deux fois, puis choisissez Suivant. Vous utiliserez ce mot de passe au cours de la procédure suivante.
12. Sur la page Fin de la sélection des approbations, passez en revue les résultats, puis choisissez Suivant.
13. Sur la page Fin de la création des approbations, passez en revue les résultats, puis choisissez Suivant.
14. Sur la page Confirmer l'approbation sortante, choisissez Non, ne pas confirmer l'approbation sortante. Ensuite, sélectionnez Next
15. Sur la page Confirmer l'approbation entrante, choisissez Non, ne pas confirmer l'approbation entrante. Ensuite, sélectionnez Next
16. Sur la page Fin de l'Assistant Nouvelle approbation, choisissez Terminer.

 Note

Les relations de confiance sont une fonctionnalité globale de AWS Managed Microsoft AD. Si vous utilisez [Configuration de la réplication multirégionale pour AWS Managed Microsoft AD](#), les procédures suivantes doivent être effectuées dans [Région principale](#). Les modifications seront appliquées automatiquement à toutes les régions répliquées. Pour de plus amples informations, veuillez consulter [Caractéristiques mondiales et régionales](#).

Pour créer un lien de confiance entre votre AWS Managed Microsoft AD et votre EC2 domaine

1. Ouvrez la [AWS Directory Service console](#).
2. Choisissez l'annuaire corp.example.com.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Trust relationships (Relations d'approbation), choisissez Actions, puis sélectionnez Add trust relationship (Ajouter une relation d'approbation).
5. Dans la boîte de dialogue Ajouter une relation d'approbation, procédez comme suit :
 - Sous Trust type (Type d'approbation) sélectionnez Forest trust (Approbation de forêt).

 Note

Assurez-vous que le type d'approbation que vous choisissez ici correspond au même type d'approbation configuré dans la procédure précédente (pour créer l'approbation de votre EC2 domaine vers votre AWS Managed Microsoft AD).

- Pour Existing or new remote domain name (Nom de domaine distant existant ou nouveau), tapez exemple.local.
- Pour Mot de passe d'approbation, saisissez le même mot de passe que vous avez fourni au cours de la procédure précédente.
- Dans Trust direction (Direction d'approbation), sélectionnez Two-Way (Bidirectionnelle).

 Note

- Si vous décidez ultérieurement d'utiliser une approbation unidirectionnelle à la place, assurez-vous que les directions d'approbation sont correctement configurées (sortant sur le domaine d'approbation, entrant sur le domaine approuvé). Pour de plus amples informations générales, veuillez consulter [Understanding trust direction](#) (français non garanti) sur le site web de Microsoft.
 - Bien que Selective authentication (Authentification sélective) soit une option, pour la simplicité de ce didacticiel, nous vous recommandons de ne pas l'activer ici. Lorsqu'elle est configurée, elle restreint l'accès sur une approbation externe ou de forêt aux seuls utilisateurs d'un domaine ou d'une forêt approuvé ayant reçu explicitement des autorisations d'authentification sur des objets informatiques (ordinateurs de ressources) résidant dans le domaine ou la forêt d'approbation. Pour de plus amples informations, veuillez consulter [Configuring selective authentication settings](#) (français non garanti).
- Dans Conditional forwarder (Redirecteur conditionnel), saisissez l'adresse IP de votre serveur DNS dans la forêt example.local (dont vous avez pris note au cours de la procédure précédente).

 Note

Un redirecteur conditionnel est un serveur DNS sur un réseau qui est utilisé pour transférer des requêtes DNS en fonction du nom de domaine DNS dans la requête. Par exemple, un serveur DNS peut être configuré pour transférer toutes les requêtes qu'il reçoit pour des noms se terminant par widgets.example.com à l'adresse IP d'un serveur DNS spécifique ou aux adresses IP de plusieurs serveurs DNS.

6. Choisissez Ajouter.

Étape 3 : vérification de l'approbation

Dans cette section, vous testez si les approbations ont été correctement configurées entre AWS et Active Directory sur Amazon EC2.

Pour vérifier l'approbation

1. Ouvrez la [AWS Directory Service console](#).
2. Choisissez l'annuaire corp.example.com.
3. Sur la page Détails de l'annuaire, procédez de l'une des manières suivantes :
 - Si plusieurs régions apparaissent sous Réplication sur plusieurs régions, sélectionnez la région principale, puis cliquez sur l'onglet Mise en réseau et sécurité. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).
 - Si aucune région n'apparaît sous Réplication sur plusieurs régions, choisissez l'onglet Réseau et sécurité.
4. Dans la section Relations d'approbation, sélectionnez la relation d'approbation que vous venez de créer.
5. Choisissez Actions, puis Vérifier la relation d'approbation.

Une fois la vérification terminée, la mention Vérifié devrait s'afficher dans la colonne Statut.

Félicitations, vous avez terminé ce didacticiel ! Vous disposez à présent d'un environnement Active Directory multi-forêts entièrement fonctionnel à partir duquel vous pouvez commencer à tester différents scénarios. Des didacticiels d'atelier de test supplémentaires sont planifiés en 2018. Revenez sur cette page occasionnellement pour découvrir les nouveautés.

AWS Quotas Microsoft AD gérés

Les quotas par défaut pour AWS Managed Microsoft AD sont les suivants. Sauf indication contraire, chaque quota est spécifique à une région.

AWS Quotas Microsoft AD gérés

Ressource	Quota par défaut
AWS Répertoires Microsoft AD gérés (éditions Standard et Enterprise)	20
AWS Répertoires Microsoft AD gérés (édition hybride)	5

Ressource	Quota par défaut
Instantanés manuels (éditions Standard et Enterprise) *	5 par Microsoft AD AWS géré
Durée des instantanés manuels **	180 jours
Nombre maximal de contrôleurs de domaine par annuaire	20
Domaines partagés via Microsoft AD standard ***	25
Domaines partagés via Microsoft AD Entreprise ***	500
Domaines partagés par Microsoft AD hybride ***	125
Nombre maximal de certificats d'autorité de certification enregistrés par annuaire	5
Nombre maximum de AWS régions au total dans un AWS seul répertoire Microsoft AD (Enterprise Edition) ****	5

* Le quota d'instantanés manuels ne peut pas être modifié.

** La durée maximale de prise en charge pour un instantané manuel est de 180 jours et ne peut pas être modifiée. Cela est dû à l'attribut appelé « Tombstone-Lifetime » des objets supprimés. Il définit la durée de conservation d'une sauvegarde de l'état du système d'Active Directory. Il n'est pas possible d'effectuer une restauration à partir d'un instantané datant de plus de 180 jours. Pour plus d'informations, veuillez consulter la section [Useful shelf life of a system-state backup of Active Directory](#) (français non garanti) sur le site web Microsoft.

*** Le quota par défaut du domaine partagé fait référence au nombre de comptes avec lesquels un répertoire individuel peut être partagé.

**** Cela inclut 1 région principale et jusqu'à 4 régions supplémentaires. Pour de plus amples informations, veuillez consulter [Régions principales et régions supplémentaires](#).

 Note

Vous ne pouvez pas associer d'adresse IP publique à votre AWS Elastic Network Interface (ENI).

Pour plus d'informations concernant la conception d'applications et de la répartition des charges, veuillez consulter [Meilleures pratiques lors de la programmation de vos applications pour un Microsoft AD AWS géré](#).

Pour les quotas de stockage et d'objets, veuillez consulter Comparison Table sur la page [AWS Directory Service Pricing](#) (français non garanti).

Résolution des problèmes liés AWS à Managed Microsoft AD

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la création ou de l'utilisation de votre répertoire Microsoft AD Active Directory AWS géré.

Problèmes liés à votre Microsoft AD AWS géré

Certaines tâches de dépannage ne peuvent être effectuées que par Support. Voici certaines des tâches à accomplir :

- Redémarrer les contrôleurs de domaine que vous Directory Service avez fournis.
- [Mise à niveau de votre Microsoft AD AWS géré](#).

Pour créer un dossier d'assistance, consultez les sections [Création de dossiers d'assistance et gestion des dossiers](#).

Problèmes liés à Netlogon et aux communications par canal sécurisé

En guise d'atténuation contre le [CVE-2020-1472](#), Microsoft a publié un correctif qui modifie la façon dont les communications par canal sécurisé Netlogon sont traitées par les contrôleurs de domaine. Depuis l'introduction de ces modifications relatives à la sécurité Netlogon, certaines connexions

Netlogon (serveurs, postes de travail et validations de confiance) peuvent ne pas être acceptées par votre Managed Microsoft AD. AWS

Pour vérifier si votre problème est lié à Netlogon ou aux communications par canal sécurisé, recherchez dans Amazon CloudWatch Logs l'événement IDs 5827 (pour les problèmes liés à l'authentification des appareils) ou 5828 (pour les problèmes liés à la validation AD Trust). Pour plus d'informations sur CloudWatch AWS Managed Microsoft AD, consultez [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#).

Pour plus d'informations sur les mesures d'atténuation contre le CVE-2020-1472, consultez [Comment gérer les modifications des connexions au canal sécurisé Netlogon associées au CVE-2020-1472 sur le site Web de Netlogon](#). Microsoft

Vous recevez un message d'erreur « État de réponse : 400 mauvaise demande » lorsque vous tentez de réinitialiser le mot de passe d'un utilisateur

Vous recevez un message d'erreur semblable au suivant lorsque vous tentez de réinitialiser le mot de passe d'un utilisateur :

Response Status: 400 Bad Request

Vous pouvez rencontrer ce problème lorsque votre unité organisationnelle Microsoft AD AWS gérée contient des objets dupliqués portant des noms d'ouverture de session utilisateur identiques. Les noms de connexion des utilisateurs doivent être uniques. Pour plus d'informations, consultez la section [Résolution des problèmes liés aux données de répertoire](#) dans la Microsoft documentation.

Récupération d'un mot de passe

Si un utilisateur oublie un mot de passe ou rencontre des difficultés pour se connecter à votre répertoire AWS Managed Microsoft AD, vous pouvez réinitialiser son mot de passe à l'aide du AWS Management Console, PowerShell ou du AWS CLI.

Pour de plus amples informations, veuillez consulter [Réinitialisation d'un AWS mot de passe utilisateur Microsoft AD géré](#).

Ressources supplémentaires

Les ressources suivantes peuvent vous aider à résoudre les problèmes pendant que vous travaillez avec AWS.

- [AWS Centre de connaissances](#) : recherchez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Centre de support](#) : bénéficiez d'une assistance technique.
- [AWS Premium Support Center](#) : bénéficiez d'un support technique haut de gamme.

Les ressources suivantes peuvent vous aider à résoudre les problèmes courants liés à Active Directory.

- [Documentation Active Directory](#)
- [AD DS Résolutions des problèmes](#)

Rubriques

- [Erreurs de jointure de domaine d'instance Amazon EC2 Linux](#)
- [AWS Microsoft AD géré, faible espace de stockage disponible](#)
- [Erreurs d'extension de schéma](#)
- [Raisons liées aux statuts de création d'une relation d'approbation](#)

Erreurs de jointure de domaine d'instance Amazon EC2 Linux

Ce qui suit peut vous aider à résoudre certains messages d'erreur que vous pourriez rencontrer lorsque vous joignez une instance Amazon EC2 Linux à votre répertoire AWS Managed Microsoft AD.

Impossible d'effectuer la jonction de domaine ou l'authentification d'instances Linux

Les instances Ubuntu 14.04, 16.04 et 18.04 doivent pouvoir être résolues à l'envers dans le DNS pour qu'un domaine puisse fonctionner avec Microsoft Active Directory. Sinon, vous risquez de rencontrer l'un des deux scénarios suivants :

Scénario 1 : Instances Ubuntu qui ne sont pas encore jointes à un domaine

Pour les instances Ubuntu qui tentent de joindre un domaine, la commande `sudo realm join` peut ne pas fournir les autorisations requises pour joindre le domaine et afficher l'erreur suivante :

! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXEMPLE.COM domain: Couldn't authenticate to

active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) !
Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain

Scénario 2 : Instances Ubuntu qui sont jointes à un domaine

Pour les instances Ubuntu déjà jointes à un domaine Microsoft Active Directory, les tentatives de connexion SSH à l'instance à l'aide des informations d'identification du domaine peuvent échouer avec les erreurs suivantes :

```
$ ssh admin@EXEMPLE.COM@198.51.100
```

aucune identité de ce type :/Users/username/.ssh/id_ed25519 : aucun fichier ou répertoire de ce type
admin@EXEMPLE.COM@198.51.100's password:

Permission denied, please try again.

admin@EXEMPLE.COM@198.51.100's password:

Si vous vous connectez à l'instance avec une clé publique et que vous vérifiez `/var/log/auth.log`, vous risquez de voir les erreurs suivantes d'utilisateur introuvable :

```
May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0
```

```
May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXEMPLE.COM
```

```
May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): received for user admin@EXEMPLE.COM: 10 (User not known to the underlying authentication module)
```

```
May 12 01:02:14 ip-192-0-2-0 sshd[2251]: Failed password for invalid user admin@EXEMPLE.COM from 203.0.113.0 port 13344 ssh2
```

```
May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0 [preauth]
```

Par contre, `kinit` pour l'utilisateur continue de fonctionner. Veuillez consulter cet exemple :

```
ubuntu @ip -192-0-2-0 : ~$ kinit admin@EXAMPLE.COM Mot de passe pour admin@EXAMPLE.COM : ubuntu @ip -192-0-2-0 : ~$ klist Cache de tickets : _1000 Principal par défaut : admin@EXAMPLE.COM FILE:/tmp/krb5cc
```

Solution

La solution recommandée actuelle pour ces deux scénarios consiste à désactiver DNS inverse dans `/etc/krb5.conf` dans la section `[libdefaults]`, comme illustré ci-dessous :

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Problème d'authentification d'approbation unidirectionnelle associé à une jonction de domaine fluide

Si une approbation sortante unidirectionnelle est établie entre votre Microsoft AD AWS géré et votre Active Directory local, vous pouvez rencontrer un problème d'authentification lorsque vous tentez de vous authentifier auprès de l'instance Linux jointe au domaine à l'aide de vos informations d'identification Active Directory fiables avec Winbind.

Erreurs

31 juillet 00:00:00 EC2 LSMWq AMAZ-T sshd [23832] : échec du mot de passe pour user@corp.example.com depuis le port xxx.xxx.xxx.xxx 18309 ssh2

31 juillet 00:05:00 EC2 AMAZ- LSMWq T sshd [23832] : pam_winbind (sshd:auth) : obtention du mot de passe (0x00000390)

31 juillet 00:05:00 EC2 AMAZ- LSMWq T sshd [23832] : pam_winbind (sshd:auth) : pam_get_item a renvoyé un mot de passe

31 juillet 00:05:00 EC2 AMAZ- LSMWq T sshd [23832] : pam_winbind (sshd:auth) : wbcLogonUser échec de la demande : WBC_ERR_AUTH_ERROR, erreur PAM : PAM_SYSTEM_ERR (4), NTSTATUS : **NT_STATUS_OBJECT_NAME_NOT_FOUND**, le message d'erreur était le suivant : Le nom de l'objet est introuvable.

31 juillet 00:05:00 EC2 AMAZ- LSMWq T sshd [23832] : pam_winbind (sshd:auth) : erreur interne du module (retval = PAM_SYSTEM_ERR (4), user = 'CORP \ user')

Solution

Pour résoudre ce problème, vous devez exclure ou supprimer une directive du fichier de configuration du module PAM (`/etc/security/pam_winbind.conf`) en procédant comme suit.

1. Ouvrez le fichier `/etc/security/pam_winbind.conf` dans un éditeur de texte.

```
sudo vim /etc/security/pam_winbind.conf
```

2. Excluez ou supprimez la directive suivante `krb5_auth = yes`.

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Arrêtez le service Winbind, puis redémarrez-le.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

AWS Microsoft AD géré, faible espace de stockage disponible

Lorsque votre Microsoft AD AWS géré est altéré en raison d'un faible espace de stockage disponible dans Active Directory, une action immédiate est requise pour rétablir l'état actif de l'annuaire. Pour connaître les deux causes les plus fréquentes de cette déficience, veuillez consulter les sections suivantes :

1. [Le dossier SYSVOL stocke des objets de politique de groupe plus qu'essentiels](#)
2. [La base de données Active Directory a atteint sa capacité maximale](#)

Pour obtenir des informations sur les tarifs relatifs au stockage Microsoft AD AWS géré, consultez la section [Directory Service Tarification](#).

Le dossier SYSVOL stocke des objets de politique de groupe plus qu'essentiels

Cette déficience est souvent causée par le stockage de fichiers non essentiels dans le dossier SYSVOL dédiés au traitement de la stratégie de groupe. Ces fichiers non essentiels peuvent être EXEs MSIs, ou tout autre fichier dont le traitement n'est pas essentiel à la stratégie de groupe. Les objets essentiels à traiter par la stratégie de groupe sont les objets de stratégie de groupe, les Logon/off scripts et le [magasin central des objets de stratégie de groupe](#). Tous les fichiers non essentiels

doivent être stockés sur un ou plusieurs serveurs de fichiers autres que vos contrôleurs de domaine Microsoft AD AWS gérés.

Si vous avez besoin de fichiers pour [l'installation du logiciel de stratégie de groupe](#), stockez-les sur un serveur de fichiers. Si vous préférez ne pas gérer vous-même un serveur de fichiers, [Amazon AWS](#) propose une option de serveur de fichiers géré FSx.

Pour supprimer les fichiers inutiles, vous pouvez accéder au partage SYSVOL via son chemin UNC (Universal Naming Convention). Par exemple, si le nom de domaine complet (FQDN) de votre domaine est exemple.com, le chemin UNC pour le SYSVOL serait « \\exemple.local\SYSVOL\exemple.local\ ». Une fois ces objets non essentiels au traitement de l'annuaire par la stratégie de groupe localisés et supprimés, l'annuaire doit redevenir actif sous 30 minutes. Si le répertoire n'est pas actif après 30 minutes, veuillez contacter le AWS Support.

En stockant seulement les fichiers de stratégie de groupe essentiels dans le dossier partagé SYSVOL, vous permettez à votre annuaire de ne pas être affecté par la distension de SYSVOL.

La base de données Active Directory a atteint sa capacité maximale

Cette déficience est souvent causée par le fait que la base de données Active Directory a atteint sa capacité maximale. Pour vérifier cela, veuillez consulter le nombre total d'objets dans votre annuaire. Nous mettons en gras le mot total pour que vous compreniez que les objets supprimés sont toujours comptabilisés dans le nombre total d'objets d'un annuaire.

Par défaut, AWS Managed Microsoft AD conserve les articles dans la corbeille de recyclage AD pendant 180 jours avant qu'ils ne deviennent des objets recyclés. Une fois un objet recyclé (désactivé), il est conservé pendant 180 jours avant d'être finalement supprimé de l'annuaire. Ainsi, un objet supprimé demeure dans la base de données de l'annuaire pendant 360 jours avant d'être définitivement supprimé. C'est pourquoi vous devez évaluer le nombre total d'objets.

Pour plus de détails sur le nombre d'objets pris en charge par AWS Managed Microsoft AD, consultez la section [Directory Service Tarification](#).

Pour obtenir le nombre total d'objets dans un répertoire qui inclut les objets supprimés, vous pouvez exécuter la PowerShell commande suivante à partir d'une instance Windows jointe au domaine. Pour apprendre à configurer une instance de gestion, reportez-vous à la section [Gestion des utilisateurs et des groupes dans AWS Managed Microsoft AD](#).

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |  
Select-Object -Property 'Count'
```

Voici un exemple de sortie de la commande ci-dessus :

```
Count
10000
```

Si le nombre total est supérieur au nombre d'objets pouvant être pris en charge par votre annuaire comme indiqué dans la note ci-dessus, cela veut dire que votre annuaire a atteint sa capacité de stockage maximale.

Voici des options permettant de résoudre cette déficience :

1. Nettoyez AD

- a. Supprimez tous les objets AD indésirables.
- b. Supprimez tous les objets indésirables de la corbeille AD. Veuillez noter que cette action est irréversible et que vous ne pourrez récupérer ces objets supprimés qu'en restaurant l'annuaire.
- c. La commande suivante supprimera définitivement tous les objets se trouvant dans la corbeille AD.

Important

Procédez avec prudence, car cette action est irréversible, et vous ne pourrez récupérer ces objets supprimés qu'en restaurant l'annuaire.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
{ ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
'*\0ADEL:*') }
Foreach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
$ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

- d. Ouvrez un dossier auprès du AWS Support pour demander la Directory Service récupération de l'espace libre.
- ## 2. Si votre répertoire est de type Standard Edition, ouvrez un dossier auprès du AWS Support pour demander que votre répertoire soit mis à niveau vers l'édition Enterprise. Cela augmentera

également le coût de votre annuaire. Pour de plus amples informations sur la tarification, veuillez consulter [Directory Service Pricing](#) (français non garanti).

Dans AWS Managed Microsoft AD, les membres du groupe AWS Delegated Deleted Object Lifetime Administrators ont la possibilité de modifier msDS-DeletedObjectLifetime l'attribut qui définit le nombre de jours pendant lesquels les objets supprimés sont conservés dans la corbeille de recyclage AD avant de devenir des objets recyclés.

Note

Il s'agit d'un sujet avancé. Si la configuration n'est pas correctement effectuée, elle peut entraîner une perte de données. Pour mieux comprendre ce procédé, nous vous invitons à passer en revue [Corbeille AD : compréhension, application, meilleures pratiques et résolution de problèmes](#).

Réduire le msDS-DeletedObjectLifetime nombre d'objets pris en charge peut vous aider à ne pas dépasser le niveau de capacité maximale. La valeur de ce nombre ne peut être inférieure à 2 jours. Une fois cette limite dépassée, vous ne pourrez plus récupérer l'objet supprimé via la corbeille AD. Pour récupérer le(s) objet(s) en question, vous devrez restaurer votre annuaire à partir d'un instantané. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#). Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné.

Pour modifier le cycle de vie de l'objet supprimé de votre annuaire, exécutez la commande suivante :

Note

Si vous exécutez la commande telle quelle, le cycle de vie de l'objet supprimé sera défini sur 30 jours. Si vous souhaitez le rallonger ou le raccourcir, remplacez « 30 » par le chiffre que vous préférez. Cependant, nous vous recommandons de ne pas dépasser 180, le nombre par défaut.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
```



```
Set-ADObject -Identity "CN=Directory Service,CN=Windows  
NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -  
Replace:@{ "msDS-DeletedObjectLifetime" = $DeletedObjectLifetime }
```

Erreurs d'extension de schéma

Les informations suivantes peuvent vous aider à résoudre certains messages d'erreur que vous pourriez rencontrer lors de l'extension du schéma de votre annuaire Microsoft AD AWS géré.

Référence

Erreur

Erreur d'ajout sur l'entrée commençant à la ligne 1 : Référence L'erreur côté serveur est : 0x202b
Une référence a été renvoyée à partir du serveur. L'erreur de serveur étendue est la suivante :
0000202B : RefErr : DSID-0310082F, données 0, 1 points d'accès \ tref 1 : 'example.com' Nombre
d'objets modifiés : 0

Résolution des problèmes

Veillez à ce que tous les champs de nom uniques disposent d'un nom de domaine correct. Dans
l'exemple ci-dessus, DC=example, dc=com doit être remplacé par le code DistinguishedName
affiché par l'applet de commande Get-ADDomain.

Impossible de lire le fichier d'importation

Erreur

Impossible de lire le fichier d'importation. Nombre d'objets modifiés : 0

Résolution des problèmes

Le fichier LDIF importé est vide (0 octet). Vérifiez que le bon fichier a été chargé.

Erreur de syntaxe

Erreur

Le fichier d'entrée Failed contient une erreur de syntaxe à la ligne 21. Le dernier jeton commence
par « q ». Nombre d'objets modifiés : 0

Résolution des problèmes

Le texte sur la ligne 21 n'a pas été formaté correctement. La première lettre du texte non valide est A. Mettez à jour la ligne 21 avec une syntaxe LDIF valide. Pour plus d'informations sur le formatage d'un fichier LDIF, veuillez consulter [Étape 1 : créer votre fichier LDIF](#).

L'attribut ou la valeur existe

Erreur

Erreur d'ajout sur l'entrée commençant à la ligne 1 : L'attribut ou la valeur existe L'erreur côté serveur est : 0x2083 Une valeur spécifique existe déjà. L'erreur de serveur étendue est la suivante : 00002083 : : DSID-03151830, #1 AtrErr : \ t0 : 00002083 : DSID-03151830, problème 1006 (ATT_OR_VALUE_EXISTS), données 0, Att 20019 (MayContain) :len 4 Nombre d'objets modifiés : 0

Résolution des problèmes

La modification du schéma a déjà été appliquée.

Aucun attribut de ce type

Erreur

Erreur d'ajout sur l'entrée commençant à la ligne 1 : Aucun attribut de ce type L'erreur côté serveur est : 0x2085 La valeur de l'attribut ne peut pas être supprimée car elle n'existe pas pour l'objet. L'erreur de serveur étendue est la suivante : 00002085 : : DSID-03152367, #1 AtrErr : \ t0 : 00002085 : DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (MayContain) :len 4 Nombre d'objets modifiés : 0

Résolution des problèmes

Le fichier LDIF essaie de supprimer un attribut d'une classe, mais cet attribut n'est actuellement pas attaché à la classe. La modification du schéma a probablement déjà été appliquée.

Erreur

Erreur d'ajout sur l'entrée commençant à la ligne 41 : Aucun attribut de ce type 0x57 Le paramètre est incorrect. L'erreur de serveur étendue est : 0x208d Objet de l'annuaire introuvable. L'erreur de serveur étendue est : « 00000057 : LdapErr : DSID-0C090D8A, commentaire : Erreur dans l'opération de conversion d'attributs, données 0, v2580" Nombre d'objets modifiés : 0

Résolution des problèmes

L'attribut répertorié à la ligne 41 est incorrect. Revérifiez l'orthographe.

Aucun objet de ce type

Erreur

Erreur d'ajout sur l'entrée commençant à la ligne 1 : Aucun attribut de ce type L'erreur côté serveur est : 0x208d Objet de l'annuaire introuvable. L'erreur de serveur étendue est la suivante : 0000208D NameErr : DSID-03100238, problème 2001 (NO_OBJECT), données 0, meilleure correspondance entre : « CN=Schema, CN=Configuration, DC=example, DC=com » Nombre d'objets modifiés : 0

Résolution des problèmes

L'objet référencé par le nom unique (DN) n'existe pas.

Raisons liées aux statuts de création d'une relation d'approbation

Lorsque la création de confiance échoue pour AWS Managed Microsoft AD, le message d'état contient des informations supplémentaires. Ce qui suit peut vous aider à comprendre le sens de ces messages.

L'accès est refusé

Accès refusé lorsque vous essayez de créer la relation d'approbation. Le mot de passe de confiance est incorrect ou les paramètres de sécurité du domaine distant ne permettent pas de configurer une approbation. Pour plus d'informations sur les fiducies, consultez [Améliorer l'efficacité de la confiance grâce aux noms de sites et DCLocator](#). Pour résoudre ce problème, essayez ce qui suit :

- Vérifiez que vous utilisez le même mot de passe de relation d'approbation que celui que vous avez utilisé lors de la création de la relation d'approbation correspondante sur le domaine distant.
- Vérifiez que les paramètres de sécurité de votre domaine permettent la création de la relation d'approbation.
- Vérifiez que votre stratégie de sécurité locale est définie correctement. En particulier, vérifiez Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously et assurez-vous que ce paramètre contient au moins les trois canaux nommés suivants :

- netlogon
 - samr
 - lsarpc
- Vérifiez que les canaux nommés ci-dessus existent en tant que valeur de la clé de NullSessionPipesregistre qui se trouve dans le chemin de registre HKLM \ SYSTEM \ \ services \ CurrentControlSet LanmanServer \ Parameters. Ces valeurs doivent être insérées sur des lignes séparées.

Note

Par défaut, Network access: Named Pipes that can be accessed anonymously n'est pas défini et affiche Not Defined. Ceci est normal, car les paramètres par défaut effectifs du contrôleur de domaine pour Network access: Named Pipes that can be accessed anonymously sont netlogon, samr, lsarpc.

- Vérifiez le paramètre de signature SMB (Server Message Block) suivant dans la politique des contrôleurs de domaine par défaut. Ces paramètres se trouvent sous Configuration de l'ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales/Options de sécurité. Ils doivent correspondre aux paramètres suivants :
 - Microsoftclient réseau : communications signées numériquement (toujours) : Par défaut : Activé
 - Microsoftclient réseau : communications signées numériquement (si le serveur est d'accord) : Par défaut : Activé
 - Microsoftserveur réseau : communications signées numériquement (toujours) : Activé
 - Microsoftserveur réseau : Signer numériquement les communications (si le client est d'accord) : Par défaut : Activé

Améliorer l'efficacité de la confiance grâce aux noms de sites et DCLocator

Le nom du premier site n' Default-First-Site-Nameest pas obligatoire pour établir des relations de confiance entre les domaines. Cependant, l'alignement des noms de sites entre les domaines peut améliorer de manière significative l'efficacité du processus Domain Controller Locator (DCLocator). Cet alignement améliore la prévision et le contrôle de la sélection des contrôleurs de domaine dans les forêts approuvées.

Le DCLocator processus est crucial pour trouver des contrôleurs de domaine dans différents domaines et forêts. Pour plus d'informations sur le DCLocator processus, consultez [Microsoftla](#)

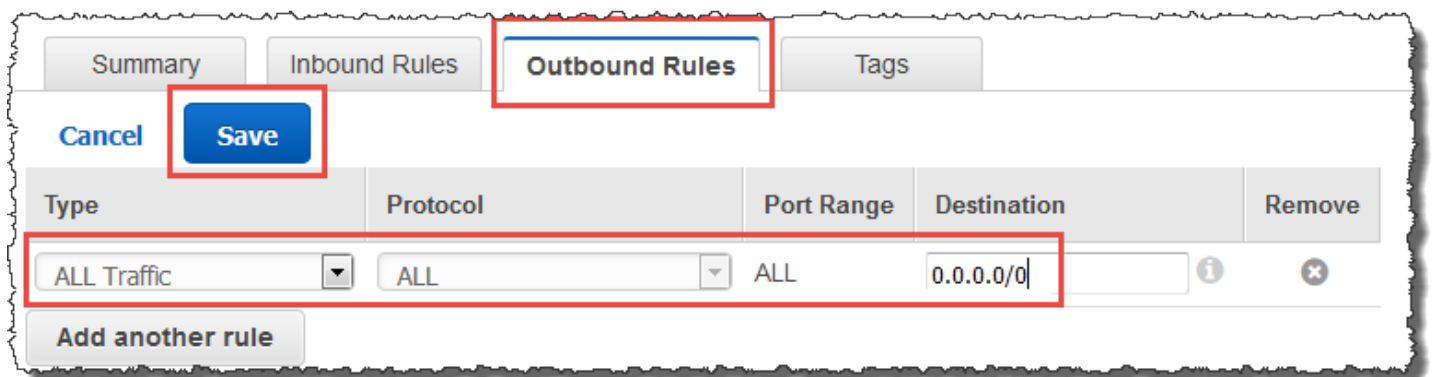
[documentation](#). Une configuration de site efficace permet une localisation plus rapide et plus précise des contrôleurs de domaine, ce qui améliore les performances et la fiabilité des opérations interforestières.

Pour plus d'informations sur la manière dont les noms de sites et les DCLocator processus interagissent, consultez les Microsoft articles suivants :

- [Comment les contrôleurs de domaine sont-ils localisés entre les trusts](#)
- [Localisateur de domaines dans les forêts](#)

Le nom de domaine spécifié n'existe pas ou n'a pas pu être contacté

Pour résoudre ce problème, assurez-vous que les paramètres du groupe de sécurité de votre domaine et de la liste de contrôle d'accès (ACL) de votre VPC sont corrects et que vous avez correctement saisi les informations relatives à votre redirecteur conditionnel. AWS configure le groupe de sécurité pour ouvrir uniquement les ports requis pour les communications Active Directory. Dans la configuration par défaut, le groupe de sécurité accepte le trafic vers ces ports à partir de n'importe quelle adresse IP. Le trafic sortant est limité au groupe de sécurité. Vous devez mettre à jour la règle sortante du groupe de sécurité pour autoriser le trafic vers votre réseau sur site. Pour plus d'informations sur les exigences de sécurité, veuillez consulter [Étape 2 : préparer votre AWS Managed Microsoft AD](#).



Si les serveurs DNS des réseaux des autres annuaires utilisent des adresses IP publiques (non conformes à la norme RFC 1918), vous devrez ajouter une route IP sur l'annuaire depuis la console Directory Services vers les serveurs DNS. Pour plus d'informations, veuillez consulter [Création, vérification ou suppression d'une relation d'approbation](#) et [Prérequis](#).

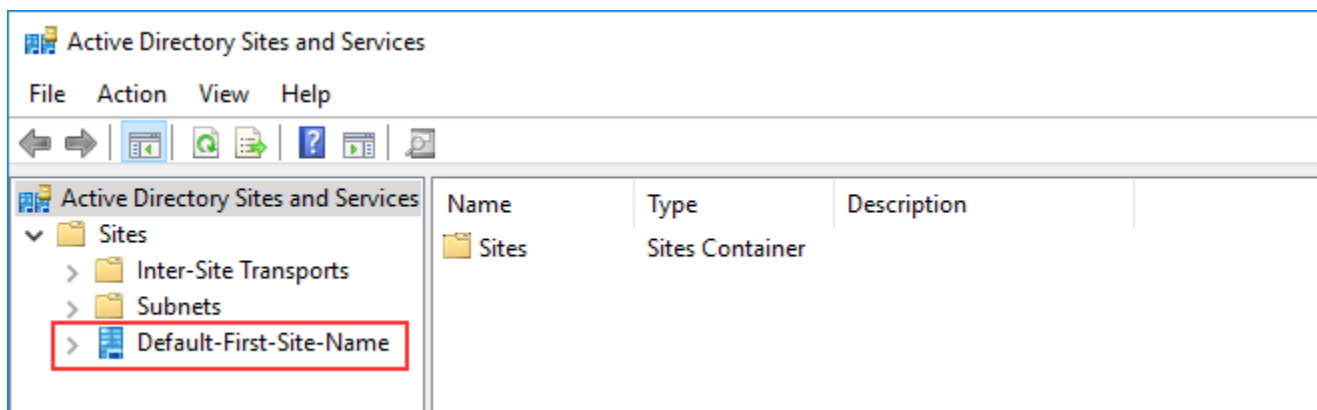
L'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants de l'espace d'adresse IP aux Internets privés :

- 10.0.0.0 - 10.255.255.255 (préfixe 10/8)
- 172.16.0.0 - 172.31.255.255 (préfixe 172.16/12)
- 192.168.0.0 - 192.168.255.255 (préfixe 192.168/16)

Pour plus d'informations, consultez <https://tools.ietf.org/html/rfc1918>.

Vérifiez que le nom du site AD par défaut de votre Microsoft AD AWS géré correspond au nom du site AD par défaut de votre infrastructure locale. L'ordinateur détermine le nom du site en utilisant un domaine dont l'ordinateur est membre, et non le domaine de l'utilisateur. Le fait de renommer le site pour qu'il corresponde au site le plus proche garantit que le localisateur de contrôleurs de domaine utilisera un contrôleur de domaine du site le plus proche. Si le problème n'est pas résolu, il est possible que les informations fournies d'un redirecteur conditionnel créé précédemment soient mises en cache et empêchent la création d'une nouvelle approbation. Patientez plusieurs minutes et essayez à nouveau de créer la confiance et un redirecteur conditionnel.

Pour plus d'informations sur son fonctionnement, consultez [Domain Locator Across a Forest Trust](#) sur le Microsoft site Web.



L'opération n'a pas pu être effectuée sur ce domaine

Pour résoudre ce problème, assurez-vous que les noms NETBIOS des deux domaines/annuaires sont différents. Si les noms NETBIOS des domaines/annuaires sont identiques, créez à nouveau l'un d'entre eux avec un nom NETBIOS différent, puis réessayez.

La création d'une relation d'approbation échoue en raison de l'erreur « Required and valid domain name » (Nom de domaine obligatoire et valide)

Les noms DNS peuvent uniquement contenir des caractères alphabétiques (A à Z), des caractères numériques (0 à 9), le signe moins (-) et un point (.). Les points ne sont autorisés que lorsqu'ils sont

utilisés pour délimiter les composants des noms de style de domaine. Éléments à prendre également en compte :

- AWS Managed Microsoft AD ne prend pas en charge les approbations avec des domaines à étiquette unique. Pour plus d'informations, consultez la section [Microsoft prise en charge des domaines à étiquette unique](#).
- Selon la RFC 1123 (<https://tools.ietf.org/html/rfc1123>), les seuls caractères pouvant être utilisés dans les étiquettes DNS sont « A » à « Z », « a » à « z », « 0 » à « 9 » et un trait d'union (« - »). Un point (.) est également utilisé dans les noms DNS, mais uniquement entre les étiquettes DNS et à la fin d'un FQDN.
- Selon la RFC 952 (<https://tools.ietf.org/html/rfc952>), un « nom » (réseau, hôte, passerelle ou nom de domaine) est une chaîne de texte comportant jusqu'à 24 caractères tirés de l'alphabet (A-Z), des chiffres (0-9), du signe moins (-) et du point (.). Notez que les points ne sont autorisés que lorsqu'ils servent à délimiter les composants des « noms de style de domaine ».

Pour plus d'informations, consultez la section [Respect des restrictions de noms pour les hôtes et les domaines](#) sur le Microsoft site Web.

Outils généraux utilisés pour tester les approbations

Les outils suivants peuvent être utilisés pour résoudre divers problèmes liés aux approbations.

AWS Outil de dépannage de Systems Manager Automation

[Support Automation Workflows \(SAW\)](#) tire parti de AWS Systems Manager Automation pour vous fournir un runbook prédéfini pour Directory Service. L'outil [AWS Support-TroubleshootDirectoryTrust](#) Runbook vous aide à diagnostiquer les problèmes courants de création de confiance entre AWS Managed Microsoft AD et un Microsoft Active Directory local.

DirectoryServicePortTest outil

L'outil de [DirectoryServicePortTest](#) peut être utile pour résoudre les problèmes de création de confiance entre AWS Managed Microsoft AD et Active Directory sur site. Pour obtenir un exemple de la manière dont l'outil peut être utilisé, veuillez consulter [Test de votre connecteur AD Connector](#).

Outils NETDOM et NLTEST

Les administrateurs peuvent utiliser les outils de ligne de commande Netdom et Nltest pour rechercher, afficher, créer, supprimer et gérer les approbations. Ces outils communiquent

directement avec l'autorité LSA d'un contrôleur de domaine. Pour un exemple d'utilisation de ces outils, consultez [Netdom](#) et [NLTEST](#) sur le Microsoft site Web.

Outil de capture de paquets

Vous pouvez utiliser l'utilitaire intégré de capture de paquets Windows pour étudier et résoudre un problème de réseau potentiel. Pour plus d'informations, veuillez consulter [Capture a Network Trace without installing anything](#) (français non garanti).

AD Connector

AD Connector est une passerelle d'annuaire grâce à laquelle vous pouvez rediriger les demandes d'annuaire vers votre site Microsoft Active Directory sans mettre en cache aucune information dans le cloud. AD Connector est disponible en deux tailles, petite et grande. Un AD Connector petit est conçu pour les petites organisations et est destiné à gérer un faible nombre d'opérations par seconde. Un grand AD Connector est conçu pour les grandes organisations et est destiné à gérer un nombre moyen à élevé d'opérations par seconde. Vous pouvez répartir les charges d'application sur plusieurs connecteurs AD Connector en fonction de vos besoins en matière de performances. Aucune limite de connexions ou d'utilisateurs n'est appliquée.

AD Connector ne prend pas en charge les approbations transitives Active Directory. Les connecteurs AD et vos domaines Active Directory locaux entretiennent une relation 1 à 1. C'est-à-dire que pour chaque domaine local, y compris les domaines enfants d'une forêt Active Directory auprès desquels vous souhaitez vous authentifier, vous devez créer un AD Connector unique.

Note

AD Connector ne peut pas être partagé avec d'autres AWS comptes. Si cela s'avère nécessaire, pensez à utiliser AWS Managed Microsoft AD pour [Partagez votre Microsoft AD AWS géré](#). AD Connector n'est pas non plus compatible avec le multi-VPC, ce qui signifie que AWS les applications de ce type [WorkSpaces](#) doivent être provisionnées dans le même VPC que votre AD Connector.

Une fois configuré, AD Connector offre les avantages suivants :

- Vos utilisateurs finaux et administrateurs informatiques peuvent utiliser leurs informations d'identification d'entreprise existantes pour se connecter à AWS des applications telles que WorkSpaces WorkDocs, ou Amazon WorkMail.
- Vous pouvez gérer AWS des ressources telles que les EC2 instances Amazon ou les compartiments Amazon S3 via un accès basé sur les rôles IAM au AWS Management Console
- Vous pouvez appliquer de manière cohérente les politiques de sécurité existantes (telles que l'expiration des mots de passe, l'historique des mots de passe et le verrouillage des comptes), que les utilisateurs ou les administrateurs informatiques accèdent aux ressources de votre infrastructure sur site ou dans le AWS cloud.

- Vous pouvez utiliser AD Connector pour activer l'authentification multifactorielle en l'intégrant à votre infrastructure MFA existante basée sur Radius afin de fournir un niveau de sécurité supplémentaire lorsque les utilisateurs accèdent aux applications. AWS

Poursuivez la lecture des rubriques de cette section pour savoir comment vous connecter à un annuaire et utiliser au mieux les fonctionnalités d'AD Connector.

Rubriques

- [Démarrer avec AD Connector](#)
- [Bonnes pratiques pour AD Connector](#)
- [Maintenance de votre annuaire AD Connector](#)
- [Sécurisation de votre annuaire AD Connector](#)
- [Surveillance de votre annuaire AD Connector](#)
- [Accès aux AWS applications et aux services depuis AD Connector](#)
- [Comment joindre une EC2 instance Amazon à votre Active Directory](#)
- [Quotas AD Connector](#)
- [Résolution des problèmes liés à AD Connector](#)

Démarrer avec AD Connector

Avec AD Connector, vous pouvez vous connecter Directory Service à l'Active Directory de votre entreprise existante. Lorsqu'il est connecté à votre annuaire existant, toutes les données de votre annuaire restent sur vos contrôleurs de domaine. Directory Service ne réplique aucune de vos données d'annuaire.

Rubriques

- [Conditions préalables requises pour AD Connector](#)
- [Création d'un AD Connector](#)
- [Ce qui est créé avec votre AD Connector](#)

Conditions préalables requises pour AD Connector

Pour vous connecter à votre annuaire existant avec AD Connector, les éléments suivants sont requis :

Amazon VPC

Configurez un VPC avec les éléments suivants :

- Au moins deux sous-réseaux. Chacun des sous-réseaux doit se trouver dans une zone de disponibilité différente et doit être du même type de réseau.

Vous pouvez l'utiliser IPv6 pour votre VPC. Pour plus d'informations, consultez la section relative à [la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

- Le VPC doit être connecté à votre réseau existant via une connexion réseau privé virtuel (VPN) ou Direct Connect.
- Le VPC doit avoir la location matérielle par défaut.

Directory Service utilise une structure à deux VPC. Les EC2 instances qui composent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, ETH0 et ETH1. ETH0 est la carte de gestion et existe en dehors de votre compte. ETH1 est créé au sein de votre compte.

La plage d'adresses IP de gestion du réseau ETH0 de votre annuaire est choisie par programmation afin de garantir qu'elle n'entre pas en conflit avec le VPC sur lequel votre annuaire est déployé. Cette plage d'adresses IP peut être comprise dans l'une des paires suivantes (car les annuaires s'exécutent dans deux sous-réseaux) :

- 10.0.1.0/24 et 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 et 192.168.2.0/24

Nous évitons les conflits en vérifiant le premier octet du CIDR ETH1. S'il commence par un 10, nous choisissons un VPC 192.168.0.0/16 avec des sous-réseaux 192.168.1.0/24 et 192.168.2.0/24. Si le premier octet est différent de 10, nous choisissons un VPC 10.0.0.0/16 avec des sous-réseaux 10.0.1.0/24 et 10.0.2.0/24.

L'algorithme de sélection n'inclut pas de routages dans votre VPC. Il est donc possible qu'un conflit de routage IP résulte de ce scénario.

Pour plus d'informations, veuillez consulter les rubriques suivantes dans le Amazon VPC Guide de l'utilisateur :

- [Qu'est-ce qu'Amazon VPC ?](#)

- [Sous-réseaux dans votre VPC](#)
- [Ajout d'une passerelle réseau privé virtuel Hardware à votre VPC](#)

Pour plus d'informations AWS Direct Connect, consultez le [guide de AWS Direct Connect l'utilisateur](#).

Active Directory existant

Vous devez vous connecter à un réseau existant doté d'un domaine Active Directory.

Note

AD Connector ne prend pas en charge les [domaines à étiquette unique](#).

Le niveau fonctionnel de ce domaine Active Directory doit être Windows Server 2003 ou supérieur. AD Connector prend également en charge la connexion à un domaine hébergé sur une EC2 instance Amazon.

Note

AD Connector ne prend pas en charge les contrôleurs de domaine en lecture seule (RODC) lorsqu'ils sont utilisés en combinaison avec la fonctionnalité de jonction de domaines Amazon EC2 .

Compte de service

Vous devez disposer des informations d'identification d'un compte de service dans l'annuaire existant auquel les privilèges suivants ont été délégués :

- Utilisateurs et groupes en lecture - Obligatoire
- Joindre des ordinateurs au domaine : obligatoire uniquement lors de l'utilisation de Seamless Domain Join et WorkSpaces
- Création d'objets informatiques : obligatoire uniquement lors de l'utilisation de Seamless Domain Join et WorkSpaces
- Le mot de passe du compte de service doit être conforme aux exigences en matière AWS de mot de passe. AWS les mots de passe doivent être :
 - Entre 8 et 128 caractères inclus.

- Contient au moins un caractère appartenant à trois des quatre catégories suivantes :
 - Lettres minuscules (a-z)
 - Lettres majuscules (A-Z)
 - Chiffres (0-9)
 - Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[];:'"<>,.?/)

Pour de plus amples informations, veuillez consulter [Délégation de privilèges à votre compte de service](#).

 Note

AD Connector utilise Kerberos pour l'authentification et l'autorisation des applications AWS . LDAP est uniquement utilisé pour les recherches d'objets par des utilisateurs et des groupes (opérations de lecture). Avec les transactions LDAP, rien n'est mutable et les informations d'identification ne sont pas transmises en texte clair. L'authentification est gérée par un service AWS interne qui utilise des tickets Kerberos pour effectuer des opérations LDAP en tant qu'utilisateur.

Autorisations des utilisateurs

Tous les utilisateurs Active Directory doivent disposer des autorisations nécessaires pour lire leurs propres attributs. Il s'agit plus précisément des attributs suivants :

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Par défaut, les utilisateurs Active Directory ont l'autorisation de lire ces attributs. Toutefois, les administrateurs peuvent modifier ces autorisations au fil du temps. Pensez donc peut-être à vérifier si vos utilisateurs disposent des autorisations en lecture avant de configurer AD Connector pour la première fois.

Adresses IP

Obtenez les adresses IP de deux contrôleurs de domaine ou serveurs DNS dans votre annuaire existant.

AD Connector obtient le `_ldap._tcp.<DnsDomainName>` et les enregistrements SRV `_kerberos._tcp.<DnsDomainName>` de ces serveurs lors de la connexion à votre annuaire, donc ces serveurs doivent comporter ces enregistrements SRV. L'AD Connector tente de trouver un contrôleur de domaine commun qui fournira à la fois les services LDAP et les services Kerberos. Ces enregistrements SRV doivent donc inclure au moins un contrôleur de domaine commun. Pour plus d'informations sur les enregistrements SRV, consultez [SRV Resource Records](#) sur Microsoft. TechNet

Ports pour les sous-réseaux

Pour qu'AD Connector redirige les demandes d'annuaire vers vos contrôleurs de domaine Active Directory existants, le pare-feu de votre réseau existant doit disposer des ports suivants ouverts vers CIDRs les deux sous-réseaux de votre Amazon VPC.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Authentification Kerberos
- TCP/UDP 389 - LDAP

Il s'agit des ports minimum requis pour qu'AD Connector puisse se connecter à votre annuaire. Votre configuration spécifique peut nécessiter l'ouverture de ports supplémentaires.

Si vous souhaitez utiliser AD Connector et Amazon WorkSpaces, l'attribut `DisableVLVSupportLDAP` doit être défini sur 0 pour vos contrôleurs de domaine. Il s'agit du paramètre par défaut pour les contrôleurs de domaine. AD Connector ne pourra pas interroger les utilisateurs de l'annuaire si l'attribut `DisableVLVSupportLDAP` est activé. Cela empêche AD Connector de fonctionner avec Amazon WorkSpaces.

Note

Si les serveurs DNS ou les serveurs de contrôleur de domaine de votre domaine Active Directory existant se trouvent dans le VPC, les ports ci-dessus doivent être ouverts aux groupes de sécurité associés à ces serveurs CIDRs pour les deux sous-réseaux du VPC.

Pour connaître les exigences de port supplémentaires, consultez la section [Exigences relatives aux ports AD et AD DS](#) dans la Microsoft documentation.

Pré-authentification Kerberos

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Pour obtenir des instructions détaillées sur la façon d'activer ce paramètre, veuillez consulter [Vérification de l'activation de l'authentification préalable Kerberos](#). Pour obtenir des informations générales sur ce paramètre, consultez la section [Préauthentification activée](#) Microsoft TechNet.

Types de chiffrement

AD Connector prend en charge les types de chiffrement suivants lors de l'authentification à vos contrôleurs de domaine Active Directory via Kerberos :

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center prérequis

Si vous envisagez d'utiliser l'IAM Identity Center avec AD Connector, vous devez vous assurer que ce qui suit est vrai :

- Votre AD Connector est configuré dans le compte de gestion de votre AWS organisation.
- Votre instance d'IAM Identity Center se trouve dans la même région que celle où votre AD Connector est configuré.

Pour plus d'informations, consultez les [conditions requises pour IAM Identity Center](#) dans le guide de l' AWS IAM Identity Center utilisateur.

Prérequis pour l'authentification multifactorielle

Pour prendre en charge l'authentification multifactorielle avec votre annuaire AD Connector, les éléments suivants sont requis :

- Un serveur [Remote Authentication Dial In User Service](#) (RADIUS) sur votre réseau existant disposant de deux points de terminaison client. Les points de terminaison client RADIUS ont les critères suivants :
 - Pour créer les points de terminaison, les adresses IP des serveurs Directory Service sont requises. Ces adresses IP peuvent être obtenues à partir du champ Directory IP Address figurant dans les détails de votre annuaire.

- Les deux points de terminaison RADIUS doivent utiliser le même code secret partagé.
- Votre réseau existant doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (1812) en provenance des Directory Service serveurs.
- Les noms d'utilisateur entre votre serveur RADIUS et votre annuaire existant doivent être identiques.

Pour en savoir plus sur l'utilisation d'AD Connector avec MFA, veuillez consulter [Enabling multi-factor authentication for AD Connector](#).

Délégation de privilèges à votre compte de service

Pour vous connecter à votre annuaire existant, vous devez disposer des informations d'identification pour votre compte de service AD Connector dans l'annuaire existant, auquel certains privilèges ont été délégués. Alors que les membres du groupe Administrateurs du domaine doivent avoir des privilèges suffisants pour se connecter à l'annuaire, en tant que bonne pratique, vous devez utiliser un compte de service disposant uniquement des privilèges minimum nécessaires pour la connexion à l'annuaire. La procédure suivante explique comment créer un nouveau groupe appelé `Connectors`, déléguer les privilèges nécessaires pour se connecter Directory Service à ce groupe, puis ajouter un nouveau compte de service à ce groupe.

Cette procédure doit être effectuée sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

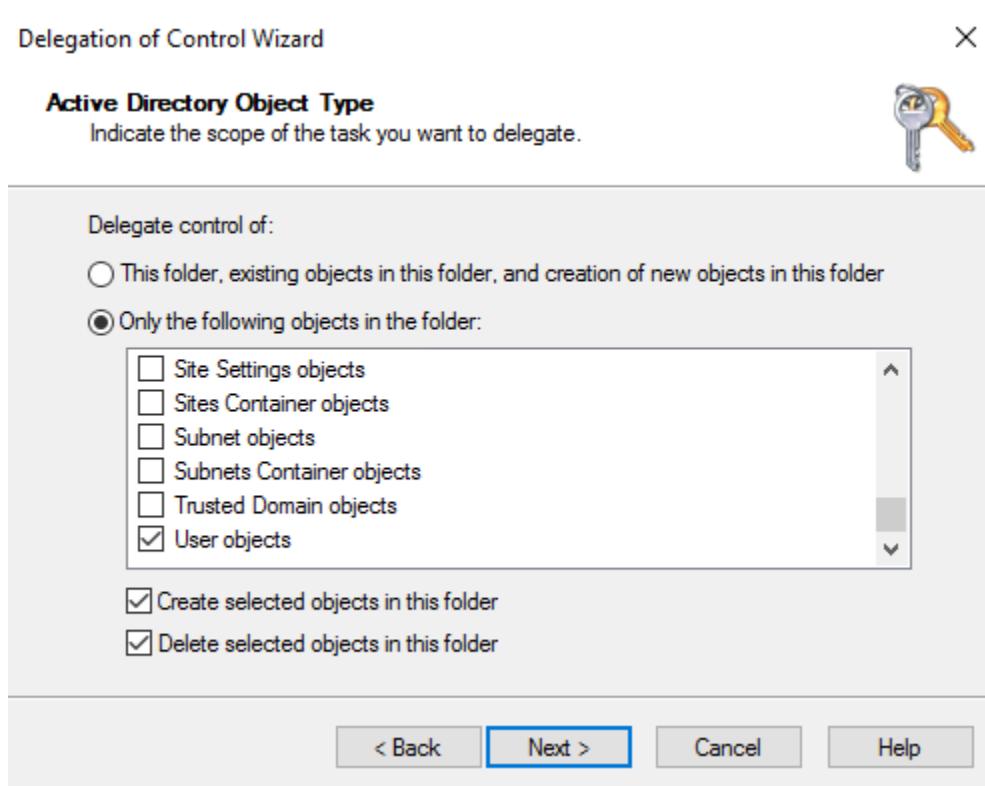
Pour déléguer des privilèges à votre compte de service

1. Ouvrez Utilisateurs et ordinateurs Active Directory, puis sélectionnez votre domaine dans l'arborescence de navigation.
2. Dans la liste du volet de gauche, effectuez un clic droit sur Utilisateurs, sélectionnez Nouveau, puis Groupe.
3. Dans la boîte de dialogue Nouvel objet - groupe, entrez la commande suivante, puis cliquez sur OK.

Champ	Valeur/sélection
Nom du groupe	Connectors

Champ	Valeur/sélection
Étendue du groupe	Solution internationale
Type de groupe	Sécurité

4. Dans l'arborescence de navigation Utilisateurs et ordinateurs Active Directory, sélectionnez identifier l'unité organisationnelle (UO) dans laquelle les comptes d'ordinateurs seront créés. Dans le menu, sélectionnez Action, puis Déléguer le contrôle. Vous pouvez sélectionner une unité d'organisation parent jusqu'au domaine au fur et à mesure que les autorisations se propagent à l'enfant OUs. Si votre AD Connector est connecté à AWS Managed Microsoft AD, vous n'aurez pas accès au contrôle délégué au niveau de la racine du domaine. Dans ce cas, pour déléguer le contrôle, sélectionnez l'unité d'organisation (UO) sous l'UO de votre annuaire où les objets ordinateur seront créés.
5. Sur la page Assistant Délégation de contrôle, cliquez sur Suivant, puis cliquez sur Ajouter.
6. Dans la boîte de dialogue Sélectionner les utilisateurs, ordinateurs ou groupes, entrez Connectors, puis cliquez sur OK. Si vous trouvez plusieurs objets, sélectionnez le groupe Connectors créé précédemment. Cliquez sur Next (Suivant).
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Sélectionnez Seulement des objets suivants dans le dossier, puis sélectionnez Objets ordinateur et Objets utilisateur.
9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.



Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

- ☐ Site Settings objects
- ☐ Sites Container objects
- ☐ Subnet objects
- ☐ Subnets Container objects
- ☐ Trusted Domain objects
- ☒ User objects

☒ Create selected objects in this folder

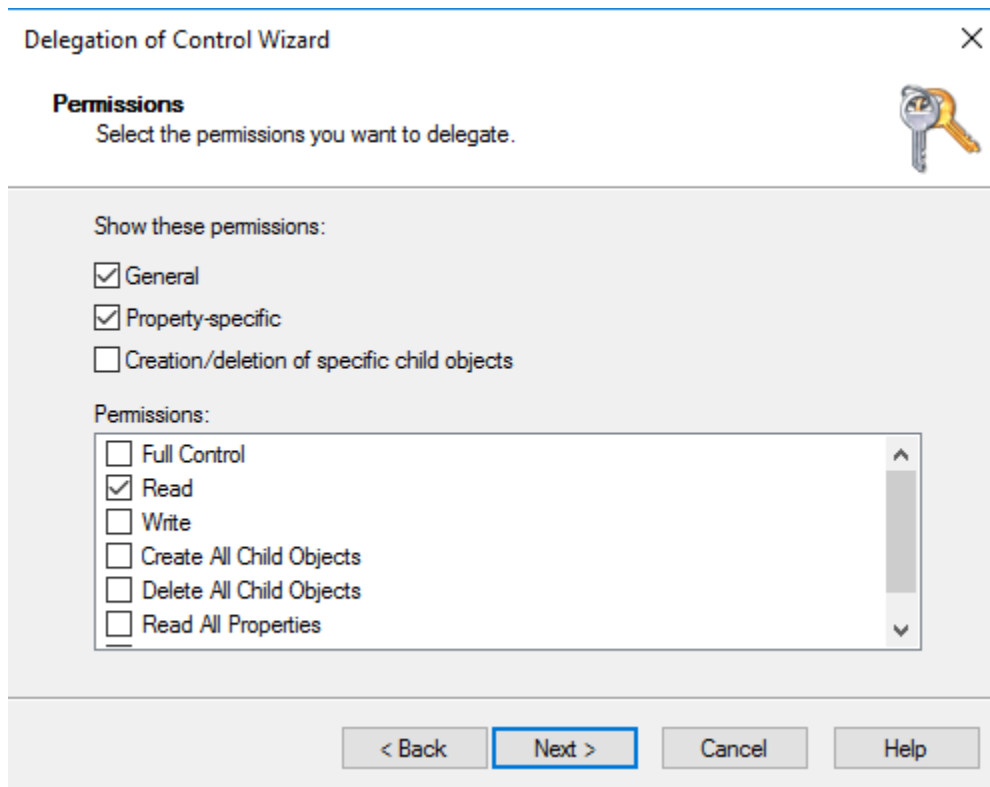
☒ Delete selected objects in this folder

< Back Next > Cancel Help

10. Sélectionnez Lecture, puis choisissez Suivant.

Note

Si vous comptez utiliser Seamless Domain WorkSpaces Join or, vous devez également activer les autorisations d'écriture afin qu'Active Directory puisse créer des objets informatiques.



11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis cliquez sur Terminer.
12. Créez un compte utilisateur avec un mot de passe fort et ajoutez-le au groupe Connectors. Cet utilisateur sera connu sous le nom de compte de service AD Connector et, comme il est désormais membre du Connectors groupe, il dispose désormais de privilèges suffisants pour se connecter Directory Service à l'annuaire.

Test de votre connecteur AD Connector

Pour qu'AD Connector puisse se connecter à votre annuaire existant, le pare-feu de votre réseau existant doit disposer de certains ports ouverts CIDRs pour les deux sous-réseaux du VPC. Pour vérifier si ces conditions sont satisfaites, exécutez les étapes suivantes :

Pour tester la connexion

1. Lancez une instance Windows dans le VPC et connectez-vous à celle-ci via RDP. L'instance doit être un membre de votre domaine existant. Les étapes restantes sont exécutées sur cette instance VPC.

2. Téléchargez et décompressez l'application de [DirectoryServicePortTest](#)test. Le code source et les fichiers de projet Visual Studio sont inclus. Vous pouvez donc modifier l'application de test si vous le souhaitez.

 Note

Ce script n'est pas pris en charge sur Windows Server 2003 ni les systèmes d'exploitation de version antérieure.

3. À partir d'une invite de commande Windows, exécutez l'application de test DirectoryServicePortTest avec les options suivantes :

 Note

L'application de DirectoryServicePortTest test ne peut être utilisée que lorsque les niveaux fonctionnels du domaine et de la forêt sont définis sur Windows Server 2012 R2 ou version inférieure.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp  
"53,88,389" -udp "53,88,389"
```

<domain_name>

Nom de domaine entièrement qualifié. Il permet de tester les niveaux fonctionnels des forêts et des domaines. Si vous excluez le nom de domaine, les niveaux fonctionnels ne seront pas testés.

<server_IP_address>

Adresse IP d'un contrôleur de domaine dans votre domaine existant. Les ports seront testés sur cette adresse IP. Si vous excluez l'adresse IP, les ports ne seront pas testés.

Cette application de test détermine si les ports nécessaires sont disponibles sur le VPC de votre domaine, et vérifie également les niveaux fonctionnels minimum des forêts et des domaines.

La sortie est similaire à ce qui suit :

```
Testing forest functional level.
```

```
Forest Functional Level = Windows2008R2Forest : PASSED
```

```
Testing domain functional level.
```

```
Domain Functional Level = Windows2008R2Domain : PASSED
```

```
Testing required TCP ports to <server_IP_address>:
```

```
Checking TCP port 53: PASSED
```

```
Checking TCP port 88: PASSED
```

```
Checking TCP port 389: PASSED
```

```
Testing required UDP ports to <server_IP_address>:
```

```
Checking UDP port 53: PASSED
```

```
Checking UDP port 88: PASSED
```

```
Checking UDP port 389: PASSED
```

Utilisez le code d'application suivant pour l'application DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;
    }
}
```

```
static void Main(string[] args)
{
    if (ParseArgs(args))
    {
        try
        {
            if (_domain.Length > 0)
            {
                try
                {
                    TestForestFunctionalLevel();

                    TestDomainFunctionalLevel();
                }
                catch (ActiveDirectoryObjectNotFoundException)
                {
                    Console.WriteLine("The domain {0} could not be found.\n",
                        _domain);
                }
            }

            if (null != _ipAddr)
            {
                if (_tcpPorts.Count > 0)
                {
                    TestTcpPorts(_tcpPorts);
                }

                if (_udpPorts.Count > 0)
                {
                    TestUdpPorts(_udpPorts);
                }
            }
        }
        catch (AuthenticationException ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
    else
    {
        PrintUsage();
    }
}
```

```
        Console.WriteLine("Press <enter> to continue.");
        Console.ReadLine();
    }

    static void PrintUsage()
    {
        string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
        Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
    }

    static bool ParseArgs(string[] args)
    {
        bool fReturn = false;
        string ipAddress = "";

        try
        {
            _tcpPorts = new List<int>();
            _udpPorts = new List<int>();

            for (int i = 0; i < args.Length; i++)
            {
                string arg = args[i];

                if ("-tcp" == arg | "/tcp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _tcpPorts = ParsePortList(portList);
                }

                if ("-udp" == arg | "/udp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
```

```
        i++;
        _domain = args[i];
    }

    if ("-ip" == arg | "/ip" == arg)
    {
        i++;
        ipAddress = args[i];
    }
}

catch (ArgumentOutOfRangeException)
{
    return false;
}

if (_domain.Length > 0 || ipAddress.Length > 0)
{
    fReturn = true;
}

if (ipAddress.Length > 0)
{
    _ipAddr = IPAddress.Parse(ipAddress);
}

return fReturn;
}

static List<int> ParsePortList(string portList)
{
    List<int> ports = new List<int>();

    char[] separators = {',', ';', ':'};

    string[] portStrings = portList.Split(separators);
    foreach (string portString in portStrings)
    {
        try
        {
            ports.Add(Convert.ToInt32(portString));
        }
        catch (FormatException)
        {
        }
    }
}
```



```
        }
    }

    return ports;
}

static void TestForestFunctionalLevel()
{
    Console.WriteLine("Testing forest functional level.");

    DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
    Forest forestContext = Forest.GetForest(dirContext);

    Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

    if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
    {
        Console.WriteLine("PASSED");
    }
    else
    {
        Console.WriteLine("FAILED");
    }

    Console.WriteLine();
}

static void TestDomainFunctionalLevel()
{
    Console.WriteLine("Testing domain functional level.");

    DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
    Domain domainObject = Domain.GetDomain(dirContext);

    Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

    if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
    {
        Console.WriteLine("PASSED");
    }
    else
```

```
        {
            Console.WriteLine("FAILED");
        }

        Console.WriteLine();
    }

    static List<int> TestTcpPorts(List<int> portList)
    {
        Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking TCP port {0}: ", port);

            TcpClient tcpClient = new TcpClient();

            try
            {
                tcpClient.Connect(_ipAddr, port);

                tcpClient.Close();
                Console.WriteLine("PASSED");
            }
            catch (SocketException)
            {
                failedPorts.Add(port);
                Console.WriteLine("FAILED");
            }
        }

        Console.WriteLine();

        return failedPorts;
    }

    static List<int> TestUdpPorts(List<int> portList)
    {
        Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();
```

```
foreach (int port in portList)
{
    Console.WriteLine("Checking UDP port {0}: ", port);

    UdpClient udpClient = new UdpClient();

    try
    {
        udpClient.Connect(_ipAddr, port);
        udpClient.Close();
        Console.WriteLine("PASSED");
    }
    catch (SocketException)
    {
        failedPorts.Add(port);
        Console.WriteLine("FAILED");
    }
}

Console.WriteLine();

return failedPorts;
}
}
```

Création d'un AD Connector

Pour vous connecter à votre annuaire existant avec AD Connector, procédez comme suit. Avant de commencer cette procédure, assurez-vous que vous avez terminé les prérequis identifiés dans [Conditions préalables requises pour AD Connector](#).

Note

Vous ne pouvez pas créer un AD Connector avec un modèle CloudFormation.

Pour vous connecter à AD Connector

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Directories (Annuaire), puis Set up directory (Configurer l'annuaire).

2. Sur la page Select directory type (Sélectionner un type d'annuaire), choisissez AD Connector, puis Next (Suivant).
3. Sur la page Enter AD Connector information (Saisir les informations AD Connector), renseignez les informations suivantes :

Taille de l'annuaire

Faites votre choix parmi les options de taille Petit ou Large. Pour en savoir plus sur les tailles, veuillez consulter [AD Connector](#).

Description de l'annuaire

Description facultative de l'annuaire.

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

VPC

VPC de l'annuaire.

Sous-réseaux

Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Connect to AD (Connecter à AD), fournissez les informations suivantes :

Nom de DNS de l'annuaire

Nom complet de votre annuaire existant, par exemple corp.example.com.

Nom NetBIOS de l'annuaire

Nom court de votre annuaire existant, tel que CORP.

DNS IP addresses (Adresses IP DNS)

Adresse IP d'au moins un serveur DNS dans votre annuaire existant. Ces serveurs doivent être accessibles à partir de chaque sous-réseau spécifié dans l'étape 4. Ces serveurs peuvent être situés à l'extérieur AWS, à condition qu'il existe une connectivité réseau entre les sous-réseaux spécifiés et les adresses IP du serveur DNS.

Nom d'utilisateur du compte de service

Nom d'utilisateur d'un utilisateur figurant dans l'annuaire existant. Pour plus d'informations sur ce compte, veuillez consulter le [Conditions préalables requises pour AD Connector](#).

Mot de passe du compte de service

Mot de passe du compte utilisateur existant. Le mot de passe est sensible à la casse et doit comporter entre 8 et 128 caractères inclus. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe du compte utilisateur existant.

6. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend plusieurs minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Pour plus d'informations sur ce qui est créé avec votre AD Connector, consultez [Ce qui est créé avec votre AD Connector](#).

Ce qui est créé avec votre AD Connector

Lorsque vous créez un AD Connector, il crée et associe Directory Service automatiquement une Elastic Network Interface (ENI) à chacune de vos instances AD Connector. Chacun de ces ENIs éléments est essentiel à la connectivité entre votre VPC et Directory Service AD Connector et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, consultez [Elastic Network Interfaces](#) dans le guide de EC2 l'utilisateur Amazon.

 Note

Les instances AD Connector sont déployées par défaut dans deux zones de disponibilité d'une région et connectées à votre cloud privé virtuel (VPC) Amazon. Les instances AD Connector qui échouent sont automatiquement remplacées dans la même zone de disponibilité en utilisant la même adresse IP.

Lorsque vous vous connectez à une AWS application ou à un service intégré à un AD Connector (AWS IAM Identity Center inclus), l'application ou le service transmet votre demande d'authentification à AD Connector, qui la transmet ensuite à un contrôleur de domaine dans votre Active Directory autogéré pour authentification. Si vous êtes authentifié avec succès auprès de votre Active Directory autogéré, AD Connector renvoie un jeton d'authentification à l'application ou au service (similaire à un jeton Kerberos). À ce stade, vous pouvez désormais accéder à l' AWS application ou au service.

Bonnes pratiques pour AD Connector

Voici quelques suggestions et directives que vous devez prendre en compte pour éviter de rencontrer des problèmes et tirer le meilleur parti d'AD Connector.

Configuration : prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.
- AD Connector connecte simplement votre Active Directory local existant à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .

- Simple AD est un annuaire de base à moindres coûts qui offre une compatibilité de base avec Active Directory. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des Directory Service options, voir [Que choisir ?](#).

Assurez-vous que vos instances VPCs et instances sont correctement configurées

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPCs répertoires auxquels ils sont associés. Consultez [Conditions préalables à la création d'un Microsoft AWS AD géré](#), [Conditions préalables requises pour AD Connector](#) ou [Prérequis pour Simple AD](#) pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans [Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré](#).

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez [AWS Quotas Microsoft AD gérés](#), [Quotas AD Connector](#) ou [Quotas Simple AD](#) pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un [groupe de sécurité](#) et l'attache aux [interfaces réseau élastiques](#) de votre annuaire qui sont accessibles depuis votre peered ou [VPCs](#) redimensionné. AWS configure le groupe de sécurité pour bloquer le trafic inutile vers le répertoire et autorise le trafic nécessaire.

Modification du groupe de sécurité de l'annuaire

Pour modifier la sécurité des répertoires de vos groupes de sécurité, vous pouvez le faire. Effectuez ces modifications uniquement si vous avez entièrement compris le fonctionnement du filtrage des groupes de sécurité. Pour plus d'informations, consultez les [groupes EC2 de sécurité Amazon pour les instances Linux](#) dans le guide de EC2 l'utilisateur Amazon. Des modifications inappropriées peuvent entraîner une perte de communication avec les ordinateurs et les instances concernés. AWS

recommande de ne pas essayer d'ouvrir des ports supplémentaires vers votre répertoire car cela réduit la sécurité de votre répertoire. Veuillez lire attentivement le [modèle de responsabilité partagée AWS](#).

 Warning

Il est techniquement possible d'associer le groupe de sécurité de l'annuaire aux autres EC2 instances que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances auxquelles vous associez le groupe de sécurité d'annuaire et peuvent interrompre le fonctionnement des instances associées. En outre, l'association du groupe de sécurité de l'annuaire à vos EC2 instances peut créer un risque de sécurité potentiel pour vos EC2 instances.

Configuration appropriée des sites locaux et des sous-réseaux dans le cadre de l'utilisation d'AD Connector

Si votre réseau sur site comporte des sites Active Directory définis, vous devez vous assurer que les sous-réseaux du VPC sur lesquels votre AD Connector réside sont définis dans un site Active Directory, et qu'il n'y a pas de conflits entre les sous-réseaux de votre VPC et les sous-réseaux de vos autres sites.

Pour découvrir les contrôleurs de domaine, AD Connector utilise le site Active Directory dont les plages d'adresses IP de sous-réseau sont proches de celles du VPC contenant l'AD Connector. Si vous avez un site comportant des sous-réseaux avec les mêmes plages d'adresses IP que votre VPC, l'AD Connector découvre les contrôleurs de domaine présents sur ce site, qui ne sont peut-être pas physiquement proches de votre région.

Comprendre les restrictions relatives aux noms d'utilisateur pour AWS les applications

Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications WorkSpaces WorkDocs, telles qu'Amazon WorkMail ou Quick Suite. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces

- Caractères multioctets
- !"#\$%&'()*+,-./:;<=>?@[\\]^_{|}~

Note

Le symbole @ est autorisé s'il précède un suffixe UPN.

Programmation de vos applications

Avant de programmer vos applications, prenez en compte les éléments suivants :

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des applications et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, répartissez votre charge parmi plusieurs annuaires du connecteur AD.

Utilisation de votre annuaire

Voici quelques suggestions à garder à l'esprit lorsque vous utilisez votre annuaire.

Effectuez une rotation régulière des informations d'identification administrateur

Modifiez régulièrement votre mot de passe administrateur de compte de service AD Connector et assurez-vous que celui-ci est conforme à vos stratégies de gestion des mots de passe Active Directory existantes. Pour obtenir des instructions sur la façon de modifier le mot de passe du compte de service, veuillez consulter [Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Management Console](#).

Utilisez des connecteurs AD uniques pour chaque domaine

Les AD Connector et vos domaines AD sur site ont une relation 1-à-1. En d'autres termes, pour chaque domaine sur site, y compris les domaines enfants dans une forêt AD par rapport à laquelle vous souhaitez vous authentifier, vous devez créer un AD Connector unique. Chaque AD Connector que vous créez doit utiliser un compte de service différent, même s'ils sont connectés dans le même annuaire.

Vérifiez la compatibilité

Lorsque vous utilisez AD Connector, vous devez vous assurer que votre annuaire local est et reste compatible avec Directory Service. Pour plus d'informations sur vos responsabilités, veuillez consulter notre [modèle de responsabilité partagée](#).

Maintenance de votre annuaire AD Connector

Vous pouvez utiliser le AWS Management Console pour gérer votre AD Connector et effectuer des tâches day-to-day administratives. Vous pouvez gérer votre répertoire de différentes manières, notamment :

- [Consultez les informations relatives à votre AD Connector](#).
- [Mettez à jour l'adresse DNS vers laquelle pointe votre AD Connector](#).
- [Supprimez votre AD Connector](#) lorsqu'il n'est plus nécessaire.

Affichage des informations de l'annuaire AD Connector

Pour afficher les informations détaillées de l'annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.

Pour de plus amples informations sur le champ Status (Statut), veuillez consulter [Comprendre le statut de votre annuaire](#).

Mise à jour du type de réseau d'annuaire

Vous pouvez mettre à jour le type de réseau de votre Directory Service annuaire en le faisant IPv4 passer à Dual-stack (IPv4 et IPv6). La mise à jour du type de réseau pour inclure les adresses IPv6 IP fournit un espace d'adressage plus important que IPv4. IPv4 et les IPv6 communications sont indépendantes l'une de l'autre.

Pour plus de détails, consultez la section [Comparer IPv4 et IPv6](#) le guide de l'utilisateur d'Amazon Virtual Private Cloud.

 Important

Il s'agit d'une opération unidirectionnelle qui ne peut pas être inversée. Testez d'abord dans un environnement hors production.

Prérequis

Avant de mettre à jour le type de réseau de votre annuaire, assurez-vous que les conditions suivantes sont remplies :

- Votre VPC doit être configuré avec des plages d'adresses IPv6 CIDR. Pour plus de détails, consultez la section relative [à la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.
- Vous avez un accès administratif au AWS Management Console.
- Votre répertoire doit être à l'état actif.
- Vous disposez des autorisations IAM appropriées pour modifier les Directory Service paramètres.

Pour mettre à jour le type de réseau d'annuaire

Pour mettre à jour votre répertoire vers un réseau à double pile

 Note

Si votre répertoire est répliqué dans plusieurs régions, effectuez cette mise à jour dans chaque région.

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sélectionnez le répertoire cible.
3. Accédez à l'onglet Réseau et sécurité.
4. Choisissez Ajouter un IPv6 support. Cette option n'est disponible que pour les répertoires IPv4 uniquement.
5. Consultez les informations de mise à jour et les détails des prix.
6. Choisissez Ajouter pour confirmer la mise à jour.

Une fois la mise à jour lancée, le statut du répertoire passe à Mise à jour pendant le processus de mise à jour. La mise à jour prend généralement 15 à 30 minutes. Une fois terminée, le statut du répertoire redevient Actif.

Mettre à jour l'adresse DNS de votre AD Connector

Utilisez les étapes suivantes pour mettre à jour les adresses DNS vers lesquelles votre AD Connector pointe.

Note

Si vous avez une mise à jour en cours, vous devez attendre la fin de son exécution avant de soumettre une nouvelle mise à jour.

Si vous utilisez WorkSpaces votre AD Connector, assurez-vous que vos adresses DNS Workspace sont également mises à jour. Pour plus d'informations, voir [Mettre à jour les serveurs DNS pour WorkSpaces](#).

Pour mettre à jour vos paramètres DNS pour AD Connector

1. Dans le volet de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Directories (Annuaire).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), choisissez l'onglet Network & Security (Réseau et sécurité).
4. Faites défiler l'écran jusqu'à la section Existing DNS settings (Paramètres DNS existants) et choisissez Update (Mettre à jour).
5. Dans la boîte de dialogue Update existing DNS addresses (Mettre à jour les adresses DNS existantes) saisissez les adresses IP DNS mises à jour, puis sélectionnez Update (Mettre à jour).

Pour plus d'informations sur la résolution des problèmes liés à AD Connector, veuillez consulter la section [Troubleshooting AD Connector](#) (français non garanti).

Supprimer votre AD Connector

Lorsqu'un connecteur AD Connector est supprimé, votre annuaire sur site reste intact. Toutes les instances qui sont jointes à l'annuaire restent également intactes et jointes à votre annuaire sur site.

Vous pouvez toutefois utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances.

Pour supprimer AD Connector

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire). Assurez-vous que vous vous trouvez Région AWS là où votre AD Connector est déployé. Pour plus d'informations, voir [Choisir une région](#).
2. Assurez-vous qu'aucune AWS application n'est activée pour l'AD Connector que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AD Connector.
 - a. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
 - b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre AD Connector.
 - Désactivez AWS Management Console l'accès. Pour de plus amples informations, veuillez consulter [Désactivation AWS Management Console de l'accès](#).
 - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez [Supprimer un répertoire](#) dans le guide d' WorkSpaces administration Amazon.
 - Pour le désactiver WorkDocs, vous devez supprimer le WorkDocs site dans la WorkDocs console. Pour plus d'informations, consultez [Supprimer un site](#) dans le guide d' WorkDocs administration Amazon.
 - Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez [Supprimer une organisation](#) dans le manuel Amazon WorkMail Administrator Guide.
 - Pour désactiver le serveur de fichiers Amazon FSx pour Windows, vous devez supprimer le système de FSx fichiers Amazon du domaine. Pour plus d'informations, consultez la section [Travailler avec Active Directory dans FSx un serveur de fichiers Windows](#) dans le guide de l'utilisateur d'Amazon FSx pour Windows File Server.
 - Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section [Managing a DB instance in a domain](#) (français non garanti) dans le Guide de l'utilisateur Amazon RDS.

- Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la [section Utilisation du Client VPN](#) dans le Guide de AWS Client VPN l'administrateur.
- Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, consultez [Supprimer votre instance Amazon Connect](#) dans le guide d'administration Amazon Connect.
- Pour désactiver Amazon Quick Suite, vous devez vous désabonner d'Amazon Quick Suite. Pour plus d'informations, consultez la section [Fermeture de votre Amazon Quick Suite compte](#) dans le guide de l'utilisateur d'Amazon Quick Suite.

 Note

Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous souhaitez supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section [Change your identity source](#) (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaire).
4. Sélectionnez uniquement l'AD Connector à supprimer, puis cliquez sur Delete (Supprimer). La suppression de l'AD Connector prend plusieurs minutes. Lorsque l'AD Connector a été supprimé, il est retiré de votre liste d'annuaire.

Sécurisation de votre annuaire AD Connector

Vous pouvez utiliser des fonctionnalités telles que l'authentification multifactorielle (MFA), le protocole Lightweight Directory Access Protocol over Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) côté client, et pour sécuriser votre AD Connector. AWS Autorité de certification privée Vous pouvez notamment sécuriser votre AD Connector :

- Activez le MFA pour renforcer la sécurité de votre AD Connector.
- Activez le protocole Lightweight Directory Access Protocol côté client via SSL (Secure Socket Layer) /Transport Layer Security (TLS) (LDAPS) afin de chiffrer les communications via LDAP et d'améliorer la sécurité.

- Activez l'authentification MTLS (Mutual Transport Layer Security) basée sur des certificats à l'aide de cartes à puce, ce qui permet aux utilisateurs de s'authentifier auprès d'Amazon Web Services via votre Active Directory et AD Connector.
- Mettez à jour les informations d'identification de votre compte de service AD Connector.
- Configurez AWS CA privée Connector for AD afin de pouvoir émettre et gérer des certificats pour votre AD Connector.

Tâches pour sécuriser votre AD Connector

- [Enabling multi-factor authentication for AD Connector](#)
- [Enabling client-side LDAPS using AD Connector](#)
- [Activation de l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce](#)
- [Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Management Console](#)
- [Configurer le AWS CA privée connecteur pour AD](#)

Enabling multi-factor authentication for AD Connector

Vous pouvez activer l'authentification multifactorielle pour AD Connector lorsque Active Directory s'exécute sur site ou sur des instances Amazon EC2 . Pour plus d'informations sur l'utilisation de l'authentification multifactorielle avec Directory Service, consultez [Conditions préalables requises pour AD Connector](#).

Note

L'authentification multifactorielle n'est pas disponible pour Simple AD. Toutefois, le MFA peut être activé pour votre annuaire AWS Microsoft AD géré. Pour de plus amples informations, veuillez consulter [Activation de l'authentification multifactorielle pour AWS Managed Microsoft AD](#).

Pour activer l'authentification multifactorielle pour AD Connector

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).

2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Networking & security (Mise en réseau et sécurité).
4. Dans la section Authentification multifactorielle, choisissez Actions, puis sélectionnez Activer.
5. Dans la page Activer l'authentification multifactorielle (MFA), indiquez les valeurs suivantes :

Afficher l'étiquette

Indiquez un nom d'étiquette.

Nom DNS ou adresses IP du serveur RADIUS

Adresses IP des points de terminaison de votre serveur RADIUS ou adresse IP de l'équilibreur de charge de votre serveur RADIUS. Vous pouvez entrer plusieurs adresses IP en les séparant par une virgule (par exemple, 192.0.0.0,192.0.0.12).

 Note

RADIUS MFA s'applique uniquement pour authentifier l' AWS Management Console accès aux applications et services Amazon Enterprise tels qu'Amazon Quick Suite ou WorkSpaces Amazon Chime. Il ne fournit pas de MFA aux charges de travail Windows exécutées sur des EC2 instances ou pour la connexion à une instance. EC2 Directory Service ne prend pas en charge Challenge/Response l'authentification RADIUS.

Les utilisateurs doivent disposer de leur code MFA au moment d'entrer leur nom d'utilisateur et leur mot de passe. Vous devez également utiliser une solution qui effectue une MFA, out-of-band telle que la vérification du texte par SMS pour l'utilisateur. Dans les solutions out-of-band MFA, vous devez vous assurer de définir la valeur du délai d'expiration RADIUS de manière appropriée pour votre solution. Lorsque vous utilisez une solution out-of-band MFA, la page de connexion invite l'utilisateur à saisir un code MFA. Dans ce cas, la bonne pratique consiste à entrer son mot de passe dans la zone de mot de passe et dans la zone MFA.

Port

Port que votre serveur RADIUS utilise pour les communications. Votre réseau local doit autoriser le trafic entrant via le port du serveur RADIUS par défaut (UDP:1812) en provenance des serveurs. Directory Service

Shared secret code

Code secret partagé qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Confirmer le code secret partagé

Confirmez le code secret partagé pour vos points de terminaison RADIUS.

Protocole

Sélectionnez le protocole qui a été spécifié lorsque vos points de terminaison RADIUS ont été créés.

Délai d'attente du serveur (en secondes)

Durée, en secondes, d'attente de la réponse du serveur RADIUS. La valeur doit être comprise entre 1 et 50.

Nombre maximal de tentatives RADIUS

Nombre de tentatives de communication avec le serveur RADIUS. La valeur doit être comprise entre 0 et 10.

L'authentification multifactorielle est disponible lorsque le paramètre RADIUS Status passe à l'état Enabled.

6. Sélectionnez Activer.

Enabling client-side LDAPS using AD Connector

La prise en charge du protocole LDAPS côté client dans AD Connector chiffre les communications entre Microsoft Active Directory (AD) et les applications. AWS Des exemples de telles applications incluent WorkSpaces, AWS IAM Identity Center, Quick Suite et Amazon Chime. Ce chiffrement vous

aide à mieux protéger les données d'identité de votre entreprise et à répondre à vos exigences en matière de sécurité.

Vous pouvez également désenregistrer et désactiver le protocole LDAPS côté client.

Rubriques

- [Prérequis](#)
- [Activation du protocole LDAPS côté client](#)
- [Gestion du LDAPS côté client](#)

Prérequis

Avant d'activer LDAPS côté client, vous devez satisfaire les exigences suivantes.

Prérequis :

- [Déployer des certificats de serveur dans Active Directory](#)
- [Exigences relatives aux certificats de CA](#)
- [Exigences liées à la mise en réseau](#)

Déployer des certificats de serveur dans Active Directory

Afin d'activer LDAPS côté client, vous devez obtenir et installer des certificats de serveur pour chaque contrôleur de domaine dans Active Directory. Ces certificats seront utilisés par le service LDAP pour écouter et accepter automatiquement les connexions SSL provenant de clients LDAP. Vous pouvez utiliser des certificats SSL émis par un déploiement ADCS (services de certificat Active Directory) interne ou achetés auprès d'un émetteur commercial. Pour plus d'informations sur les exigences relatives aux certificats de serveur Active Directory, veuillez consulter [LDAP over SSL \(LDAPS\) Certificate](#) (français non garanti) sur le site web de Microsoft.

Exigences relatives aux certificats de CA

Un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats de serveur, est requis pour le fonctionnement de LDAPS côté client. Les certificats d'une autorité de certification sont mis en correspondance avec les certificats de serveur présentés par vos contrôleurs de domaine Active Directory pour chiffrer les communications LDAP. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- Pour que vous puissiez enregistrer un certificat, celui-ci doit expirer dans plus de 90 jours.

- Les certificats doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats d'autorité de certification à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Cinq (5) certificats d'une autorité de certification au maximum peuvent être stockés par l'annuaire AD Connector.
- Les certificats utilisant l'algorithme de signature RSASSA-PSS ne sont pas pris en charge.

Exigences liées à la mise en réseau

AWS le trafic LDAP de l'application s'exécutera exclusivement sur le port TCP 636, sans retour sur le port LDAP 389. Toutefois, les communications LDAP Windows prenant en charge la réplication, les approbations, etc. continueront d'utiliser le port LDAP 389 avec une sécurité native Windows. Configurez les groupes de AWS sécurité et les pare-feux réseau pour autoriser les communications TCP sur le port 636 dans AD Connector (sortie) et dans Active Directory autogéré (entrée).

Activation du protocole LDAPS côté client

Pour activer LDAPS côté client, vous importez votre certificat d'une autorité de certification dans AD Connector, puis vous activez LDAPS sur votre annuaire. Une fois activé, tout le trafic LDAP entre les AWS applications et votre Active Directory autogéré sera crypté par canal SSL (Secure Sockets Layer).

Vous pouvez utiliser deux méthodes différentes pour activer LDAPS côté client pour votre annuaire. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Enregistrement du certificat dans Directory Service

Utilisez l'une des méthodes suivantes pour enregistrer un certificat dans Directory Service.

Méthode 1 : Pour enregistrer votre certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client sélectionnez le menu Actions, puis Enregistrer le certificat.
5. Dans la boîte de dialogue Enregistrer un certificat d'une autorité de certification, sélectionnez Parcourir, puis le certificat et choisissez Ouvrir.
6. Choisissez Register certificate (Enregistrer le certificat).

Méthode 2 : Pour enregistrer votre certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Un ID de certificat sera fourni dans la réponse.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data  
file://your_file_path
```

Vérification de l'état de l'enregistrement

Pour afficher l'état d'un enregistrement de certificat ou d'une liste de certificats enregistrés, utilisez l'une des méthodes suivantes.

Méthode 1 : pour vérifier le statut d'enregistrement du certificat dans Directory Service (AWS Management Console)

- Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
- Vérifiez l'état de l'enregistrement de certificat actuel qui s'affiche sous la colonne État de l'enregistrement. Lorsque la valeur de l'état de l'enregistrement passe à Enregistré, cela signifie que votre certificat a été enregistré avec succès.

Méthode 2 : pour vérifier le statut d'enregistrement du certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Si la valeur de l'état renvoie Registered, cela signifie que votre certificat a été enregistré avec succès.

```
aws ds list-certificates --directory-id your_directory_id
```

Activation du protocole LDAPS côté client

Utilisez l'une des méthodes suivantes pour activer le protocole LDAPS côté client dans Directory Service

Note

Avant de pouvoir activer LDAPS côté client, vous devez avoir enregistré avec succès au moins un certificat.

Méthode 1 : pour activer le protocole LDAPS côté client dans () Directory ServiceAWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Sélectionnez Activer. Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
3. Dans la boîte de dialogue Activer LDAPS côté client choisissez Activer.

Méthode 2 : pour activer le protocole LDAPS côté client dans () Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Vérification de l'état du LDAPS

Utilisez l'une des méthodes suivantes pour vérifier l'état du LDAPS dans Directory Service.

Méthode 1 : pour vérifier le statut LDAPS dans Directory Service ()AWS Management Console

1. Accédez à la section LDAPS côté client sur la page Détails de l'annuaire.
2. Si la valeur d'état est affichée en tant que Activé, cela signifie que LDAPS a été configuré avec succès.

Méthode 2 : pour vérifier le statut LDAPS dans Directory Service ()AWS CLI

- Exécutez la commande suivante. Si la valeur d'état renvoie Enabled, cela signifie que LDAPS a été configuré avec succès.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Pour plus d'informations sur l'affichage de votre certificat LDAPS côté client, le désenregistrement ou la désactivation de votre certificat LDAPS, consultez. [Gestion du LDAPS côté client](#)

Gestion du LDAPS côté client

Utilisez ces commandes pour gérer votre configuration LDAPS.

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres LDAPS côté client. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : pour afficher les détails du certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Les informations relatives au certificat sont affichées dans la section LDAPS côté client sous Certificats d'une autorité de certification.

Méthode 2 : pour afficher les détails du certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

Note

Si un seul certificat est enregistré, vous devez d'abord désactiver LDAPS avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : pour annuler l'enregistrement d'un certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.

3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Actions, puis Annuler l'enregistrement du certificat.
5. Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : pour annuler l'enregistrement d'un certificat dans Directory Service ()AWS CLI

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Désactiver LDAPS côté client

Utilisez l'une des méthodes suivantes pour désactiver LDAPS côté client.

Méthode 1 : pour désactiver le protocole LDAPS côté client dans () Directory ServiceAWS Management Console

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section LDAPS côté client choisissez Désactiver.
5. Dans la boîte de dialogue Désactiver LDAPS côté client, choisissez Désactiver.

Méthode 2 : pour désactiver le protocole LDAPS côté client dans () Directory ServiceAWS CLI

- Exécutez la commande suivante.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Activation de l'authentification mTLS dans AD Connector pour une utilisation avec des cartes à puce

Vous pouvez utiliser l'authentification mTLS (Mutual Transport Layer Security) basée sur des certificats avec des cartes à puce pour authentifier les utilisateurs sur Amazon WorkSpaces par le biais de votre Active Directory (AD) et de votre AD Connector autogérés. Lorsque cette option est activée, les utilisateurs sélectionnent leur carte à puce sur l'écran de WorkSpaces connexion et saisissent un code PIN pour s'authentifier, au lieu d'utiliser un nom d'utilisateur et un mot de passe. À partir de là, le bureau virtuel Windows ou Linux utilise la carte à puce pour s'authentifier auprès d'AD à partir du système d'exploitation de bureau natif.

Note

L'authentification par carte à puce dans AD Connector n'est disponible que dans les Régions AWS versions suivantes, et uniquement avec WorkSpaces. Les autres AWS applications ne sont pas prises en charge pour le moment.

- USA Est (Virginie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Europe (Irlande)
- AWS GovCloud (US-Ouest)
- AWS GovCloud (USA Est)

Vous pouvez également désenregistrer et désactiver les certificats.

Rubriques

- [Prérequis](#)
- [Activation de l'authentification par carte à puce](#)
- [Gestion des paramètres d'authentification par carte à puce](#)

Prérequis

Pour activer l'authentification mTLS (Mutual Transport Layer Security) basée sur des certificats à l'aide de cartes à puce pour le WorkSpaces client Amazon, vous avez besoin d'une infrastructure de cartes à puce opérationnelle intégrée à votre Active Directory autogéré. Pour plus d'informations sur la configuration de l'authentification par carte à puce avec Amazon WorkSpaces et Active Directory, consultez le [guide d' WorkSpaces administration Amazon](#).

Avant d'activer l'authentification par carte à puce pour WorkSpaces, veuillez vérifier les conditions préalables suivantes :

- [Exigences relatives aux certificats de CA](#)
- [Exigences relatives aux certificats utilisateur](#)
- [Processus de vérification de la révocation des certificats](#)
- [Considérations](#)

Exigences relatives aux certificats de CA

AD Connector nécessite un certificat d'autorité de certification (CA), qui représente l'émetteur de vos certificats utilisateur, pour l'authentification par carte à puce. AD Connector associe les certificats CA aux certificats présentés par vos utilisateurs avec leurs cartes à puce. Notez les exigences suivantes relatives aux certificats d'autorité de certification :

- Avant de pouvoir enregistrer un certificat CA, celui-ci doit expirer dans plus de 90 jours.
- Les certificats CA doivent être au format PEM (Privacy-Enhanced Mail). Si vous exportez des certificats CA à partir d'Active Directory, choisissez X.509 codé en base64 (.CER) comme format de fichier d'exportation.
- Pour que l'authentification par carte à puce réussisse, tous les certificats CA racine et intermédiaire qui relient une CA émettrice aux certificats utilisateur doivent être téléchargés.
- Cent (100) certificats CA au maximum peuvent être stockés par l'annuaire AD Connector.
- AD Connector ne prend pas en charge l'algorithme de signature RSASSA-PSS pour les certificats CA.
- Vérifiez que le service de propagation des certificats est réglé sur Automatique et qu'il est en cours d'exécution.

Exigences relatives aux certificats utilisateur

Voici certaines des exigences relatives au certificat utilisateur :

- Le certificat de carte à puce de l'utilisateur possède un nom alternatif d'objet (SAN) correspondant à celui de l'utilisateur `userPrincipalName` (UPN).
- Le certificat de carte à puce de l'utilisateur comporte une utilisation améliorée des clés en tant que connexion par carte à puce (1.3.6.1.4.1.311.20.2.2) Authentification du client (1.3.6.1.5.5.7.3.2).
- Les informations du protocole OCSP (Online Certificate Status Protocol) pour le certificat de carte à puce de l'utilisateur doivent être Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) dans le champ Authority Information Access.

Pour plus d'informations sur les exigences relatives à l'AD Connector et à l'authentification par carte à puce, consultez la section [Exigences](#) du guide d' WorkSpaces administration Amazon. Pour obtenir de l'aide pour résoudre WorkSpaces les problèmes liés à Amazon, tels que la connexion WorkSpaces, la réinitialisation du mot de passe ou la connexion à Amazon WorkSpaces, consultez la section [Résoudre les problèmes liés aux WorkSpaces clients](#) dans le guide de WorkSpaces l'utilisateur Amazon.

Processus de vérification de la révocation des certificats

Pour effectuer l'authentification par carte à puce, AD Connector doit vérifier l'état de révocation des certificats utilisateur à l'aide du protocole OCSP (Online Certificate Status Protocol). Pour vérifier la révocation des certificats, l'URL d'un répondeur OCSP doit être accessible par Internet. Si vous utilisez un nom DNS, l'URL d'un répondeur OCSP doit utiliser un domaine de premier niveau figurant dans la [Base de données de la zone racine de l'Internet Assigned Numbers Authority \(IANA\)](#).

La vérification de la révocation des certificats AD Connector se déroule de la manière suivante :

- AD Connector doit vérifier que l'extension Authority Information Access (AIA) du certificat utilisateur contient une URL de répondeur OCSP, puis AD Connector utilise l'URL pour vérifier la révocation.
- Si AD Connector ne parvient pas à résoudre l'URL trouvée dans l'extension AIA du certificat utilisateur ou à trouver une URL de répondeur OCSP dans le certificat utilisateur, AD Connector utilise alors l'URL OCSP optionnelle fournie lors de l'enregistrement du certificat CA racine.

Si l'URL de l'extension AIA du certificat utilisateur est résolue, mais ne répond pas, l'authentification de l'utilisateur échoue.

- Si l'URL du répondeur OCSP fournie lors de l'enregistrement du certificat CA racine ne peut pas être résolue, ne répond pas ou si aucune URL du répondeur OCSP n'a été fournie, l'authentification de l'utilisateur échoue.
- Le serveur OCSP doit être conforme à la norme [RFC 6960](#). En outre, le serveur OCSP doit prendre en charge les demandes utilisant la méthode GET pour les demandes dont la valeur totale est inférieure ou égale à 255 octets.

 Note

AD Connector nécessite une URL HTTP pour l'URL du répondeur OCSP.

Considérations

Avant d'activer l'authentification par carte à puce dans AD Connector, tenez compte des points suivants :

- AD Connector utilise l'authentification mutuelle basée sur des certificats (protocole TLS mutuel) pour authentifier les utilisateurs auprès d'Active Directory à l'aide de certificats de carte à puce matériels ou logiciels. Seules les cartes d'accès communes (CAC) et les cartes de vérification d'identité personnelle (PIV) sont prises en charge pour le moment. D'autres types de cartes à puce matérielles ou logicielles peuvent fonctionner mais leur utilisation avec le protocole de WorkSpaces streaming n'a pas été testée.
- L'authentification par carte à puce remplace l'authentification par nom d'utilisateur et mot de passe par WorkSpaces.

Si d'autres AWS applications sont configurées sur votre annuaire AD Connector avec l'authentification par carte à puce activée, ces applications présentent toujours l'écran de saisie du nom d'utilisateur et du mot de passe.

- L'activation de l'authentification par carte à puce limite la durée de session utilisateur à la durée de vie maximale des tickets de service Kerberos. Vous pouvez configurer ce paramètre à l'aide d'une politique de groupe, qui est fixé par défaut à 10 heures. Pour plus d'informations sur ce paramètre, veuillez consulter la [documentation Microsoft](#).
- Le type de chiffrement Kerberos pris en charge par le compte de service AD Connector doit correspondre à chacun des types de chiffrement Kerberos pris en charge par le contrôleur de domaine.

Activation de l'authentification par carte à puce

Pour activer l'authentification par carte à puce WorkSpaces sur votre AD Connector, vous devez d'abord importer vos certificats d'autorité de certification (CA) dans AD Connector. Vous pouvez importer vos certificats CA dans AD Connector à l'aide de AWS Directory Service la console, de l'[API](#) ou de la [CLI](#). Suivez les étapes ci-dessous pour importer vos certificats CA et activer ensuite l'authentification par carte à puce.

Étapes

- [Activation de la délégation contrainte Kerberos pour le compte de service AD Connector](#)
- [Enregistrement du certificat CA dans AD Connector](#)
- [Activation de l'authentification par carte à puce pour les AWS applications et services pris en charge](#)

Activation de la délégation contrainte Kerberos pour le compte de service AD Connector

Pour utiliser l'authentification par carte à puce avec AD Connector, vous devez activer la délégation Kerberos contrainte (KCD) pour le compte service AD Connector vers le service LDAP dans l'annuaire AD autogéré.

La délégation Kerberos contrainte est une fonctionnalité de Windows Server. Cette fonctionnalité permet aux administrateurs de définir et d'appliquer les limites de confiance des applications en limitant la portée dans laquelle les services applicatifs peuvent agir au nom d'un utilisateur. Pour plus d'informations, veuillez consulter la section [Kerberos constrained delegation](#) (français non garanti).

Note

Kerberos Constrained Delegation (KCD) nécessite que la partie nom d'utilisateur du compte de service AD Connector corresponde au AMAccount nom s du même utilisateur. Le AMAccount nom s est limité à 20 caractères. Le AMAccount nom s est un attribut Microsoft Active Directory utilisé comme nom de connexion pour les versions antérieures des clients et serveurs Windows.

1. Utilisez la commande SetSpn pour définir un nom principal du service (SPN) pour le compte de service AD Connector dans l'AD autogéré. Cela active le compte de service pour la configuration de la délégation.

Le SPN peut être n'importe quelle combinaison de service ou de noms, mais ne peut pas être une copie d'un SPN existant. Le -s vérifie la présence de doublons.

```
setspn -s my/spn service_account
```

2. Dans AD Users and Computers (Utilisateurs et ordinateurs AD), ouvrez le menu contextuel (clic droit) et choisissez le compte de service AD Connector, puis Properties (Propriétés).
3. Choisissez l'onglet Delegation (Délégation).
4. Choisissez les options Trust this user for delegation to specified service only (Approuver cet utilisateur pour la délégation au service spécifié uniquement) et Use any authentication protocol (Utiliser n'importe quel protocole d'authentification).
5. Choisissez Add (Ajouter), puis Users or Computers (Utilisateurs ou ordinateurs) pour localiser le contrôleur de domaine.
6. Cliquez sur OK pour afficher une liste des services disponibles utilisés pour la délégation.
7. Choisissez le type de service LDAP et cliquez sur OK.
8. Cliquez à nouveau sur OK pour enregistrer la configuration.
9. Répétez ce processus pour les autres contrôleurs de domaine dans Active Directory. Vous pouvez également automatiser le processus en utilisant PowerShell.

Enregistrement du certificat CA dans AD Connector

Utilisez l'une des méthodes suivantes pour enregistrer un certificat CA pour votre annuaire AD Connector.

Méthode 1 : pour enregistrer votre certificat CA dans AD Connector (AWS Management Console)

1. Dans le volet de navigation de la [AWS Directory Service console](#), sélectionnez Annuaire.
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), choisissez Actions, puis sélectionnez Register certificate (Enregistrer le certificat).
5. Dans la boîte de dialogue Register a certificate (Enregistrer un certificat), sélectionnez Choose file (Choisir un fichier), puis un certificat et cliquez sur Open (Ouvrir). Vous pouvez éventuellement choisir d'effectuer une vérification de révocation pour ce certificat en fournissant

une URL du répondeur OCSP (Online Certificate Status Protocol). Pour plus d'informations sur le protocole OCSP, veuillez consulter [Processus de vérification de la révocation des certificats](#).

6. Choisissez Register certificate (Enregistrer le certificat). Lorsque le statut du certificat passe à Registered (Enregistré), cela signifie que le processus d'enregistrement s'est terminé avec succès.

Méthode 2 : pour enregistrer votre certificat CA dans AD Connector (AWS CLI)

- Exécutez la commande suivante. Pour les données de certificat, pointez vers l'emplacement de votre fichier de certificat de CA. Pour fournir une adresse de répondeur OCSP secondaire, utilisez l'objet ClientCertAuthSettings facultatif.

```
aws ds register-certificate --directory-id your_directory_id --certificate-  
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings  
OCSPUrl=http://your_OCSP_address
```

En cas de succès, la réponse fournit un identifiant de certificat. Vous pouvez également vérifier que votre certificat CA a bien été enregistré en exécutant la commande CLI suivante :

```
aws ds list-certificates --directory-id your_directory_id
```

Si la valeur du statut renvoie Registered, cela signifie que votre certificat a été enregistré avec succès.

Activation de l'authentification par carte à puce pour les AWS applications et services pris en charge

Utilisez l'une des méthodes suivantes pour enregistrer un certificat CA pour votre annuaire AD Connector.

Méthode 1 : pour activer l'authentification par carte à puce dans AD Connector (AWS Management Console)

1. Accédez à la section Smart card authentication (Authentification par carte à puce) sur la page Directory details (Détails de l'annuaire), puis choisissez Enable (Activer). Si cette option n'est pas disponible, vérifiez qu'un certificat valide a bien été enregistré, puis réessayez.
2. Dans la boîte de dialogue Enable smart card authentication (Activer l'authentification par carte à puce), sélectionnez Enable (Activer).

Méthode 2 : pour activer l'authentification par carte à puce dans AD Connector (AWS CLI)

- Exécutez la commande suivante.

```
aws ds enable-client-authentication --directory-id your_directory_id --type SmartCard
```

En cas de succès, AD Connector renvoie une réponse HTTP 200 avec un corps HTTP vide.

Pour plus d'informations sur l'affichage, le désenregistrement ou la désactivation de votre certificat, consultez. [Gestion des paramètres d'authentification par carte à puce](#)

Gestion des paramètres d'authentification par carte à puce

Vous pouvez utiliser deux méthodes différentes pour gérer les paramètres des cartes à puce. Vous pouvez utiliser la AWS Management Console méthode ou la AWS CLI méthode.

Rubriques

- [Afficher les détails du certificat](#)
- [Annuler l'enregistrement d'un certificat](#)
- [Désactiver l'authentification par carte à puce](#)

Afficher les détails du certificat

Utilisez l'une des méthodes suivantes pour voir lorsqu'un certificat est défini pour expirer.

Méthode 1 : pour afficher les détails du certificat dans Directory Service (AWS Management Console)

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
3. Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
4. Dans la section Smart card authentication (Authentification par carte à puce), sous CA certificates (Certificats CA), choisissez l'ID du certificat pour en afficher les détails.

Méthode 2 : pour afficher les détails du certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Annuler l'enregistrement d'un certificat

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'un certificat.

Note

Si un seul certificat est enregistré, vous devez d'abord désactiver l'authentification par carte à puce avant de pouvoir annuler l'enregistrement d'un certificat.

Méthode 1 : pour annuler l'enregistrement d'un certificat dans Directory Service (AWS Management Console)

- Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
- Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
- Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
- Dans la section Smart card authentication (Authentification par carte à puce), sous CA certificates (Certificats CA), sélectionnez le certificat dont vous souhaitez annuler l'enregistrement, cliquez sur Actions, puis sur Deregister certificate (Annuler l'enregistrement du certificat).

Important

Assurez-vous que le certificat dont vous vous apprêtez à annuler l'enregistrement n'est pas actif ou qu'il est actuellement utilisé dans le cadre d'une chaîne de certificats CA pour l'authentification par carte à puce.

- Dans la boîte de dialogue Annuler l'enregistrement d'un certificat d'une autorité de certification, choisissez Annuler l'enregistrement.

Méthode 2 : pour annuler l'enregistrement d'un certificat dans Directory Service (AWS CLI)

- Exécutez la commande suivante. Pour l'ID de certificat, utilisez l'identifiant renvoyé par `register-certificate` ou `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
```

Désactiver l'authentification par carte à puce

Utilisez l'une des méthodes suivantes pour désactiver l'authentification par carte à puce.

Méthode 1 : pour désactiver l'authentification par carte à puce dans Directory Service (AWS Management Console)

- Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
- Choisissez le lien de l'ID correspondant à votre annuaire AD Connector.
- Sur la page Détails de l'annuaire, choisissez l'onglet Mise en réseau et sécurité.
- Dans la section Smart card authentication (Authentification par carte à puce), choisissez Disable (Désactiver).
- Dans la section Disable smart card authentication (Désactiver l'authentification par carte à puce), choisissez Disable (Désactiver).

Méthode 2 : pour désactiver l'authentification par carte à puce dans Directory Service (AWS CLI)

- Exécutez la commande suivante.

```
aws ds disable-client-authentication --directory-id your_directory_id --type SmartCard
```

Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Management Console

Les informations d'identification AD Connector que vous fournissez Directory Service représentent le compte de service utilisé pour accéder à votre annuaire local existant. Vous pouvez modifier

les informations d'identification du compte de service en Directory Service effectuant les étapes suivantes.

 Note

Si cette option AWS IAM Identity Center est activée pour le répertoire, le nom principal du service (SPN) Directory Service doit être transféré du compte de service actuel vers le nouveau compte de service. Si le compte de service actuel n'a pas l'autorisation de supprimer le SPN ou que le nouveau compte de service n'a pas l'autorisation d'ajouter le SPN, vous serez invité à fournir les informations d'identification d'un compte d'annuaire disposant de l'autorisation d'effectuer les deux actions. Ces informations d'identification ne sont pas utilisées pour transférer le SPN et ne sont pas stockées par le service.

Pour mettre à jour les informations d'identification de votre compte de service AD Connector dans Directory Service

1. Dans le volet de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Directories (Annuaire).
2. Choisissez le lien de l'ID correspondant à votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), faites défiler la page vers le bas jusqu'à la section Service account credentials (Informations d'identification du compte de service).
4. Dans la section Informations d'identification du compte de service choisissez Mettre à jour.
5. Dans la boîte de dialogue Update service account credentials (Mettre à jour les informations d'identification du compte de service), tapez le nom d'utilisateur et le mot de passe du compte de service. Saisissez à nouveau le mot de passe pour le confirmer, puis cliquez sur Update (Mettre à jour).

Configurer le AWS CA privée connecteur pour AD

Vous pouvez intégrer votre Active Directory autogéré à AWS Autorité de certification privée l'aide d'AD Connector pour émettre et gérer des certificats pour les utilisateurs, les groupes et les machines associés à votre domaine AD. AWS CA privée Connector for AD fournit une solution entièrement gérée AWS CA privée en remplacement de votre entreprise autogérée CAs sans que vous ayez à déployer, à appliquer des correctifs ou à mettre à jour des agents locaux ou des serveurs proxy.

Vous pouvez configurer cette intégration par le biais de la Directory Service console, de la console AWS CA privée Connector for AD ou en appelant l'[CreateTemplateAPI](#). Pour utiliser la console AWS CA privée Connector for Active Directory, consultez [AWS CA privée Connector for Active Directory](#). Les sections suivantes décrivent comment configurer cette intégration depuis la Directory Service console.

Prérequis

Pour les instructions de configuration, voir [Configurer le connecteur pour AD](#) dans le guide de l'utilisateur du AWS CA privée connecteur pour AD.

Configuration AWS CA privée du connecteur pour AD

Pour créer un connecteur CA privé pour Active Directory

1. Connectez-vous à la Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Dans l'onglet Gestion des AWS applications et dans la section Applications et services, sélectionnez AWS CA privée Connector for AD.
4. Sur la page Créer un certificat d'autorité de certification privée pour Active Directory, suivez les étapes de création de votre connecteur d'autorité de certification privée pour Active Directory.

Pour de plus amples informations, veuillez consulter [Creating a connector](#) (français non garanti).

Afficher votre AWS CA privée connecteur pour AD

Pour afficher les détails du connecteur Private CA

1. Connectez-vous à la Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Dans l'onglet Gestion des AWS applications et dans la section Applications et services, consultez vos connecteurs d'autorité de certification privée et l'autorité de certification privée associée. Les champs suivants s'affichent :
 - a. AWS CA privée ID du connecteur : identifiant unique d'un AWS CA privée connecteur. Sélectionnez-le pour afficher la page de détails.

- b. AWS CA privée objet — Informations concernant le nom distinctif de l'autorité de certification. Sélectionnez-le pour afficher la page de détails.
- c. État — Résultats de la vérification de l'état du AWS CA privée connecteur et AWS CA privée :
 - Actif — Les deux contrôles sont réussis
 - Échec d'une demi-vérification — échec d'une vérification
 - Échec : les deux vérifications échouent

Pour obtenir des informations sur le statut d'échec, passez le pointeur de la souris sur le lien hypertexte pour voir quelle vérification a échoué.

- d. État d'inscription des certificats DC — Vérification de l'état du certificat du contrôleur de domaine :
 - Activé — L'inscription aux certificats est activée
 - Désactivé — L'inscription au certificat est désactivée
- e. Date de création : date de création AWS CA privée du connecteur.

Pour plus d'informations, veuillez consulter [View connector details](#) (français non garanti).

Vérifier l'émission de certificats aux utilisateurs d'AD

Procédez comme suit pour confirmer que des certificats AWS CA privée sont émis pour votre Active Directory autogéré :

- Redémarrez vos contrôleurs de domaine locaux.
- Consultez vos certificats avec Microsoft Management Console. Pour plus d'informations, consultez [Microsoftla documentation](#).

Surveillance de votre annuaire AD Connector

Vous pouvez tirer le meilleur parti de votre AD Connector en découvrant les différents statuts d'AD Connector et ce qu'ils signifient pour votre AD Connector. Vous pouvez également utiliser Amazon Simple Notification Service pour recevoir des notifications concernant le statut de votre AD Connector.

Tâches pour surveiller votre AD Connector :

- [Comprendre le statut de votre annuaire](#)
- [Activation des notifications d'état de l'annuaire AD Connector avec Amazon SNS](#)

Comprendre le statut de votre annuaire

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le [centre AWS Support](#).

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Il s'agit notamment des activités de maintenance opérationnelle normales telles que l'application de correctifs ou la rotation des EC2 instances, le repérage temporaire par

une application sur l'un de vos contrôleurs de domaine ou les modifications que vous avez apportées à votre réseau qui perturbent par inadvertance les communications d'annuaire. Pour plus d'informations, veuillez consulter [Résolution des problèmes liés AWS à Managed Microsoft AD](#), [Résolution des problèmes liés à AD Connector](#), [Résolution des problèmes de Simple AD](#). Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le [centre AWS Support](#).

 Important

Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#).

Inopérable

L'annuaire n'est pas fonctionnel. Tous les points de terminaison de l'annuaire ont signalé des problèmes.

Demandé

La demande de création de votre annuaire est actuellement en attente.

Activation des notifications d'état de l'annuaire AD Connector avec Amazon SNS

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre annuaire passe du statut Active (Actif) au [statut Impaired \(Défaillant\) ou Inoperable \(Inutilisable\)](#). Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article Directory Service en tant qu'éditeur

à une rubrique Amazon SNS. Lorsqu'il Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de l'annuaire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter [Qu'est-ce qu'Amazon SNS ?](#)

Pour activer la messagerie SNS pour votre annuaire

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Créer une notification.
5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

 Note

Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.

Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

 Note

Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique [DirectoryServiceFullAccess](#) gérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre rubrique, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Sélectionnez Create (Créer).

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambda ou, vous pouvez le faire depuis la console Amazon [SNS](#).

Pour supprimer les messages de statut de l'annuaire d'une rubrique

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée. Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console [Amazon SNS](#).

 Note

Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.

Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant la rubrique supprimée, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance de l'annuaire indiquant que la rubrique est introuvable.

Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Accès aux AWS applications et aux services depuis AD Connector

Vous pouvez autoriser votre AD Connector à accéder aux AWS applications et aux services de votre Active Directory connecté. Parmi les AWS applications et services pris en charge, citons :

- Amazon Chime
- Amazon WorkSpaces
- IAM Identity Center
- AWS Management Console

Aucune application tierce ne fonctionne avec AD Connector.

Tâches permettant d'accéder aux AWS applications et aux services depuis AD Connector

- [Politique de compatibilité des applications pour AD Connector](#)
- [Permettre l'accès aux AWS applications et aux services depuis AD Connector](#)

Politique de compatibilité des applications pour AD Connector

Comme alternative à AWS Directory Service pour Microsoft Active Directory ([AWS Microsoft AD géré](#)), AD Connector est un proxy Active Directory réservé aux applications et services AWS créés. Vous configurez le proxy de manière à ce qu'il utilise un domaine Active Directory spécifié. Lorsque l'application doit rechercher un utilisateur ou un groupe dans Active Directory, AD Connector relaie la demande à l'annuaire. De même, lorsqu'un utilisateur se connecte à l'application, AD Connector relaie la demande d'authentification à l'annuaire. Aucune application tierce ne fonctionne avec AD Connector.

Voici une liste des AWS applications et services compatibles :

- Amazon Chime : pour obtenir des instructions détaillées, veuillez consulter la section [Connect to your Active Directory](#) (français non garanti).

- Amazon Connect : pour plus d'informations, veuillez consulter la section [How Amazon Connect works](#) (français non garanti).
- Amazon EC2 pour Windows ou Linux : vous pouvez utiliser la fonctionnalité transparente de jonction de domaines Active Directory d'Amazon EC2 Windows ou Linux pour joindre votre instance à votre Active Directory autogéré (sur site). Une fois jointe, l'instance communique directement avec votre Active Directory et contourne AD Connector. Pour de plus amples informations, veuillez consulter [Comment joindre une EC2 instance Amazon à votre Active Directory](#).
- AWS Management Console — Vous pouvez utiliser AD Connector pour authentifier AWS Management Console les utilisateurs à l'aide de leurs informations d'identification Active Directory sans configurer d'infrastructure SAML. Pour de plus amples informations, veuillez consulter [Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées](#).
- Quick Suite - Pour plus d'informations, voir [Gestion des comptes utilisateurs dans Quick Suite Enterprise Edition](#).
- AWS IAM Identity Center - Pour des instructions détaillées, voir [Connect IAM Identity Center à un Active Directory local](#).
- AWS Transfer Family - Pour obtenir des instructions détaillées, consultez la section [Directory Service Utilisation de Microsoft Active Directory](#).
- AWS Client VPN - Pour des instructions détaillées, consultez [Authentification et autorisation du client](#).
- WorkDocs - Pour obtenir des instructions détaillées, consultez la section [Connexion à votre annuaire local avec AD Connector](#).
- Amazon WorkMail - Pour des instructions détaillées, consultez [Intégrer Amazon WorkMail à un annuaire existant \(configuration standard\)](#).
- WorkSpaces - Pour des instructions détaillées, voir [Lancer un connecteur WorkSpace à l'aide d'AD Connector](#).

 Note

Amazon RDS est compatible avec AWS Managed Microsoft AD uniquement et n'est pas compatible avec AD Connector. Pour plus d'informations, consultez la section Microsoft AD AWS géré de la [Directory Service FAQs](#) page.

Permettre l'accès aux AWS applications et aux services depuis AD Connector

Les utilisateurs peuvent autoriser AD Connector à autoriser AWS des applications et des services, tels qu'Amazon WorkSpaces, à accéder à votre Active Directory. Les AWS applications et services suivants peuvent être activés ou désactivés pour fonctionner avec AD Connector.

AWS application/service	En savoir plus...
Amazon Chime	Pour plus d'informations, consultez la section Connexion à Active Directory .
Amazon Connect	Pour plus d'informations, veuillez consulter le Guide d'administration Amazon Connect .
Amazon WorkDocs	Pour plus d'informations, consultez le guide Getting started with Amazon WorkDocs .
Amazon WorkMail	Pour plus d'informations, consultez la section Création d'une organisation .
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez le guide d'WorkSpaces administration Amazon.
AWS Client VPN	Pour plus d'informations, veuillez consulter le Guide de l'utilisateur AWS Client VPN .
AWS IAM Identity Center	Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS IAM Identity Center .
AWS Management Console	Pour de plus amples informations, veuillez consulter Activation de AWS Management

AWS application/service	En savoir plus...
	Console l'accès avec les informations d'identification Microsoft AD AWS gérées.
AWS Transfer Family	Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS Transfer Family .

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire. Pour trouver les liens vers AWS les applications et les services décrits ci-dessus dans la Directory Service console, effectuez les opérations suivantes.

Pour afficher les applications et les services d'un annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaires.
2. Sur la page Directories (Annuaires), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Consultez la liste dans la section Applications et services AWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant Directory Service, consultez [Autorisation pour AWS les applications et les services utilisant Directory Service](#).

Comment joindre une EC2 instance Amazon à votre Active Directory

AD Connector est une passerelle d'annuaire grâce à laquelle vous pouvez rediriger les demandes d'annuaire vers votre Microsoft Active Directory local sans mettre en cache aucune information dans le cloud. Voici plus d'informations sur la façon dont vous pouvez associer un Amazon EC2 à un domaine Active Directory :

- Vous pouvez facilement joindre une EC2 instance Amazon à votre domaine Active Directory lorsque l'instance est lancée. Pour plus d'informations sur l'association d'une instance EC2

Windows à un Microsoft AD AWS géré, consultez [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#).

- Si vous devez joindre manuellement une EC2 instance à votre domaine Active Directory, vous devez lancer l'instance dans le groupe de sécurité ou le sous-réseau approprié Région AWS , puis joindre l'instance au domaine Active Directory.
- Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela nécessite qu'une passerelle Internet soit attachée à votre Amazon VPC et que l'instance possède une adresse IP publique. Pour obtenir plus d'informations sur la connexion à Internet à l'aide d'une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti).

Note

Une fois que vous avez joint une instance à votre Active Directory autogéré (sur site), l'instance communique directement avec votre Active Directory et contourne AD Connector.

Quotas AD Connector

Voici les quotas par défaut pour AD Connector. Sauf indication contraire, chaque quota est spécifique à une région.

Quotas AD Connector

Ressource	Quota par défaut
Annuaire AD Connector	10
Nombre maximal de certificats d'autorité de certification enregistrés par annuaire	5

Résolution des problèmes liés à AD Connector

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la création ou de l'utilisation de votre AD Connector.

Rubriques

- [Problèmes liés à la création](#)
- [Problèmes de connectivité](#)
- [Problèmes d'authentification](#)
- [Problèmes de maintenance](#)
- [Je ne parviens pas à supprimer mon AD Connector](#)
- [Outils généraux pour enquêter sur les émetteurs d'AD Connector](#)

Problèmes liés à la création

Les problèmes de création suivants sont courants pour AD Connector

- [L'erreur « AZ Constrained » s'affiche lorsque je crée un annuaire](#)
- [Je reçois le message d'erreur « Problèmes de connectivité détectés » lorsque j'essaie de créer un AD Connector](#)

L'erreur « AZ Constrained » s'affiche lorsque je crée un annuaire

Certains AWS comptes créés avant 2012 peuvent avoir accès aux zones de disponibilité des régions de l'est des États-Unis (Virginie du Nord), de l'ouest des États-Unis (Californie du Nord) ou de l'Asie-Pacifique (Tokyo) qui ne prennent pas en charge les Directory Service annuaires. Si vous recevez une telle erreur lors de la création d'un Active Directory, choisissez un sous-réseau dans une autre zone de disponibilité et réessayez de créer le répertoire.

Je reçois le message d'erreur « Problèmes de connectivité détectés » lorsque j'essaie de créer un AD Connector

Si vous recevez le message d'erreur « Problème de connectivité détecté » lorsque vous essayez de créer un AD Connector, cela peut être dû à la disponibilité du port ou à la complexité du mot de passe AD Connector. Vous pouvez tester la connexion de votre connecteur AD pour vérifier si les ports suivants sont disponibles :

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Pour tester votre connexion, consultez [Test de votre connecteur AD Connector](#). Le test de connexion doit être effectué sur l'instance jointe aux deux sous-réseaux auxquels les adresses IP du connecteur AD sont associées.

Si le test de connexion est réussi et que l'instance rejoint le domaine, vérifiez le mot de passe de votre connecteur AD. AD Connector doit répondre aux exigences AWS de complexité des mots de passe. Pour plus d'informations, consultez la section Compte de service dans [Conditions préalables requises pour AD Connector](#).

Si votre AD Connector ne répond pas à ces exigences, recréez-le avec un mot de passe conforme à ces exigences.

Je reçois le message « Une erreur de service interne s'est produite lors de la connexion à l'annuaire. Veuillez réessayer l'opération. » erreur lors de la création d'un AD Connector

Cette erreur se produit généralement lorsque l'AD Connector ne parvient pas à créer et ne parvient pas à se connecter à un contrôleur de domaine valide pour votre domaine Active Directory autogéré.

 Note

[La meilleure pratique](#) est que si des sites Active Directory sont définis sur votre réseau autogéré, vous devez vous assurer que les points suivants sont respectés :

- Les sous-réseaux VPC sur lesquels réside votre AD Connector sont définis dans un site Active Directory.
- Il n'existe aucun conflit entre vos sous-réseaux VPC et les sous-réseaux de vos autres sites.

AD Connector utilise le site Active Directory dont les plages d'adresses IP de sous-réseau sont proches de celles du VPC qui contient l'AD Connector pour découvrir vos contrôleurs de domaine AD. Si vous avez un site dont les sous-réseaux ont les mêmes plages d'adresses IP que celles de votre VPC, AD Connector découvrira les contrôleurs de domaine de ce site. Le contrôleur de domaine n'est peut-être pas physiquement proche de la région dans laquelle réside votre AD Connector.

- Incohérences dans les enregistrements DNS SRV (ces enregistrements utilisent la syntaxe suivante : `_ldap._tcp.<DnsDomainName>` et `_kerberos._tcp.<DnsDomainName>`) créées

dans le domaine Active Directory géré par le client. Cela peut se produire lorsque AD Connector ne parvient pas à trouver un contrôleur de domaine valide et à s'y connecter sur la base de ces enregistrements SRV.

- Problèmes de réseau entre AD Connector et AD géré par le client, tels que les dispositifs de pare-feu.

Vous pouvez utiliser la [capture de paquets réseau](#) sur vos contrôleurs de domaine, vos serveurs DNS et les journaux de flux VPC des interfaces réseau d'annuaire pour étudier ce problème. Contactez-nous [AWS Support](#) pour obtenir de l'aide supplémentaire.

Problèmes de connectivité

Les problèmes de connectivité courants liés à AD Connector sont les suivants :

- [L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site](#)
- [L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site](#)
- [L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site](#)

L'erreur « Connectivity issues detected » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Vous recevez un message d'erreur similaire au suivant lorsque vous vous connectez à votre annuaire local : Problèmes de connectivité détectés : LDAP non disponible (port TCP 389) pour IP : *<IP address>* Kerberos/authentication indisponible (port TCP 88) pour IP : *<IP address>* assurez-vous que les ports répertoriés sont disponibles et recommencez l'opération.

AD Connector doit être capable de communiquer avec vos contrôleurs de domaine sur site via les protocoles TCP et UDP sur les ports suivants. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ces ports. Pour de plus amples informations, veuillez consulter [Conditions préalables requises pour AD Connector](#).

- 88 (Kerberos)
- 389 (LDAP)

Vous aurez peut-être besoin de TCP/UDP ports supplémentaires en fonction de vos besoins. Consultez la liste suivante pour certains de ces ports. Pour plus d'informations sur les ports utilisés

par Active Directory, consultez la section [Comment configurer un pare-feu pour les domaines et les approbations Active Directory](#) dans Microsoft la documentation.

- 135 (mappeur de points de terminaison RPC)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

L'erreur « DNS unavailable » s'affiche lorsque j'essaie de me connecter à mon annuaire sur site

Un message d'erreur similaire à ce qui suit s'affiche lors de la connexion à votre annuaire sur site :

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector doit être capable de communiquer avec vos serveurs DNS sur site via les protocoles TCP et UDP sur le port 53. Vérifiez que vos groupes de sécurité et pare-feu sur site autorisent la communication TCP et UDP sur ce port. Pour de plus amples informations, veuillez consulter [Conditions préalables requises pour AD Connector](#).

L'erreur « SRV record » s'affiche lorsque je tente de me connecter à mon annuaire sur site

Un message d'erreur similaire à un ou plusieurs des messages suivants s'affiche lors de la connexion à votre annuaire sur site :

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos  
does not exist for IP: <DNS IP address>
```

AD Connector doit obtenir les enregistrements SRV `_ldap._tcp.<DnsDomainName>` et `_kerberos._tcp.<DnsDomainName>` lors de la connexion à votre annuaire. Cette erreur s'affiche si le service ne peut pas obtenir ces enregistrements auprès des serveurs DNS que vous avez spécifiés lors de la connexion à votre annuaire. Pour plus d'informations sur ces enregistrements SRV, veuillez consulter [SRV record requirements](#).

Problèmes d'authentification

Voici quelques problèmes d'authentification courants liés à AD Connector :

- [Je reçois un message d'erreur « Échec de la validation du certificat » lorsque j'essaie de me connecter à l' Amazon WorkSpaces aide d'une carte à puce](#)
- [L'erreur « Invalid Credentials » s'affiche lorsque le compte de service utilisé par AD Connector tente une authentification](#)
- [Je reçois un message d'erreur « Impossible de m'authentifier » lorsque j'utilise AWS des applications pour rechercher des utilisateurs ou des groupes](#)
- [Je reçois un message d'erreur concernant mes informations d'identification d'annuaire lorsque j'essaie de mettre à jour le compte du service AD Connector](#)
- [Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon annuaire](#)

Je reçois un message d'erreur « Échec de la validation du certificat » lorsque j'essaie de me connecter à l' Amazon WorkSpaces aide d'une carte à puce

Vous recevez un message d'erreur semblable au suivant lorsque vous essayez de vous connecter à votre compte à l' WorkSpaces aide d'une carte à puce : ERREUR : échec de la validation du certificat. Réessayez en redémarrant votre navigateur ou votre application et assurez-vous de sélectionner le bon certificat. L'erreur se produit si le certificat de la carte à puce n'est pas correctement stocké sur le client qui utilise les certificats. Pour plus d'informations sur les exigences relatives à l'AD Connector et aux cartes à puce, consultez [Prérequis](#).

Utilisez les procédures suivantes pour résoudre les problèmes liés à la capacité de la carte à puce à stocker des certificats dans le magasin de certificats de l'utilisateur :

1. Sur l'appareil qui rencontre des difficultés pour accéder aux certificats, accédez au Microsoft Management Console (MMC).

Important

Avant de poursuivre, créez une copie du certificat de la carte à puce.

2. Accédez au magasin de certificats dans la MMC. Supprimez le certificat de carte à puce de l'utilisateur du magasin de certificats. Pour plus d'informations sur l'affichage du magasin de

certificats dans la MMC, voir [Comment : afficher les certificats avec le composant logiciel enfichable MMC dans la](#) documentation. Microsoft

3. Retirez la carte à puce.
4. Réinsérez la carte à puce afin qu'elle puisse remplir à nouveau le certificat de carte à puce dans le magasin de certificats de l'utilisateur.

 Warning

Si la carte à puce ne recharge pas le certificat dans le magasin de l'utilisateur, elle ne peut pas être utilisée pour l'authentification par carte à WorkSpaces puce.

Le compte de service du connecteur AD doit comporter les éléments suivants :

- my/spnajouté au nom du principe de service
- Délégué pour le service LDAP

Une fois le certificat rechargé sur la carte à puce, le contrôleur de domaine sur site doit être vérifié pour déterminer s'il est bloqué lors du mappage du nom d'utilisateur principal (UPN) pour le nom alternatif du sujet. Pour plus d'informations sur cette modification, consultez [Comment désactiver le nom alternatif du sujet pour le mappage UPN](#) dans Microsoft la documentation.

Pour vérifier la clé de registre de votre contrôleur de domaine, procédez comme suit :

- Dans l'éditeur de registre, accédez à la clé de ruche suivante

HKEY_LOCAL_MACHINE \ SYSTÈME \ \ Services \ Kdc \ CurrentControlSet
UseSubjectAltName

- Vérifiez la valeur de UseSubjectAltName :
 - i. Si la valeur est définie sur 0, le mappage du nom alternatif du sujet est désactivé et vous devez mapper explicitement un certificat donné à un seul utilisateur. Si un certificat est mappé à plusieurs utilisateurs et que cette valeur est égale à 0, la connexion avec ce certificat échouera.
 - ii. Si la valeur n'est pas définie ou définie sur 1, vous devez mapper explicitement un certificat donné à un seul utilisateur ou utiliser le champ Nom alternatif du sujet pour vous connecter.

- A. Si le champ Nom alternatif du sujet existe sur le certificat, il sera priorisé.
- B. Si le champ Nom alternatif du sujet n'existe pas sur le certificat et que le certificat est explicitement mappé à plusieurs utilisateurs, la connexion avec ce certificat échouera.

 Note

Si la clé de registre est définie sur les contrôleurs de domaine locaux, l'AD Connector ne sera pas en mesure de localiser les utilisateurs dans Active Directory et le message d'erreur ci-dessus s'affichera.

Les certificats de l'autorité de certification (CA) doivent être téléchargés sur le certificat de carte à puce AD Connector. Le certificat doit contenir des informations OCSP. La liste suivante répertorie les exigences supplémentaires pour l'autorité de certification :

- Le certificat doit se trouver dans l'autorité racine sécurisée du contrôleur de domaine, du serveur de l'autorité de certification et du WorkSpaces.
- Les certificats hors ligne et Root CA ne contiendront pas les informations OCSP. Ces certificats contiennent des informations relatives à leur révocation.
- Si vous utilisez un certificat CA tiers pour l'authentification par carte à puce, le certificat CA et les certificats intermédiaires doivent être publiés dans le NTAAuth magasin Active Directory. Ils doivent être installés dans l'autorité racine approuvée pour tous les contrôleurs de domaine, serveurs d'autorités de certification et WorkSpaces.
- Vous pouvez utiliser la commande suivante pour publier des certificats dans le NTAAuth magasin Active Directory :

```
certutil -dspublish -f Third_Party_CA.cer NTAAuthCA
```

Pour plus d'informations sur la publication de certificats dans le NTAAuth magasin, consultez [Importer le certificat CA émetteur dans le NTAAuth magasin Enterprise](#) dans le guide d'installation d'Access Amazon WorkSpaces with Common Access Cards.

Vous pouvez vérifier si le certificat utilisateur ou les certificats de chaîne CA sont vérifiés par OCSP en suivant cette procédure :

1. Exportez le certificat de carte à puce vers un emplacement sur la machine locale, tel que le lecteur C :.
2. Ouvrez une invite de ligne de commande et naviguez jusqu'à l'emplacement où le certificat de carte à puce exporté est stocké.
3. Entrez la commande suivante :

```
certutil -URL Certificate_name.cer
```

4. Une fenêtre contextuelle devrait apparaître à la suite de la commande. Sélectionnez l'option OCSP dans le coin droit, puis sélectionnez Récupérer. Le statut devrait revenir tel que vérifié.

Pour plus d'informations sur la commande certutil, consultez [certutil](#) dans la documentation Microsoft

L'erreur « Invalid Credentials » s'affiche lorsque le compte de service utilisé par AD Connector tente une authentification

Cela peut se produire si le disque dur de votre contrôleur de domaine manque d'espace libre. Assurez-vous que les disques durs de votre contrôleur de domaine ne sont pas pleins.

Je reçois le message « Une erreur s'est produite » ou « Une erreur inattendue » lorsque j'essaie de mettre à jour le compte de service AD Connector

Les erreurs ou symptômes suivants se produisent lors de la recherche d'utilisateurs dans des applications AWS d'entreprise telles qu'[Amazon WorkSpaces Console Launch Wizard](#) :

- Une erreur s'est produite. Si le problème persiste, contactez l' AWS Support équipe sur les forums communautaires et via le Support AWS Premium.
- Une erreur s'est produite. Votre répertoire a besoin d'une mise à jour des informations d'identification. Veuillez mettre à jour les informations d'identification du répertoire.

Si vous essayez de mettre à jour les informations d'identification de votre compte de service AD Connector dans AD Connector, les messages d'erreur suivants peuvent s'afficher :

- Erreur inattendue. Une erreur inattendue s'est produite.

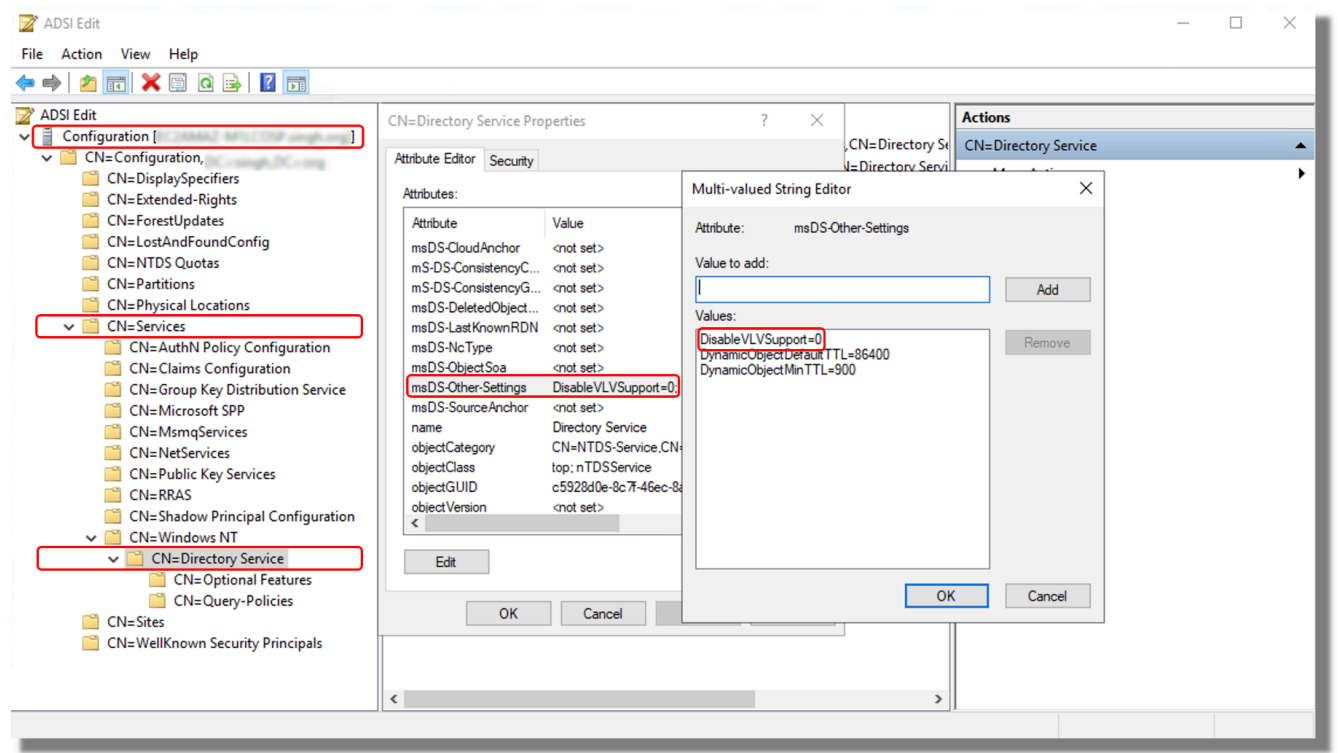
- Une erreur s'est produite. Une erreur s'est produite dans la account/password combinaison de services. Veuillez réessayer.

Le compte de service de l'annuaire AD Connector réside dans l'Active Directory géré par le client. Le compte est utilisé comme identité pour effectuer des requêtes et des opérations sur le domaine Active Directory géré par le client via l'AD Connector pour le compte d' AWS Enterprise Applications. AD Connector utilise Kerberos et LDAP pour effectuer ces opérations.

La liste suivante explique la signification de ces messages d'erreur :

- Il y a peut-être un problème avec la synchronisation de l'heure et Kerberos. AD Connector envoie des demandes d'authentification Kerberos à Active Directory. Ces demandes sont urgentes et, si elles sont retardées, elles échoueront. Assurez-vous qu'il n'y a aucun problème de synchronisation horaire entre les contrôleurs de domaine gérés par le client. Pour résoudre ce problème, consultez la section [Recommandation - Configurer le PDC racine avec une source temporelle officielle et éviter un décalage temporel généralisé dans la documentation](#). Microsoft Pour plus d'informations sur le service horaire et la synchronisation, consultez les rubriques suivantes :
 - [Comment fonctionne le Windows Time Service](#)
 - [Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur](#)
 - [WindowsOutils et paramètres du service de gestion du temps](#)
- Un périphérique réseau intermédiaire, avec une restriction de [MTU](#) réseau, telle que des configurations matérielles de pare-feu ou de VPN, entre l'AD Connector et les contrôleurs de domaine gérés par le client, peut provoquer cette erreur en raison de la [fragmentation du réseau](#).
 - Pour vérifier la restriction MTU, vous pouvez effectuer un [test Ping](#) entre le contrôleur de domaine géré par le client et une EC2 instance Amazon lancée dans l'un des sous-réseaux de votre annuaire connecté via AD Connector. La taille du cadre ne doit pas être supérieure à la taille par défaut de 1 500 octets.
 - Le test ping vous aidera à déterminer si la taille des trames est supérieure à 1 500 octets (également appelées trames Jumbo) et si elles peuvent atteindre le VPC et le sous-réseau AD Connector sans qu'il soit nécessaire de les fragmenter. Vérifiez auprès de votre équipe réseau que les trames Jumbo sont autorisées sur les périphériques réseau intermédiaires.
- Vous pouvez rencontrer ce problème si le protocole [LDAPS côté client](#) est activé sur AD Connector et que les certificats ont expiré. Assurez-vous que le certificat côté serveur et le certificat CA sont valides, qu'ils n'ont pas expiré et qu'ils répondent aux exigences de la [LDAPsdocumentation](#).

- Si le [support d'affichage de liste virtuelle](#) est désactivé dans le domaine Active Directory géré par le client, AWS les applications ne seront pas en mesure de rechercher des utilisateurs car AD Connector utilise la recherche VLV dans les requêtes LDAP. Le support d'affichage de liste virtuelle est désactivé lorsque la valeur Disable VLVSupport est définie sur une valeur différente de zéro. Assurez-vous que le [support VLV \(Virtual List View\)](#) est activé dans Active Directory en procédant comme suit :
 1. Connectez-vous au contrôleur de domaine en tant que propriétaire du rôle principal du schéma à l'aide d'un compte doté des informations d'identification d'administrateur du schéma.
 2. Sélectionnez Démarrer, puis Exécuter, puis entrez **Adsiedit.msc**.
 3. Dans l'outil ADSI Edit, connectez-vous à la partition de configuration et développez le nœud Configuration [DomainController].
 4. Développez le conteneur CN=Configuration, DomainName DC=.
 5. Développez l'objet CN=Services.
 6. Développez l'objet CN=Windows NT.
 7. Sélectionnez l'objet CN=Directory Service. Sélectionnez Propriétés.
 8. Dans la liste Attributs, sélectionnez MSDS-Other-Settings. Tâche de sélection Modifier.
 9. Dans la liste des valeurs, sélectionnez une instance de Disable VLVSupport =x où x n'est pas égal à 0, puis sélectionnez Supprimer.
 10. Après le retrait, entrez **DisableVLVSupport=0**. Sélectionnez Ajouter.
 11. Sélectionnez OK. Vous pouvez fermer l'outil ADSI Edit. L'image suivante montre la boîte de dialogue Éditeur de chaînes à valeurs multiples dans la fenêtre d'édition ADSI :



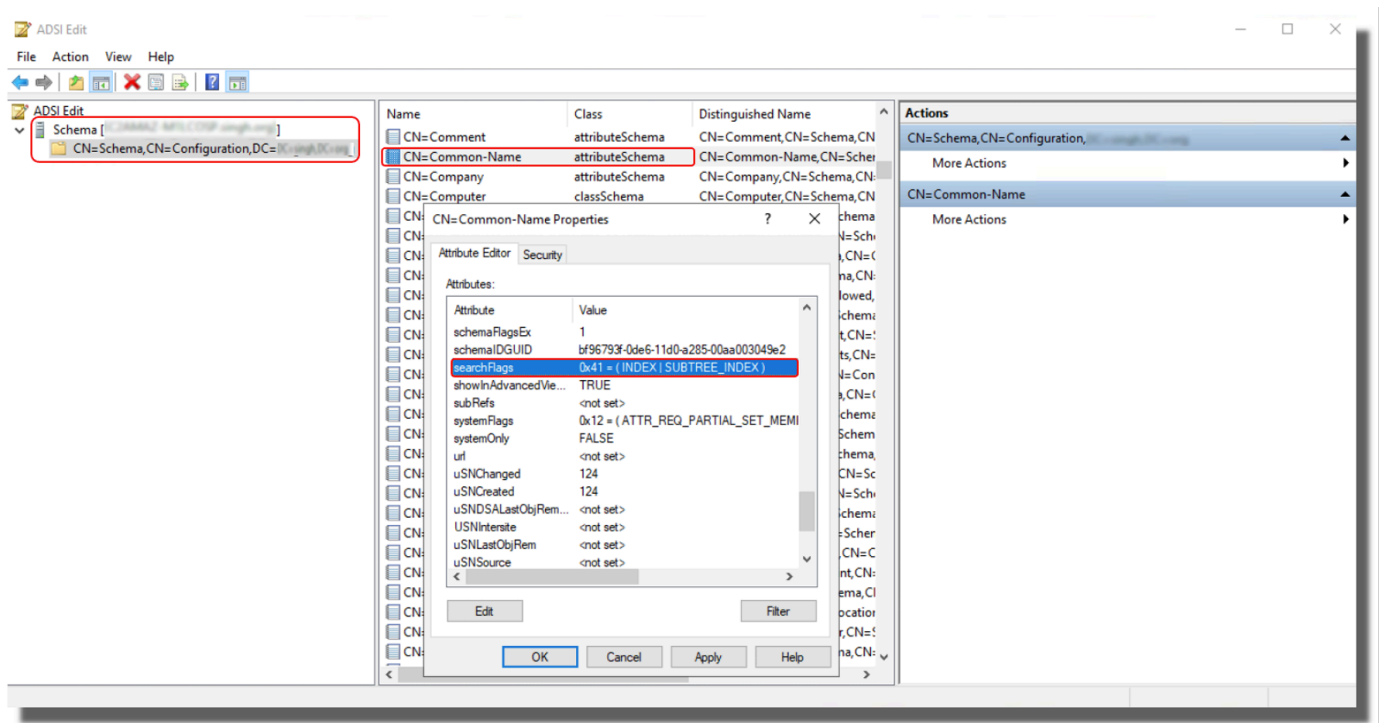
Note

Dans une infrastructure Active Directory de plus de 100 000 utilisateurs, il est possible que vous ne puissiez rechercher que des utilisateurs spécifiques. Cependant, si vous essayez de répertorier tous les utilisateurs (par exemple, Show All Users in WorkSpaces Launch Wizard) en même temps, la même erreur peut se produire même si le support VLV est activé. AD Connector nécessite que les résultats soient triés pour l'attribut « CN » à l'aide de l'index des sous-arbres. L'index de sous-arborescence est le type d'index qui prépare les contrôleurs de domaine à effectuer une opération de recherche LDAP (Virtual List View) qui permet à AD Connector d'effectuer une recherche triée. Cet index améliore la recherche VLV et empêche l'utilisation de la table de base de données temporaire appelée [MaxTempTableSize](#). La taille de cette table peut varier, mais par défaut, le nombre maximum d'entrées est de 10 000 (MaxTempTableSize paramètre de la politique de requête par défaut). L'augmentation de MaxTempTableSize est moins efficace que l'utilisation de l'indexation des sous-arbres. Pour éviter ces erreurs dans les environnements Active Directory de grande taille, il est conseillé d'utiliser l'indexation par sous-arborescence.

Vous pouvez activer l'index Subtree en modifiant l'attribut [searchflags](#) sur la définition de l'attribut, dans le schéma Active Directory, avec une valeur de 65 (0x41), en suivant ADSEdit les étapes suivantes :

1. Connectez-vous au contrôleur de domaine en tant que propriétaire du rôle principal du schéma à l'aide d'un compte doté des informations d'identification d'administrateur du schéma.
2. Sélectionnez Démarrer et exécuter, puis entrez **Adsiedit.msc**.
3. Dans l'outil ADSI Edit, connectez-vous à Schema Partition.
4. Développez le conteneur CN=Schema, CN=Configuration, DC=. DomainName
5. Localisez l'attribut « Common-Name », cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
6. Localisez l'attribut SearchFlags et remplacez sa valeur par « **65 (0x41)** pour activer l' SubTree indexation avec l'index normal ».

L'image suivante montre la boîte de dialogue des propriétés CN=common-name dans la fenêtre d'édition ADSI :



7. Sélectionnez OK. Vous pouvez fermer l'outil ADSI Edit.
8. Pour la confirmation, vous devriez être en mesure de voir un ID d'événement 1137 (Source : Active Directory_DomainServices), qui indique que l'AD a créé avec succès le nouvel index pour l'attribut spécifié.

Pour plus d'informations, consultez [Microsoftla documentation](#).

Je reçois un message d'erreur « Impossible de m'authentifier » lorsque j'utilise AWS des applications pour rechercher des utilisateurs ou des groupes

Vous pouvez rencontrer des erreurs lorsque vous recherchez des utilisateurs ou lorsque vous vous connectez à AWS des applications, telles que WorkSpaces Quick Suite, même lorsque le statut AD Connector était actif. Si le mot de passe du compte de service AD Connector a été modifié ou a expiré, AD Connector ne peut plus interroger le domaine Active Directory. Contactez votre administrateur AD et vérifiez les points suivants :

- Vérifiez que le mot de passe du compte de service AD Connector n'a pas expiré
- Cette case est cochée sur le compte de service AD Connector. L'option L'utilisateur doit changer de mot de passe à la prochaine connexion n'est pas activée.
- Vérifiez que le compte de service AD Connector n'est pas verrouillé.
- Si vous ne savez pas si le mot de passe a expiré ou a été modifié, vous pouvez réinitialiser le mot de passe du compte de service et également [mettre à jour](#) le même mot de passe dans AD Connector.

Je reçois un message d'erreur concernant mes informations d'identification d'annuaire lorsque j'essaie de mettre à jour le compte du service AD Connector

Vous recevez un message d'erreur similaire à l'un ou plusieurs des suivants lorsque vous essayez de mettre à jour le compte de service AD Connector :

Message : Une erreur s'est produite Votre répertoire a besoin d'une mise à jour des informations d'identification. Veuillez mettre à jour les informations d'identification du répertoire. Une erreur s'est produite Votre répertoire a besoin d'une mise à jour des informations d'identification. Veuillez mettre à jour les informations d'identification de l'annuaire en suivant le message Mettre à jour les informations d'identification de votre compte de service AD Connector : Une erreur s'est produite Votre demande pose problème. Veuillez consulter les informations suivantes. Une erreur s'est produite dans la combinaison compte de service/mot de passe

Il y a peut-être un problème avec la synchronisation de l'heure et Kerberos. AD Connector envoie des demandes d'authentification Kerberos à Active Directory. Ces demandes sont urgentes et, si elles sont retardées, elles échoueront. Pour résoudre ce problème, consultez la section [Recommandation - Configurer le PDC racine avec une source temporelle officielle et éviter un décalage temporel](#)

[généralisé dans la documentation](#). Microsoft Pour plus d'informations sur le service horaire et la synchronisation, voir ci-dessous :

- [Comment fonctionne le Windows Time Service](#)
- [Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur](#)
- [WindowsOutils et paramètres du service de gestion du temps](#)

Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon annuaire

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, mais il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section [Préauthentification activée](#) Microsoft TechNet.

Problèmes de maintenance

Les problèmes de maintenance courants liés à AD Connector sont les suivants :

- Mon annuaire est bloqué à l'état « Demandé »
- La jointure de domaine fluide pour les EC2 instances Amazon a cessé de fonctionner

Mon annuaire est bloqué à l'état « Demandé »

Si vous avez un annuaire qui se trouve à l'état « Demandé » depuis plus de cinq minutes, essayez de supprimer l'annuaire et de le recréer. Si le problème persiste, contactez [AWS Support](#).

La jointure de domaine fluide pour les EC2 instances Amazon a cessé de fonctionner

Si la jointure fluide des domaines pour les EC2 instances fonctionnait puis s'arrêtait alors que l'AD Connector était actif, les informations d'identification de votre compte de service AD Connector ont peut-être expiré. Les informations d'identification ayant expiré peuvent empêcher AD Connector de créer des objets ordinateur dans votre Active Directory.

Pour résoudre ce problème, mettez à jour le mot de passe du compte de service dans l'ordre suivant afin que les mots de passe soient identiques :

1. Mettez à jour le mot de passe du compte de service dans votre Active Directory.

2. Mettez à jour le mot de passe du compte de service dans votre AD Connector dans Directory Service. Pour de plus amples informations, veuillez consulter [Mettre à jour les informations d'identification de votre compte de service AD Connector dans AWS Management Console](#).

Important

La mise à jour du mot de passe uniquement dans Directory Service n'entraîne pas le changement de mot de passe dans votre Active Directory local existant. Il est donc important de le faire dans l'ordre indiqué dans la procédure précédente.

Je ne parviens pas à supprimer mon AD Connector

Si votre AD Connector passe à un statut inutilisable, vous n'avez plus accès à vos contrôleurs de domaine. Nous bloquons la suppression d'un AD Connector lorsque des applications y sont encore liées, car l'une de ces applications utilise peut-être encore l'annuaire. Pour obtenir la liste des applications que vous devez désactiver pour supprimer votre AD Connector, consultez [Supprimer votre AD Connector](#). Si vous ne parvenez toujours pas à supprimer votre AD Connector, vous pouvez demander de l'aide via [AWS Support](#).

Outils généraux pour enquêter sur les émetteurs d'AD Connector

Les outils suivants peuvent être utilisés pour résoudre divers problèmes liés à l'AD Connector liés à la création, à l'authentification et à la connectivité :

DirectoryServicePortTest outil

L'outil de [DirectoryServicePortTest](#) peut être utile pour résoudre les problèmes de connectivité entre AD Connector et les serveurs Active Directory ou DNS gérés par le client. Pour plus d'informations sur l'utilisation de l'outil, consultez [Test de votre connecteur AD Connector](#).

Outil de capture de paquets

Vous pouvez utiliser l'utilitaire de capture de Windows packages intégré ([netsh](#)) pour étudier et résoudre un problème potentiel de communication réseau ou Active Directory (LDAP et Kerberos). Pour plus d'informations, veuillez consulter [Capture a Network Trace without installing anything](#) (français non garanti).

Journaux de flux VPC

Pour mieux comprendre quelles demandes sont reçues et envoyées depuis AD Connector, vous pouvez configurer les [journaux de flux VPC pour les interfaces](#) réseau de l'annuaire. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation Directory Service par la description :AWS created network interface for directory *your-directory-id*.

Un cas d'utilisation simple est celui de la création d'un connecteur AD Connector avec un domaine Active Directory géré par le client avec un grand nombre de contrôleurs de domaine. Vous pouvez utiliser les journaux de flux VPC et filtrer par le port Kerberos (88) pour savoir quels contrôleurs de domaine de l'Active Directory géré par le client sont contactés à des fins d'authentification.

Simple AD

Simple AD est un annuaire géré et autonome alimenté par un serveur compatible Active Directory avec Samba 4. Il est disponible en deux formats.

- Small : prend en charge 500 utilisateurs maximum (environ 2 000 objets parmi lesquels des utilisateurs, des groupes et des ordinateurs).
- Large : prend en charge 5 000 utilisateurs maximum (environ 20 000 objets parmi lesquels des utilisateurs, des groupes et des ordinateurs).

Simple AD fournit un sous-ensemble des fonctionnalités proposées par AWS Managed Microsoft AD, notamment la possibilité de gérer les comptes utilisateurs et les appartenances à des groupes, de créer et d'appliquer des politiques de groupe, de se connecter en toute sécurité aux EC2 instances Amazon et de fournir une authentification unique (SSO) basée sur Kerberos. Notez toutefois que Simple AD ne prend pas en charge les fonctionnalités telles que l'authentification multifactorielle (MFA), les relations de confiance avec d'autres domaines, le centre d'administration Active Directory, le support PowerShell, la corbeille Active Directory, les comptes de services gérés par des groupes et les extensions de schéma pour les applications POSIX et Microsoft.

Simple AD offre de nombreux avantages :

- Simple AD facilite la [gestion des EC2 instances Amazon exécutant Linux et Windows](#) et le déploiement d'applications Windows dans le AWS cloud.
- Un grand nombre des applications et outils utilisés aujourd'hui et qui requièrent la prise en charge de Microsoft Active Directory peuvent être utilisés avec Simple AD.
- Les comptes utilisateur dans Simple AD permettent d'accéder à AWS des applications telles que WorkSpaces WorkDocs, ou Amazon WorkMail.
- Vous pouvez gérer les AWS ressources via un accès basé sur les rôles IAM au AWS Management Console
- Des instantanés automatisés quotidiens permettent la point-in-time restauration.

Simple AD ne prend en charge aucun des éléments suivants :

- WorkSpaces Applications Amazon
- Amazon Chime

- Amazon FSx
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- Relations d'approbation avec d'autres domaines
- Centre d'administration Active Directory
- PowerShell
- Corbeille Active Directory
- Comptes de service gérés de groupe
- Extensions de schéma pour les applications POSIX et Microsoft

Poursuivez la lecture des rubriques de cette section pour savoir comment créer votre propre Simple AD.

Rubriques

- [Mise en route avec Simple AD](#)
- [Bonnes pratiques pour Simple AD](#)
- [Maintenance de votre annuaire Simple AD](#)
- [Sécurisez votre annuaire Simple AD](#)
- [Surveillance de votre annuaire Simple AD](#)
- [Accès aux AWS applications et aux services depuis votre Simple AD](#)
- [Comment associer une EC2 instance Amazon à votre Simple AD](#)
- [Gestion des utilisateurs et des groupes dans Simple AD](#)
- [Quotas Simple AD](#)
- [Résolution des problèmes de Simple AD](#)

Mise en route avec Simple AD

Simple AD crée un annuaire entièrement géré basé sur Samba dans le AWS cloud. Lorsque vous créez un annuaire avec Simple AD, il Directory Service crée deux contrôleurs de domaine et deux

serveurs DNS en votre nom. Les contrôleurs de domaine sont créés dans différents sous-réseaux d'un Amazon VPC. Cette redondance permet de garantir que votre répertoire reste accessible même en cas de panne.

Rubriques

- [Prérequis pour Simple AD](#)
- [Créez votre Simple AD](#)
- [Qu'est-ce qui est créé avec votre Simple AD](#)

Prérequis pour Simple AD

Pour créer un répertoire Active Directory Simple AD, vous avez besoin d'un Amazon VPC avec les éléments suivants :

- Le VPC doit avoir la location matérielle par défaut.

Vous pouvez l'utiliser IPv6 pour votre VPC. Pour plus d'informations, consultez la section relative à [la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

- Au moins deux sous-réseaux situés dans deux zones de disponibilité différentes doivent être du même type de réseau. Les sous-réseaux doivent se trouver dans la même plage de routage interdomaine sans classe (CIDR). Si vous souhaitez étendre ou redimensionner le VPC pour votre annuaire, assurez-vous de sélectionner les deux sous-réseaux de contrôleur de domaine pour la plage d'adresses CIDR de VPC étendu. Lorsque vous créez un Simple AD, vous Directory Service créez deux contrôleurs de domaine et deux serveurs DNS en votre nom.
 - Pour plus d'informations sur la plage d'adresses CIDR, consultez la section [Adressage IP pour vos sous-réseaux VPCs et sous-réseaux](#) dans le guide de l'utilisateur Amazon VPC.
- Si vous avez besoin du support LDAPS avec Simple AD, nous vous recommandons de le configurer à l'aide d'un Network Load Balancer connecté au port 389. Ce modèle vous permet d'utiliser un certificat fort pour la connexion LDAPS, de simplifier l'accès à LDAPS par le biais d'une seule adresse IP NLB et de définir un basculement automatique avec NLB. Simple AD ne prend pas en charge l'utilisation de certificats auto-signés sur le port 636. Pour plus d'informations sur la configuration de LDAPS avec Simple AD, reportez-vous à la section [How to Configure an LDAPS Endpoint for Simple AD \(Comment configurer un point de terminaison LDAPS pour Simple AD\)](#) dans le blog sur la sécuritéAWS .
- Les types de chiffrement suivants doivent être activés dans l'annuaire :
 - RC4_HMAC_ MD5

- AES128_HMAC_SHA1
- AES256_HMAC_SHA1
- Futurs types de chiffrement

 Note

Si vous désactivez ces types de chiffrement, cela risque d'engendrer des problèmes de communication avec les outils d'administration de serveur distant (RSAT) et de nuire à la disponibilité ou à votre annuaire.

- Pour de plus amples informations, veuillez consulter [Qu'est-ce qu'Amazon VPC ?](#) dans le Guide de l'utilisateur Amazon VPC.

Directory Service utilise une structure à deux VPC. Les EC2 instances qui composent votre répertoire s'exécutent en dehors de votre AWS compte et sont gérées par AWS. Elles ont deux cartes réseau, ETH0 et ETH1. ETH0 est la carte de gestion et existe en dehors de votre compte. ETH1 est créé au sein de votre compte.

La plage d'adresses IP de gestion du réseau ETH0 de votre annuaire est choisie par programmation afin de garantir qu'elle n'entre pas en conflit avec le VPC sur lequel votre annuaire est déployé. Cette plage d'adresses IP peut être comprise dans l'une des paires suivantes (car les annuaires s'exécutent dans deux sous-réseaux) :

- 10.0.1.0/24 et 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 et 192.168.2.0/24

Nous évitons les conflits en vérifiant le premier octet du CIDR ETH1. S'il commence par un 10, nous choisissons un VPC 192.168.0.0/16 avec des sous-réseaux 192.168.1.0/24 et 192.168.2.0/24. Si le premier octet est différent de 10, nous choisissons un VPC 10.0.0.0/16 avec des sous-réseaux 10.0.1.0/24 et 10.0.2.0/24.

L'algorithme de sélection n'inclut pas de routages dans votre VPC. Il est donc possible qu'un conflit de routage IP résulte de ce scénario.

 Important

Si l'un des prérequis de Simple AD est modifié après la création de votre Simple AD, celui-ci peut devenir altéré. Pour résoudre le problème lié à la fonction Simple AD, vous devez contacter [AWS Support](#).

Créez votre Simple AD

Cette procédure vous guide à travers toutes les étapes nécessaires à la création d'un Simple AD. Il est destiné à vous permettre de démarrer rapidement et facilement avec Simple AD, mais il n'est pas destiné à être utilisé dans un environnement de production à grande échelle.

Étapes

- [Prérequis](#)
- [Création et configuration de votre Amazon VPC pour votre Simple AD](#)
- [Création de votre Simple AD](#)

Prérequis

Cette procédure suppose ce qui suit :

- Vous avez un actif Compte AWS.
- Votre compte n'a pas atteint la limite d'Amazon VPCs pour la région dans laquelle vous souhaitez utiliser Simple AD. Pour plus d'informations sur le VPC, consultez [Qu'est-ce qu'Amazon VPC ?](#) et les [sous-réseaux de votre VPC dans](#) le guide de l'utilisateur Amazon VPC.
- Vous n'avez pas de VPC existant dans la région avec un CIDR de. 10.0.0.0/16
- Vous vous trouvez dans une région où Simple AD est disponible. Pour de plus amples informations, veuillez consulter [Disponibilité de la région pour Directory Service](#).

Pour de plus amples informations, veuillez consulter [Prérequis pour Simple AD](#).

Création et configuration de votre Amazon VPC pour votre Simple AD

Tout d'abord, vous allez créer et configurer un Amazon VPC à utiliser avec votre Simple AD. Avant de commencer cette procédure, assurez-vous que vous avez terminé [Prérequis](#).

Le VPC que vous allez créer comportera deux sous-réseaux publics. Directory Service nécessite deux sous-réseaux dans votre VPC, et chaque sous-réseau doit se trouver dans une zone de disponibilité différente.

Création d'un VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le tableau de bord VPC, choisissez Créer un VPC.
3. Sous Paramètres VPC, choisissez VPC et plus encore.
4. Complétez les champs comme suit :
 - Conservez l'option Généré automatiquement sélectionnée sous Génération automatique d'identifications de noms. Redéfinissez le projet sur ADS VPC.
 - Le bloc IPv4 CIDR doit être. 10.0.0.0/16
 - Conservez l'option Aucun blocage IPv6 CIDR sélectionnée.
 - La location doit rester par défaut.
 - Sélectionnez 2 pour le nombre de zones de disponibilité (AZs).
 - Sélectionnez 2 pour le champ Nombre de sous-réseaux publics. Le nombre de sous-réseaux privés peut être redéfini sur 0.
 - Choisissez Personnaliser les blocs CIDR du sous-réseau pour configurer la plage d'adresses IP du sous-réseau public. Les blocs CIDR du sous-réseau public doivent être 10.0.0.0/20 et 10.0.16.0/20
5. Sélectionnez Create VPC (Créer un VPC). La création du VPC prend quelques minutes.

Création de votre Simple AD

Pour créer un nouveau Simple AD, effectuez les étapes suivantes. Avant de commencer cette procédure, assurez-vous d'avoir effectué les opérations suivantes dans [Prérequis](#) et [Création et configuration de votre Amazon VPC pour votre Simple AD](#).

Créez un Simple AD

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire, puis Configurer un annuaire.
2. Sur la page Sélectionner un type d'annuaire, choisissez Simple AD, puis Suivant.

3. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

Taille de l'annuaire

Faites votre choix parmi les options de taille Petit ou Large. Pour en savoir plus sur les tailles, veuillez consulter [Simple AD](#).

Nom de l'organisation

Nom d'organisation unique pour votre répertoire qui sera utilisé pour enregistrer les appareils clients.

Ce champ n'est disponible que si vous créez votre répertoire dans le cadre du lancement WorkSpaces.

Nom de DNS de l'annuaire

Nom complet de l'annuaire, par exemple corp.example.com.

Nom NetBIOS de l'annuaire

Nom court de l'annuaire, par exemple CORP.

Mot de passe administrateur

Mot de passe de l'administrateur de l'annuaire. Le processus de création du répertoire crée un compte administrateur avec le nom d'utilisateur Administrator et ce mot de passe.

Le mot de passe de l'administrateur de l'annuaire est sensible à la casse et doit comporter entre 8 et 64 caractères (inclus). Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

 Important

Assurez-vous d'enregistrer ce mot de passe. Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous pouvez toutefois réinitialiser un mot de passe depuis la Directory Service console ou à l'aide de l'[ResetUserPasswordAPI](#).

Description de l'annuaire

Description facultative de l'annuaire.

4. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes, puis choisissez Next (Suivant).

VPC

VPC de l'annuaire.

Sous-réseaux

Choisissez les sous-réseaux pour les contrôleurs de domaine. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

5. Sur la page Review & create (Vérifier et créer), vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire). La création de l'annuaire prend plusieurs minutes. Une fois l'annuaire créé, le champ Statut prend la valeur Actif.

Pour plus d'informations sur ce qui est créé avec votre Simple AD, consultez [Qu'est-ce qui est créé avec votre Simple AD](#).

Qu'est-ce qui est créé avec votre Simple AD

Lorsque vous créez un Active Directory avec Simple AD, il Directory Service exécute les tâches suivantes en votre nom :

- Configure un annuaire basé sur Samba dans le VPC.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Administrator et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

 Important

N'oubliez pas de sauvegarder ce mot de passe. Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré. Vous pouvez toutefois réinitialiser un mot de passe depuis la Directory Service console ou à l'aide de l'[ResetUserPasswordAPI](#).

- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.
- Crée un compte avec le nom AWSAdminD-**xxxxxxxx** qui dispose des privilèges d'administration de domaine. Ce compte est utilisé pour effectuer des opérations automatisées pour les opérations de maintenance des annuaires, telles que la prise de clichés d'annuaires et les transferts de rôles FSMO. Directory Service Les informations d'identification pour ce compte sont stockées en toute sécurité par Directory Service.
- Crée et associe automatiquement une interface réseau Elastic (ENI) à chacun de vos contrôleurs de domaine. Chacun d'entre ENIs eux est essentiel pour la connectivité entre votre VPC et les contrôleurs de Directory Service domaine et ne doit jamais être supprimé. Vous pouvez identifier toutes les interfaces réseau réservées à l'utilisation Directory Service par la description : « interface réseau AWS créée pour le répertoire directory-id ». Pour plus d'informations, consultez [Elastic Network Interfaces](#) dans le guide de EC2 l'utilisateur Amazon. Le serveur DNS par défaut de l'annuaire Microsoft AD Active Directory AWS géré est le serveur DNS VPC avec Classless Inter-Domain Routing (CIDR) +2. Pour plus d'informations, consultez le [serveur Amazon DNS](#) dans le guide de l'utilisateur Amazon VPC.

 Note

Les contrôleurs de domaine sont déployés par défaut dans deux zones de disponibilité d'une région et connectés à votre cloud privé virtuel (VPC) Amazon. Les sauvegardes sont effectuées automatiquement une fois par jour, et les volumes Amazon Elastic Block Store (EBS) sont chiffrés pour garantir la sécurité des données au repos. Les contrôleurs de domaine qui échouent sont automatiquement remplacés dans la même zone de disponibilité à l'aide de la même adresse IP, et une reprise après sinistre complète peut être effectuée avec la dernière sauvegarde.

Bonnes pratiques pour Simple AD

Voici quelques suggestions et directives à prendre en compte pour éviter les problèmes et tirer le meilleur parti de Simple AD.

Configuration : prérequis

Pensez à utiliser ces consignes avant de créer votre annuaire.

Vérifiez que vous avez le type d'annuaire approprié

Directory Service propose plusieurs méthodes d'utilisation Microsoft Active Directory avec d'autres AWS services. Vous pouvez choisir le service d'annuaire doté des fonctionnalités dont vous avez besoin à un prix adapté à votre budget :

- AWS Directory Service pour Microsoft Active Directory est un service géré riche en fonctionnalités Microsoft Active Directory hébergé sur le AWS cloud. AWS Managed Microsoft AD est votre meilleur choix si vous avez plus de 5 000 utilisateurs et que vous avez besoin d'établir une relation de confiance entre un annuaire AWS hébergé et vos annuaires locaux.
- AD Connector connecte simplement votre Active Directory local existant à AWS. AD Connector est votre meilleur allié si vous souhaitez utiliser votre annuaire sur site existant avec les services AWS .
- Simple AD est un annuaire de base à moindres coûts qui offre une compatibilité de base avec Active Directory. Il prend en charge jusqu'à 5 000 utilisateurs, des applications compatibles avec Samba 4 et une compatibilité LDAP pour les applications LDAP.

Pour une comparaison plus détaillée des Directory Service options, voir [Que choisir ?](#).

Assurez-vous que vos instances VPCs et instances sont correctement configurées

Pour vous connecter à vos annuaires, les gérer et les utiliser, vous devez configurer correctement les VPCs répertoires auxquels ils sont associés. Consultez [Conditions préalables à la création d'un Microsoft AWS AD géré](#), [Conditions préalables requises pour AD Connector](#) ou [Prérequis pour Simple AD](#) pour obtenir plus d'informations sur les exigences de sécurité et de mise en réseau des VPC.

Si vous ajoutez une instance à votre domaine, assurez-vous de disposer d'une connectivité et d'un accès à distance à votre instance, comme décrit dans [Comment associer une EC2 instance Amazon à votre Microsoft AD AWS géré](#).

Tenez compte des limites

Découvrez les différentes limites applicables à votre type d'annuaire spécifique. Le stockage disponible et la taille globale de vos objets sont les seules limites quant au nombre d'objets que vous pouvez stocker dans votre annuaire. Consultez [AWS Quotas Microsoft AD gérés](#), [Quotas AD Connector](#) ou [Quotas Simple AD](#) pour plus d'informations sur l'annuaire que vous avez choisi.

Comprenez la configuration et l'utilisation AWS des groupes de sécurité de votre annuaire

AWS crée un [groupe de sécurité](#) et l'attache aux [interfaces réseau élastiques](#) du contrôleur de domaine de votre annuaire. AWS configure le groupe de sécurité pour bloquer le trafic inutile vers le répertoire et autorise le trafic nécessaire.

Modification du groupe de sécurité de l'annuaire

Vous pouvez modifier les groupes de sécurité pour vos annuaires, mais uniquement si vous comprenez parfaitement le filtrage des groupes de sécurité. Pour plus d'informations, consultez les [groupes EC2 de sécurité Amazon pour les instances Linux](#) dans le guide de EC2 l'utilisateur Amazon. Des modifications inappropriées peuvent perturber les communications avec les ordinateurs et les instances concernés. AWS recommande de ne pas ouvrir de ports supplémentaires vers votre répertoire car cela réduit la sécurité. Passez en revue le [modèle de responsabilité AWS partagée](#) avant d'apporter des modifications.

Warning

Il est techniquement possible d'associer le groupe de sécurité de l'annuaire aux autres EC2 instances que vous créez. Il AWS déconseille toutefois cette pratique. AWS peut avoir des raisons de modifier le groupe de sécurité sans préavis pour répondre aux besoins fonctionnels ou de sécurité du répertoire géré. Ces modifications affectent toutes les instances auxquelles vous associez le groupe de sécurité d'annuaire et peuvent interrompre le fonctionnement des instances associées. En outre, l'association du groupe de sécurité de l'annuaire à vos EC2 instances peut créer un risque de sécurité potentiel pour vos EC2 instances.

Utilisez AWS Managed Microsoft AD si des approbations sont requises

Simple AD ne prend pas en charge des relations d'approbation. Si vous devez établir une relation de confiance entre votre Directory Service annuaire et un autre annuaire, vous devez utiliser AWS Directory Service pour Microsoft Active Directory.

Configuration : création de votre annuaire

Voici quelques suggestions à prendre en compte lorsque vous créez votre annuaire.

Rétention de vos ID et mot de passe d'administrateur

Lorsque vous configurez votre annuaire, vous fournissez un mot de passe pour le compte d'administrateur. Cet ID de compte est un administrateur pour Simple AD. Retenez le mot de passe créé pour ce compte, sinon vous ne serez pas en mesure d'ajouter des objets à votre annuaire.

Comprendre les restrictions relatives aux noms d'utilisateur pour AWS les applications

Directory Service prend en charge la plupart des formats de caractères pouvant être utilisés dans la construction des noms d'utilisateur. Cependant, certaines restrictions de caractères sont appliquées aux noms d'utilisateur qui seront utilisés pour se connecter à AWS des applications WorkSpaces WorkDocs, telles qu'Amazon WorkMail ou Quick Suite. Ces restrictions empêchent l'utilisation des caractères suivants :

- Espaces
- Caractères multioctets
- !"#\$%&'()*+,-./:;<=>?@[\\]^`{|}~

Note

Le symbole @ est autorisé s'il précède un suffixe UPN.

Programmation de vos applications

Avant de programmer vos applications, prenez en compte les éléments suivants :

Utilisez le service de localisation des contrôleurs de domaine de Windows

Lorsque vous développez des applications, utilisez le service de localisation Windows DC ou le service DNS dynamique (DDNS) de votre Managed AWS Microsoft AD pour localiser les contrôleurs de domaine (DCs). Ne codez pas en dur les applications avec l'adresse d'un contrôleur de domaine. Le service de localisation des contrôleurs de domaine permet de garantir que l'annuaire est distribué et vous permet de tirer parti de la mise à l'échelle horizontale en ajoutant des contrôleurs de domaine à votre déploiement. Si vous liez votre application à un contrôleur de domaine fixe et que celui-ci est soumis à des correctifs ou à une restauration, votre application perdra l'accès au contrôleur de domaine au lieu d'utiliser l'un des autres contrôleurs. DCs En outre, le codage en dur du contrôleur de domaine peut entraîner la création d'un point chaud sur un seul contrôleur de domaine. Dans des cas extrêmes, la création de ce point chaud peut entraîner une absence de réponse de votre contrôleur de domaine. Dans de tels cas, l'automatisation de l' AWS annuaire peut également signaler le répertoire comme étant altéré et peut déclencher des processus de restauration qui remplacent le contrôleur de domaine qui ne répond pas.

Testez la charge avant de lancer la production

Assurez-vous de procéder à des tests avec des objets et des requêtes représentatifs de votre charge de travail de production afin de confirmer que l'annuaire s'adapte à la charge de travail de votre application. Si vous avez besoin de capacité supplémentaire, vous devez utiliser Directory Service Microsoft Active Directory, qui vous permet d'ajouter des contrôleurs de domaine pour des performances élevées. Pour de plus amples informations, veuillez consulter [Déploiement de contrôleurs de domaine supplémentaires pour votre Microsoft AD AWS géré](#).

Utilisez des requêtes LDAP efficaces

De vastes requêtes LDAP effectuées dans un contrôleur de domaine sur des milliers d'objets peuvent consommer des cycles de processeur considérables sur un seul contrôleur de domaine, ce qui se traduit par la création de points chauds. Ces points chauds peuvent affecter les applications qui partagent le même contrôleur de domaine lors de la requête.

Maintenance de votre annuaire Simple AD

Vous pouvez utiliser le AWS Management Console pour gérer votre Simple AD et effectuer des tâches day-to-day administratives. Vous pouvez gérer votre Simple AD de différentes manières :

- [Consultez les détails de votre Simple AD](#), tels que le nom DNS, l'ID du répertoire et le statut du répertoire.

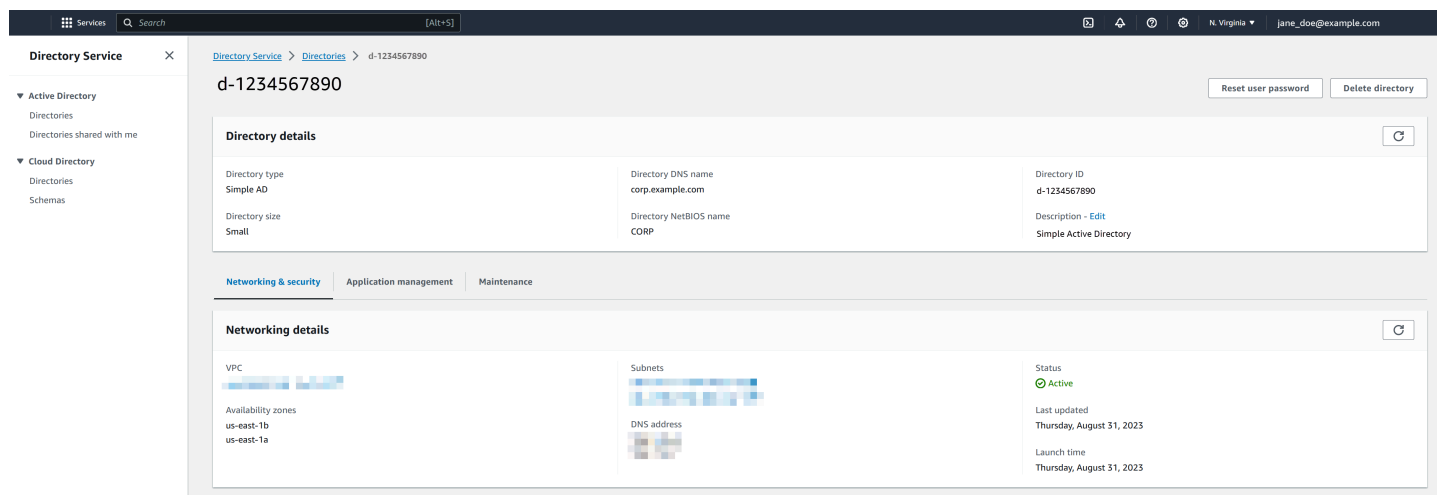
- [Mettez à jour l'adresse DNS de votre Simple AD.](#)
- [Restaurez votre Simple AD à l'aide de snapshots.](#) Vous pouvez également créer et supprimer des instantanés.
- [Supprimez votre Simple AD](#) lorsqu'il n'est plus nécessaire.

Afficher les informations d'un annuaire Simple AD

Pour afficher les informations détaillées de l'annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), sous Active Directory, sélectionnez Annuaires.
2. Choisissez le lien de l'ID correspondant à votre annuaire. Les informations relatives à l'annuaire sont affichées sur la page Détails de l'annuaire.

Pour de plus amples informations sur le champ Status (Statut), veuillez consulter [Comprendre le statut de votre annuaire Simple AD](#).



Mise à jour du type de réseau d'annuaire

Vous pouvez mettre à jour le type de réseau de votre Directory Service annuaire en le faisant IPv4 passer à Dual-stack (IPv4 et IPv6). La mise à jour du type de réseau pour inclure les adresses IPv6 IP fournit un espace d'adressage plus important que IPv4. IPv4 et les IPv6 communications sont indépendantes l'une de l'autre.

Pour plus de détails, consultez la section [Comparer IPv4 et IPv6](#) le guide de l'utilisateur d'Amazon Virtual Private Cloud.

 Important

Il s'agit d'une opération unidirectionnelle qui ne peut pas être inversée. Effectuez d'abord un test dans un environnement hors production.

Prérequis

Avant de mettre à jour le type de réseau de votre annuaire, assurez-vous que les conditions suivantes sont remplies :

- Votre VPC doit être configuré avec des plages d'adresses IPv6 CIDR. Pour plus de détails, consultez la section relative [à la prise en IPv6 charge de votre VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.
- Vous disposez d'un accès administratif au AWS Management Console.
- Votre répertoire doit être à l'état actif.
- Vous disposez des autorisations IAM appropriées pour modifier les Directory Service paramètres.

Pour mettre à jour le type de réseau d'annuaire

Pour mettre à jour votre répertoire vers un réseau à double pile

 Note

Si votre répertoire est répliqué dans plusieurs régions, effectuez cette mise à jour dans chaque région.

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sélectionnez le répertoire cible.
3. Accédez à l'onglet Réseau et sécurité.
4. Choisissez Ajouter un IPv6 support. Cette option n'est disponible que pour les répertoires IPv4 uniquement.

IPv6 seuls les répertoires ne sont pas pris en charge.

5. Consultez les informations de mise à jour et les détails des prix.

6. Choisissez Ajouter pour confirmer la mise à jour.

Une fois la mise à jour lancée, le statut du répertoire passe à Mise à jour pendant le processus de mise à jour. La mise à jour prend généralement 15 à 30 minutes. Une fois terminée, le statut du répertoire redevient Actif.

Configuration des serveurs DNS pour Simple AD

Simple AD transfère les demandes DNS à l'adresse IP des serveurs DNS fournis par Amazon pour votre VPC Amazon. Ces serveurs DNS résolvent les noms configurés dans vos zones hébergées privées Amazon Route 53. En pointant vos ordinateurs sur site vers votre Simple AD, vous pouvez désormais résoudre les demandes DNS dans la zone hébergée privée. Pour plus d'informations sur Route 53, veuillez consulter [What is Route 53](#) (français non garanti).

Notez que pour activer votre Simple AD pour répondre aux requêtes DNS externes, la liste de contrôle d'accès (ACL) réseau pour le VPC contenant votre Simple AD doit être configurée pour autoriser le trafic depuis l'extérieur du VPC.

- Si vous n'utilisez pas les zones hébergées privées Route 53, vos demandes DNS seront transmises aux serveurs DNS publics.
- Si vous utilisez des serveurs DNS personnalisés situés en dehors de votre VPC et que vous souhaitez utiliser un DNS privé, vous devez reconfigurer pour utiliser des serveurs DNS personnalisés sur les EC2 instances de votre VPC. Pour plus d'informations, veuillez consulter [Utilisation des zones hébergées privées](#).
- Si vous voulez que votre Simple AD résolve les noms à l'aide des serveurs DNS au sein de votre VPC et des serveurs DNS privés en dehors de votre VPC, vous pouvez le faire à l'aide d'un jeu d'options DHCP. Pour obtenir un exemple détaillé, veuillez consulter [cet article](#).
- [Intégrer votre Directory Service's résolution DNS avec Amazon Route 53 Resolver](#).

Note

Les mises à jour dynamiques DNS ne sont pas prises en charge dans les domaines Simple AD. En revanche, vous pouvez effectuer les modifications directement en connectant votre annuaire à l'aide du Gestionnaire DNS sur une instance qui est jointe à votre domaine.

Restauration de votre Simple AD à l'aide d'un instantané

AWS Directory Service permet de prendre des instantanés manuels des données de votre annuaire Simple AD. Ces instantanés peuvent être utilisés pour effectuer une point-in-time restauration de votre répertoire. Il est impossible de prendre des instantanés des annuaires AD Connector.

Rubriques

- [Création d'un instantané de votre annuaire.](#)
- [Restauration de l'annuaire à partir d'un instantané.](#)
- [Suppression d'un instantané](#)

Création d'un instantané de votre annuaire.

Un instantané vous permet de restaurer votre répertoire tel qu'il était au moment où il a été pris. Pour créer un instantané manuel de votre annuaire, exécutez les étapes suivantes.

Note

Vous êtes limité à 5 instantanés manuels par annuaire. Si vous avez déjà atteint cette limite, vous devez supprimer un de vos instantanés manuels existants avant de pouvoir en créer un autre.

Pour créer un snapshot manuel

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis sélectionnez Créer un instantané.
5. Dans la boîte de dialogue Créer un instantané d'annuaire, entrez une description de l'instantané, si vous le souhaitez. Lorsque vous êtes prêt, choisissez Créer.

Selon la taille de votre répertoire, la création de l'instantané peut prendre plusieurs minutes. Lorsque l'instantané est prêt, la valeur Statut devient Completed.

Restauration de l'annuaire à partir d'un instantané.

Restaurer un annuaire à partir d'un instantané revient à le déplacer dans le temps. Les instantanés d'annuaire sont propres à l'annuaire à partir duquel ils ont été créés. Un instantané ne peut être restauré que dans l'annuaire à partir duquel il a été créé. En outre, la durée maximale de prise en charge pour un instantané manuel est de 180 jours. Pour plus d'informations, veuillez consulter la section [Useful shelf life of a system-state backup of Active Directory](#) (français non garanti) sur le site web Microsoft.

Warning

Nous vous recommandons de contacter le [Centre AWS Support](#) avant toute restauration à partir d'un instantané ; nous pourrions peut-être vous aider à éviter d'avoir à effectuer une restauration à partir d'un instantané. Toute restauration à partir d'un instantané peut entraîner une perte de données, car les instantanés correspondent à un moment donné. Il est important que vous sachiez que tous les serveurs DNS DCs et les serveurs DNS associés à l'annuaire seront hors ligne jusqu'à ce que l'opération de restauration soit terminée.

Pour restaurer un annuaire à partir d'un instantané, procédez comme suit :

Pour restaurer un annuaire à partir d'un instantané

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, sélectionnez un instantané dans la liste, choisissez Actions, puis sélectionnez Restaurer l'instantané.
5. Passez en revue les informations contenues dans la boîte de dialogue Restaurer un instantané d'annuaire, puis sélectionnez Restaurer.

La restauration d'un annuaire Simple AD peut prendre plusieurs minutes. Une fois la restauration réussie, la valeur Statut du répertoire devient Active. Toutes les modifications apportées à l'annuaire après la date de l'instantané sont remplacées.

Suppression d'un instantané

Suppression d'un instantané

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Maintenance.
4. Dans la section Instantanés, choisissez Actions, puis Supprimer l'instantané.
5. Vérifiez que vous souhaitez supprimer l'instantané, puis sélectionnez Supprimer.

Supprimer votre Simple AD

Lorsqu'un Simple AD est supprimé, toutes les données de l'annuaire et les instantanés sont supprimés et ne peuvent pas être récupérés. Une fois que l'annuaire est supprimé, toutes les instances qui sont jointes à l'annuaire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous y connecter avec un compte utilisateur qui est local à l'instance.

Lorsqu'un annuaire Microsoft AD AWS géré, Simple AD ou hybride est supprimé, toutes les données de l'annuaire et les instantanés sont supprimés et ne peuvent pas être restaurés. Une fois que l'annuaire est supprimé, toutes les instances qui sont jointes à l'annuaire restent intactes. Toutefois, vous ne pouvez pas utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances. Vous devez vous y connecter avec un compte utilisateur qui est local à l'instance.

Lorsqu'un connecteur AD Connector est supprimé, votre annuaire sur site reste intact. Toutes les instances qui sont jointes à l'annuaire restent également intactes et jointes à votre annuaire sur site. Vous pouvez toutefois utiliser les informations d'identification de votre annuaire pour vous connecter à ces instances.

Pour supprimer un annuaire

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire). Assurez-vous que vous vous trouvez à l' Région AWS endroit où votre Active Directory est déployé. Pour plus d'informations, voir [Choisir une région](#).

2. Assurez-vous qu'aucune AWS application n'est activée pour le répertoire que vous souhaitez supprimer. AWS Les applications activées vous empêcheront de supprimer votre AWS Managed Microsoft AD ou Simple AD.
 - a. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
 - b. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications). Dans la section AWS Applications et services, vous pouvez voir quelles AWS applications sont activées pour votre annuaire.
 - Désactivez AWS Management Console l'accès. Pour de plus amples informations, veuillez consulter [Désactivation AWS Management Console de l'accès](#).
 - Pour désactiver Amazon WorkSpaces, vous devez désenregistrer le service depuis le répertoire de la WorkSpaces console. Pour plus d'informations, consultez [Supprimer un répertoire](#) dans le guide d' WorkSpaces administration Amazon.
 - Pour le désactiver WorkDocs, vous devez supprimer le WorkDocs site dans la WorkDocs console. Pour plus d'informations, consultez [Supprimer un site](#) dans le guide d' WorkDocs administration Amazon.
 - Pour désactiver Amazon WorkMail, vous devez supprimer l' WorkMail organisation Amazon dans la WorkMail console Amazon. Pour plus d'informations, consultez [Supprimer une organisation](#) dans le manuel Amazon WorkMail Administrator Guide.
 - Pour désactiver le serveur de fichiers Amazon FSx pour Windows, vous devez supprimer le système de FSx fichiers Amazon du domaine. Pour plus d'informations, consultez la section [Travailler avec Active Directory dans FSx un serveur de fichiers Windows](#) dans le guide de l'utilisateur d'Amazon FSx pour Windows File Server.
 - Pour désactiver Amazon Relational Database Service, vous devez supprimer l'instance Amazon RDS du domaine. Pour plus d'informations, veuillez consulter la section [Managing a DB instance in a domain](#) (français non garanti) dans le Guide de l'utilisateur Amazon RDS.
 - Pour désactiver le AWS Client VPN service, vous devez supprimer le service d'annuaire du point de terminaison VPN du Client. Pour plus d'informations, consultez la [section Utilisation du Client VPN](#) dans le Guide de AWS Client VPN l'administrateur.
 - Pour désactiver Amazon Connect, vous devez supprimer l'instance Amazon Connect. Pour plus d'informations, consultez [Supprimer votre instance Amazon Connect](#) dans le guide d'administration Amazon Connect.

- Pour désactiver Amazon Quick Suite, vous devez vous désabonner d'Amazon Quick Suite. Pour plus d'informations, consultez la section [Fermeture de votre Amazon Quick Suite compte](#) dans le guide de l'utilisateur d'Amazon Quick Suite.

 Note

Si vous l'utilisez AWS IAM Identity Center et que vous l'avez déjà connecté au répertoire AWS Managed Microsoft AD que vous souhaitez supprimer, vous devez d'abord modifier la source d'identité avant de pouvoir la supprimer. Pour plus d'informations, veuillez consulter la section [Change your identity source](#) (français non garanti) dans le Guide de l'utilisateur IAM Identity Center.

3. Dans le volet de navigation, choisissez Directories (Annuaire).
4. Sélectionnez uniquement l'annuaire à supprimer, puis cliquez sur Supprimer. La suppression de l'annuaire prend plusieurs minutes. Lorsque l'annuaire a été supprimé, il est retiré de votre liste d'annuaires.

Sécurisez votre annuaire Simple AD

Cette section décrit les considérations relatives à la sécurisation de votre environnement Simple AD.

Rubriques

- [Comment réinitialiser le mot de passe d'un compte Simple AD krbtgt](#)

Comment réinitialiser le mot de passe d'un compte Simple AD krbtgt

Le compte krbtgt joue un rôle important dans les échanges de billets Kerberos. Le compte krbtgt est un compte spécial utilisé pour le chiffrement des tickets d'octroi de tickets (TGT) Kerberos, et il joue un rôle crucial dans la sécurité du protocole d'authentification Kerberos. Dans Samba AD, krbtgt est représenté comme un compte utilisateur (désactivé). Le mot de passe de ce compte est généré de manière aléatoire au moment de la mise en service du domaine. L'accès à ce secret peut entraîner une compromission totale indétectable du domaine, car les nouveaux tickets Kerberos peuvent être imprimés sans audit. Pour plus d'informations, consultez la [documentation Samba](#).

Il est recommandé de changer ce mot de passe régulièrement tous les 90 jours. Vous pouvez réinitialiser le mot de passe du compte krbtgt depuis une EC2 Windows instance Amazon associée à votre Simple AD.

 Note

AWS Simple AD est développé par Samba-AD. Samba-AD ne stocke pas le hachage N-1 pour le compte krbtgt. Par conséquent, lorsque le mot de passe du compte krbtgt est réinitialisé, le client Kerberos devra négocier un nouveau ticket d'octroi de ticket (TGT) lors de sa prochaine demande de service ticket (ST). Pour minimiser les interruptions de service potentielles, vous devez planifier la réinitialisation du mot de passe du compte krbtgt en dehors des heures de bureau. Cette approche atténue les impacts sur les opérations en cours et garantit une continuité d'authentification fluide.

Les procédures suivantes montrent comment réinitialiser le mot de passe du compte krbtgt depuis une instance Amazon EC2 Windows.

Prérequis

- Avant de commencer cette procédure, effectuez les opérations suivantes :
 - Votre domaine a joint une EC2 instance à votre annuaire Simple AD.
 - Pour plus d'informations sur la façon de joindre une EC2 Windows instance à un Simple AD, consultez [the section called “Rejoindre une instance Windows”](#).
 - Vous disposez des informations d'identification de l'administrateur de l'annuaire Simple AD. Vous allez vous connecter en tant qu'administrateur de l'annuaire Simple AD pour cette procédure.

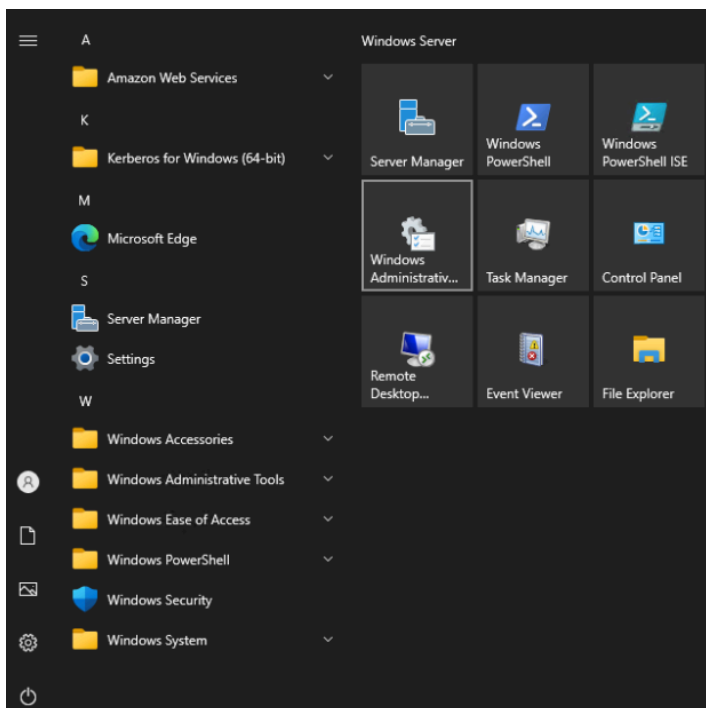
 Note

Certains Services AWS comme Amazon WorkDocs et Amazon WorkSpaces, créeront un Simple AD en votre nom.

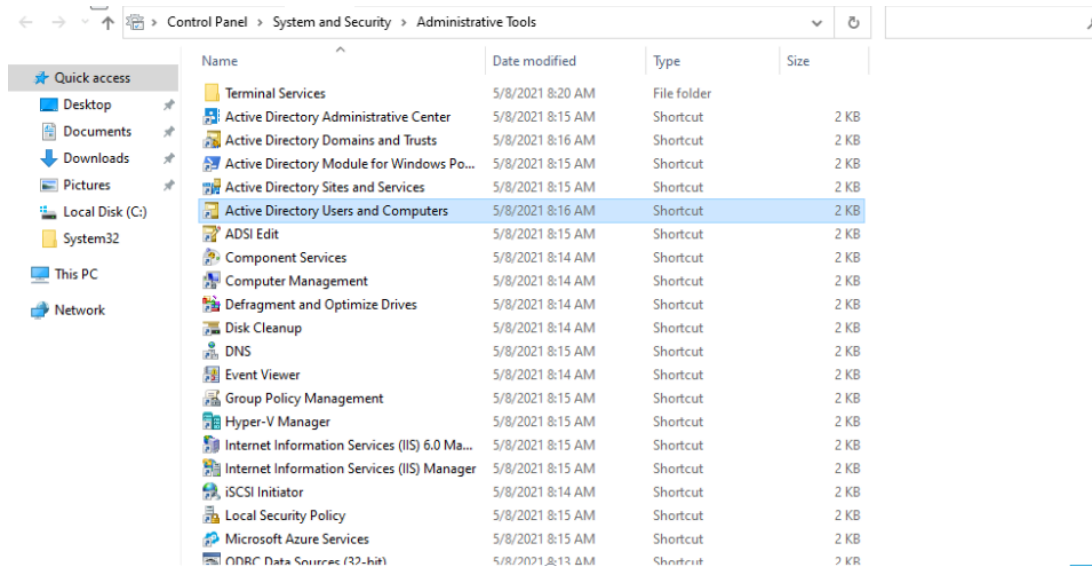
Réinitialiser le mot de passe du compte Simple AD krbtgt

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.

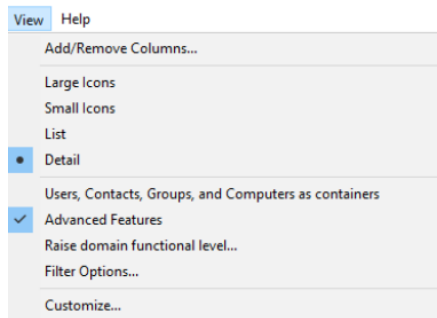
2. Dans la EC2 console Amazon, choisissez Instances et sélectionnez l'instance de Windows serveur. Choisissez ensuite Connect (Connecter).
3. Dans la page Se connecter à l'instance, sélectionnez Client RDP.
4. Dans la boîte de dialogue de sécurité Windows, copiez vos informations d'identification d'administrateur local pour que l'ordinateur Windows serveur puisse se connecter. Le nom d'utilisateur peut être dans les formats suivants : NetBIOS-Name\administrator ou DNS-Name\administrator. Par exemple, corp\administrator ce serait le nom d'utilisateur si vous avez suivi la procédure dans [the section called “Créez votre Simple AD”](#).
5. Une fois connecté à l'ordinateur Windows serveur, ouvrez les outils d'Windowsadministration dans le menu Démarrer en choisissant le dossier Outils d'Windowsadministration.



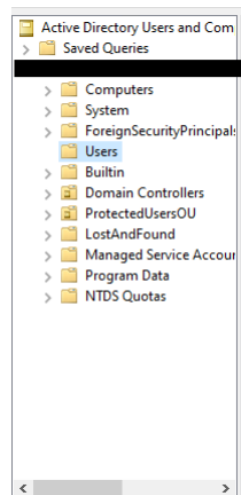
6. Dans le tableau de bord des outils d'Windowsadministration, ouvrez Utilisateurs et ordinateurs Active Directory en choisissant Utilisateur et ordinateurs Active Directory.



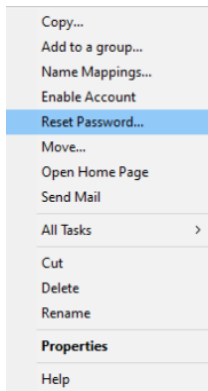
7. Dans la fenêtre Utilisateurs et ordinateurs Active Directory, sélectionnez Afficher, puis sélectionnez Activer les fonctionnalités avancées.



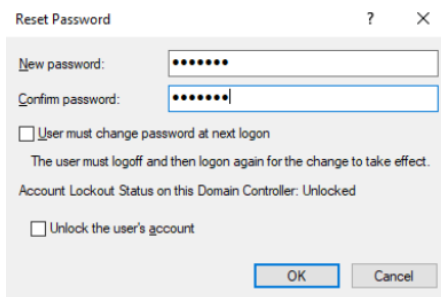
8. Dans la fenêtre Utilisateurs et ordinateurs Active Directory, sélectionnez Utilisateurs dans le panneau de gauche.



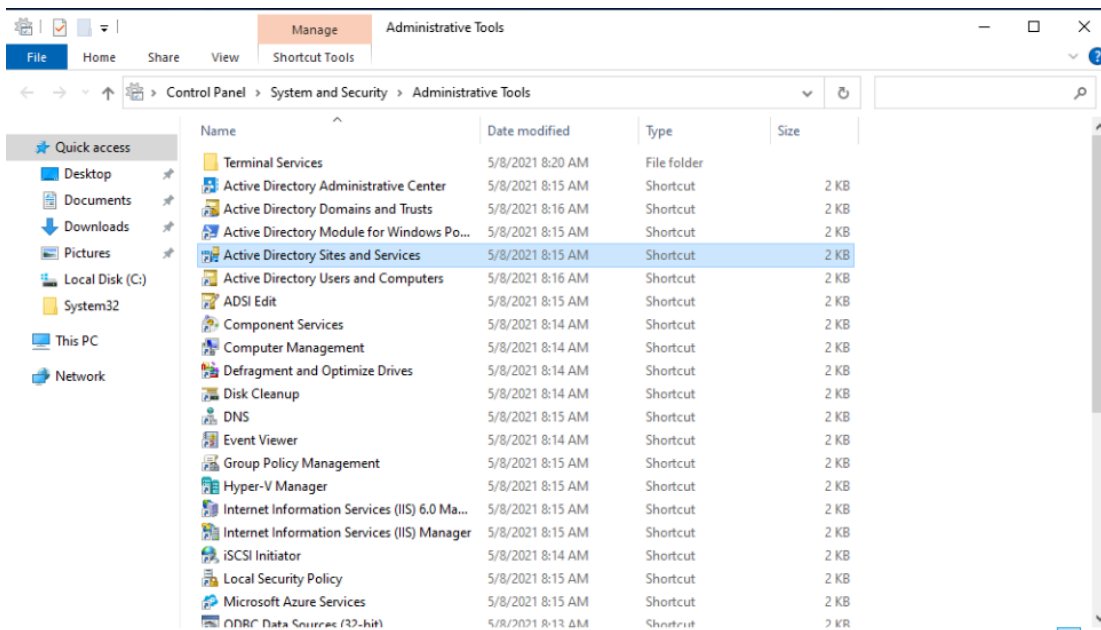
9. Trouvez l'utilisateur nommé krbtgt, cliquez dessus avec le bouton droit de la souris et sélectionnez Réinitialiser le mot de passe.



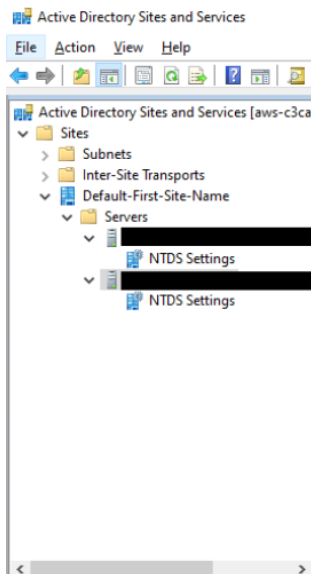
10. Dans la nouvelle fenêtre, entrez le nouveau mot de passe, saisissez-le à nouveau, puis cliquez sur OK pour réinitialiser le mot de passe du compte krbtgt.



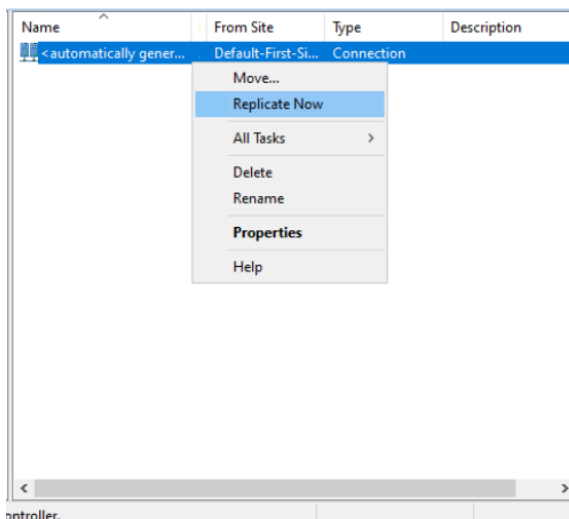
11. Dans le tableau de bord des outils d'Windowsadministration, sélectionnez Sites et services Active Directory.



12. Dans la fenêtre Sites et services Active Directory, développez Site, Default-First-Site-Name et Servers.



13. Dans la fenêtre des paramètres NTDS, cliquez avec le bouton droit sur le serveur et sélectionnez Répliquer maintenant.



14. Répétez les étapes 13 à 14 pour vos autres serveurs.

Surveillance de votre annuaire Simple AD

Vous pouvez tirer le meilleur parti de votre Simple AD en découvrant les différents statuts de Simple AD et ce qu'ils signifient pour votre Simple AD. Vous pouvez également utiliser AWS des services tels qu'Amazon Simple Notification Service pour surveiller votre Simple AD. Amazon Simple Notification Service peut vous envoyer des notifications concernant le statut de votre annuaire Simple AD.

Tâches pour surveiller votre Simple AD

- [Comprendre le statut de votre annuaire Simple AD](#)
- [Activation des notifications d'état de l'annuaire Simple AD avec Amazon Simple Notification Service](#)

Comprendre le statut de votre annuaire Simple AD

Voici les différents statuts possibles pour un annuaire.

Actif

L'annuaire fonctionne normalement. Aucun problème n'a été détecté par Directory Service pour votre annuaire.

Création

L'annuaire est en cours de création. La création de l'annuaire prend généralement entre 20 et 45 minutes, mais peut varier selon la charge du système.

Supprimé

L'annuaire a été supprimé. Toutes les ressources de l'annuaire ont été libérées. Une fois qu'un annuaire se trouve dans cet état, il ne peut pas être récupéré.

Suppression en cours

L'annuaire est en cours de suppression. L'annuaire restera dans cet état jusqu'à ce qu'il soit totalement supprimé. Une fois qu'un annuaire se trouve dans cet état, l'opération de suppression ne peut pas être annulée, et l'annuaire ne peut pas être récupéré.

Échec

L'annuaire n'a pas pu être créé. Veuillez supprimer cet annuaire. Si le problème persiste, veuillez contacter le [centre AWS Support](#).

Dégradé

L'annuaire est en cours d'exécution dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles. Il existe de nombreuses raisons pouvant expliquer que l'annuaire se trouve dans cet état. Il s'agit notamment des activités de maintenance opérationnelle normales telles que l'application de correctifs ou la rotation des EC2 instances, le repérage temporaire par une application sur l'un de vos contrôleurs de domaine ou les modifications que vous avez apportées

à votre réseau qui perturbent par inadvertance les communications d'annuaire. L'état de votre répertoire peut être altéré si vous modifiez les paramètres décrits dans [Prérequis pour Simple AD](#). Pour plus d'informations, veuillez consulter [Résolution des problèmes liés AWS à Managed Microsoft AD](#), [Résolution des problèmes liés à AD Connector](#), [Résolution des problèmes de Simple AD](#). Pour les problèmes normaux liés à la maintenance, AWS les problèmes sont résolus dans les 40 minutes. Si, après avoir consulté la rubrique de dépannage, votre annuaire reste à l'état Dégradé pendant plus de 40 minutes, nous vous recommandons de contacter le [centre AWS Support](#).

 Important

Ne restaurez pas un instantané lorsqu'un annuaire est dans un état dégradé. Il est rare qu'une restauration d'instantané soit nécessaire pour résoudre les problèmes d'état dégradé. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#).

Inopérable

L'annuaire n'est pas fonctionnel. Tous les points de terminaison de l'annuaire ont signalé des problèmes.

Demandé

La demande de création de votre annuaire est actuellement en attente.

RestoreFailed

Échec de la restauration de l'annuaire à partir d'un instantané. Renouvelez l'opération de restauration. Si le problème persiste, utilisez un autre instantané ou contactez le [centre AWS Support](#).

Restauration en cours

L'annuaire est en cours de restauration à partir d'un instantané automatique ou manuel. La restauration à partir d'un instantané prend généralement plusieurs minutes, selon la taille des données de l'annuaire dans l'instantané.

Pour de plus amples informations, veuillez consulter [Résolution des messages d'état de l'annuaire Simple AD](#).

Activation des notifications d'état de l'annuaire Simple AD avec Amazon Simple Notification Service

Avec Amazon Simple Notification Service (Amazon SNS), vous pouvez recevoir des e-mails ou des messages texte (SMS) lorsque le statut de votre annuaire change. Vous êtes averti lorsque votre annuaire passe du statut Active (Actif) au [statut Impaired \(Défaillant\) ou Inoperable \(Inutilisable\)](#). Vous recevez également une notification lorsque l'annuaire renvoie un statut Active (Actif).

Comment ça marche

Amazon SNS utilise des « rubriques » pour collecter et diffuser des messages. Chaque rubrique compte un ou plusieurs abonnés qui reçoivent les messages qui ont été publiés dans cette rubrique. En suivant les étapes ci-dessous, vous pouvez ajouter un article Directory Service en tant qu'éditeur à une rubrique Amazon SNS. Lorsqu'il Directory Service détecte un changement dans le statut de votre annuaire, il publie un message sur ce sujet, qui est ensuite envoyé aux abonnés du sujet.

Vous pouvez associer plusieurs annuaires en tant que diffuseurs de publication à une même rubrique. Vous pouvez également ajouter des messages de statut de l'annuaire aux rubriques que vous avez créées précédemment dans Amazon SNS. Vous avez un contrôle détaillé sur les personnes autorisées à publier et à s'abonner à une rubrique. Pour obtenir des informations détaillées sur Amazon SNS, veuillez consulter [Qu'est-ce qu'Amazon SNS ?](#)

Pour activer la messagerie SNS pour votre annuaire

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, choisissez Actions, puis sélectionnez Créer une notification.
5. Sur la page Créer une notification, sélectionnez Choisir un type de notification, puis choisissez Créer une notification. Si vous avez déjà une rubrique SNS existante, vous pouvez également choisir Associer une rubrique SNS existante pour envoyer des messages de statut de cet annuaire à cette rubrique.

Note

Si vous choisissez Créer une nouvelle notification, mais que vous utilisez le même nom de rubrique pour une rubrique SNS qui existe déjà, Amazon SNS ne crée pas de

rubrique, mais ajoute simplement les nouvelles informations d'abonnement à la rubrique existante.

Si vous choisissez Associer une rubrique SNS existante, vous ne pourrez choisir qu'une rubrique SNS située dans la même région que l'annuaire.

6. Choisissez le type de destinataire et saisissez les coordonnées du destinataire. Si vous saisissez un numéro de téléphone pour les SMS, utilisez uniquement des chiffres. N'incluez pas de tirets, d'espaces, ni de parenthèses.
7. (Facultatif) Donnez un nom à votre rubrique et un nom d'affichage SNS. Le nom d'affichage est un nom court de 10 caractères maximum inclus dans tous les messages SMS de cette rubrique. Lorsque vous utilisez l'option SMS, le nom d'affichage est obligatoire.

 Note

Si vous êtes connecté à l'aide d'un utilisateur ou d'un rôle IAM doté uniquement de la politique [DirectoryServiceFullAccess](#) gérée, le nom de votre rubrique doit commencer par « DirectoryMonitoring ». Si vous souhaitez personnaliser davantage le nom de votre rubrique, vous aurez besoin de privilèges supplémentaires pour SNS.

8. Sélectionnez Create (Créer).

Si vous souhaitez désigner des abonnés SNS supplémentaires, tels qu'une adresse e-mail supplémentaire, des files d'attente Amazon SQS AWS Lambda ou, vous pouvez le faire depuis la console Amazon [SNS](#).

Pour supprimer les messages de statut de l'annuaire d'une rubrique

1. Connectez-vous à la [Directory Service console AWS Management Console et ouvrez-la](#).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sélectionnez l'onglet Maintenance.
4. Dans la section Surveillance de l'annuaire, sélectionnez le nom d'une rubrique SNS dans la liste, choisissez Actions, puis sélectionnez Supprimer.
5. Sélectionnez Remove (Supprimer).

Cela supprime votre annuaire en tant que diffuseur de publication pour la rubrique SNS sélectionnée. Si vous souhaitez supprimer le sujet dans son intégralité, vous pouvez le faire depuis la console [Amazon SNS](#).

Note

Avant de supprimer une rubrique Amazon SNS à l'aide de la console SNS, vous devez vous assurer qu'aucun annuaire n'envoie de messages de statut à cette rubrique.

Si vous supprimez une rubrique Amazon SNS à l'aide de la console SNS, cette modification ne sera pas immédiatement reflétée dans la console Directory Services. Vous ne serez averti que la prochaine fois qu'un annuaire publiera une notification concernant la rubrique supprimée, auquel cas vous verrez un statut mis à jour dans l'onglet Surveillance de l'annuaire indiquant que la rubrique est introuvable.

Par conséquent, pour éviter de manquer des messages importants sur le statut du répertoire, avant de supprimer toute rubrique recevant des messages Directory Service, associez votre annuaire à une autre rubrique Amazon SNS.

Accès aux AWS applications et aux services depuis votre Simple AD

Vous pouvez autoriser les utilisateurs de Simple AD à accéder aux AWS applications et aux services. Certains de ces services et AWS applications incluent :

- Amazon WorkDocs
- AWS Management Console
- Amazon WorkSpaces

Vous pouvez également utiliser l'accès URLs et l'authentification unique avec votre Simple AD.

Rubriques

- [Politique de compatibilité des applications pour Simple AD](#)
- [Permettre l'accès aux AWS applications et aux services pour votre Simple AD](#)
- [Permettre l'accès à l' AWS Management Console aide des informations d'identification Simple AD](#)
- [Création d'une URL d'accès pour Simple AD](#)

- [Activation de l'authentification unique](#)

Politique de compatibilité des applications pour Simple AD

Simple AD est une implémentation de Samba qui fournit la plupart des fonctionnalités de base d'Active Directory. En raison de l'ampleur des off-the-shelf applications personnalisées et commerciales qui utilisent Active Directory, AWS Active Directory n'effectue pas et ne peut pas effectuer de vérification formelle ou étendue de la compatibilité des applications tierces avec Simple AD. Bien que AWS nous travaillons avec les clients pour tenter de surmonter les éventuels problèmes d'installation d'applications qu'ils pourraient rencontrer, nous ne sommes pas en mesure de garantir qu'une application est ou restera compatible avec Simple AD.

Les applications tierces suivantes sont compatibles avec Simple AD :

- Microsoft Internet Information Services (IIS) sur les plateformes suivantes :
 - Windows Server 2003 R2
 - Windows Server 2008 R1
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
- Microsoft SQL Server:
 - SQL Server 2005 R2 (éditions Express, Web et Standard)
 - SQL Server 2008 R2 (éditions Express, Web et Standard)
 - SQL Server 2012 (éditions Express, Web et Standard)
 - SQL Server 2014 (éditions Express, Web et Standard)
- Microsoft SharePoint :
 - SharePoint Fondation 2010
 - SharePoint Entreprise 2010
 - SharePoint Entreprise 2013

Les clients peuvent choisir d'utiliser AWS Directory Service pour Microsoft Active Directory ([AWS Microsoft AD géré](#)) pour bénéficier d'un niveau de compatibilité supérieur basé sur Active Directory réel.

Permettre l'accès aux AWS applications et aux services pour votre Simple AD

Les utilisateurs peuvent autoriser Simple AD à autoriser AWS des applications et des services, tels qu'Amazon WorkSpaces, à accéder à votre Active Directory. Les AWS applications et services suivants peuvent être activés ou désactivés pour fonctionner avec Simple AD.

AWS application/service	En savoir plus...
Amazon WorkDocs	Pour plus d'informations, consultez le guide d'WorkDocs administration Amazon
Amazon WorkMail	Pour plus d'informations, consultez le guide de WorkMail l'administrateur Amazon .
Amazon WorkSpaces	Vous pouvez créer un Simple AD, AWS Managed Microsoft AD ou AD Connector directement à partir de WorkSpaces. Il vous suffit de lancer la configuration avancée lors de la création de votre Workspace. Pour plus d'informations, consultez le guide d'WorkSpaces administration Amazon.
AWS Management Console	Pour de plus amples informations, veuillez consulter Activation de AWS Management Console l'accès avec les informations d'identification Microsoft AD AWS gérées .

Une fois activé, vous gérez l'accès à vos annuaires dans la console de l'application ou du service auquel vous souhaitez donner accès à votre répertoire. Pour trouver les liens vers AWS les applications et les services décrits ci-dessus dans la Directory Service console, effectuez les opérations suivantes.

Pour afficher les applications et les services d'un annuaire

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaires.

2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Consultez la liste dans la section Applications et services AWS .

Pour plus d'informations sur la manière d'autoriser ou d'annuler l'autorisation d' AWS applications et de services utilisant Directory Service, consultez [Autorisation pour AWS les applications et les services utilisant Directory Service](#).

Permettre l'accès à l' AWS Management Console aide des informations d'identification Simple AD

Directory Service vous permet d'accorder aux membres de votre annuaire l'accès au AWS Management Console. Par défaut, les membres de votre répertoire n'ont accès à aucune AWS ressource. Vous attribuez des rôles IAM aux membres de votre annuaire pour leur donner accès aux différents AWS services et ressources. Le rôle IAM définit les services, les ressources et le niveau d'accès des membres de votre annuaire.

Avant que vous puissiez accorder l'accès à la console aux membres de votre annuaire, celui-ci doit disposer d'une URL d'accès. Pour plus d'informations sur la manière d'afficher les détails de l'annuaire et d'obtenir votre URL d'accès, veuillez consulter [Affichage des informations de l'annuaire Microsoft AD AWS géré](#). Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter [Création d'une URL d'accès pour AWS Managed Microsoft AD](#).

Pour plus d'informations sur la façon de créer et d'attribuer des rôles IAM aux membres de votre annuaire, veuillez consulter [Octroi aux utilisateurs et aux groupes de AWS Managed Microsoft AD d'accéder aux AWS ressources avec des rôles IAM](#).

Rubriques

- [Permettre AWS Management Console l'accès](#)
- [Désactivation AWS Management Console de l'accès](#)
- [Configuration de la durée de la session de connexion](#)

Article AWS de blog sur la sécurité connexe

- [Comment accéder à l' AWS Management Console aide de AWS Managed Microsoft AD et de vos informations d'identification locales](#)

AWS re:Post Article connexe

- [Comment puis-je accorder l'accès au AWS Management Console pour les utilisateurs d'Active Directory locaux ?](#)

Permettre AWS Management Console l'accès

Par défaut, l'accès à la console n'est activé pour aucun annuaire. Pour activer l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour activer l'accès à la console

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section AWS Management Console, choisissez Activer. L'accès à la console est désormais activé pour votre annuaire.

Important

Avant que les utilisateurs puissent se connecter à la console avec votre URL d'accès, vous devez d'abord les ajouter au rôle IAM. Pour des informations générales sur l'attribution d'utilisateurs à des rôles IAM, veuillez consulter [Affectation d'utilisateurs ou de groupes à un rôle IAM existant](#). Une fois les rôles IAM attribués, les utilisateurs peuvent accéder à la console à l'aide de votre URL d'accès. Par exemple, si l'URL d'accès à votre répertoire est example-corp.awsapps.com, l'URL permettant d'accéder à la console est. <https://example-corp.awsapps.com/console/>

Désactivation AWS Management Console de l'accès

Pour désactiver l'accès à la console pour les utilisateurs et les groupes de votre annuaire, effectuez les opérations suivantes :

Pour désactiver l'accès à la console

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.

2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section AWS Management Console, choisissez Désactiver. L'accès à la console est désormais désactivé pour votre annuaire.
5. Si des rôles IAM ont été attribués à des utilisateurs ou à des groupes dans l'annuaire, le bouton Désactiver n'est peut-être pas disponible. Dans ce cas, vous devez supprimer toutes les affectations de rôles IAM correspondant à l'annuaire avant de continuer, y compris les affectations d'utilisateurs ou de groupes de votre annuaire qui ont été supprimées et qui apparaissent sous le libellé Utilisateur supprimé ou Groupe supprimé.

Une fois que toutes les affectations de rôles IAM ont été supprimées, répétez les étapes ci-dessus.

Configuration de la durée de la session de connexion

Par défaut, les utilisateurs disposent d'une heure pour utiliser leur session après s'être correctement connectés à la console avant d'être déconnectés. Ensuite, les utilisateurs doivent se reconnecter pour démarrer la prochaine session d'une heure avant d'être à nouveau déconnectés. Vous pouvez utiliser la procédure suivante pour modifier la durée jusqu'à 12 heures par session.

Définir la durée de la session de connexion

1. Dans le panneau de navigation de la [console AWS Directory Service](#), choisissez Annuaire.
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Sous la section Applications et services AWS, choisissez AWS Management Console.
5. Dans la boîte de dialogue Gérer l'accès aux AWS ressources, choisissez Continuer.
6. Sur la page Affecter des utilisateurs et des groupes à des rôles IAM, sous Définir la durée de la session de connexion, modifiez la valeur numérotée, puis choisissez Enregistrer.

Création d'une URL d'accès pour Simple AD

Une URL d'accès est utilisée avec AWS des applications et des services, tels qu'Amazon WorkDocs, pour accéder à une page de connexion associée à votre annuaire. L'URL doit être globalement unique. Vous pouvez créer une URL d'accès pour votre annuaire en effectuant les étapes suivantes.

Warning

Une fois l'URL d'accès aux applications créée pour cet annuaire, elle ne peut pas être modifiée. Une fois votre URL d'accès créée, personne d'autre que vous ne pourra l'utiliser. Si vous supprimez votre annuaire, l'URL d'accès sera également supprimée et pourra alors être utilisée par un autre compte.

Pour créer une URL d'accès

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section Application access URL (URL d'accès à l'application), si aucune URL d'accès n'a été attribuée à l'annuaire, le bouton Créer s'affiche. Entrez un alias d'annuaire, puis choisissez Créer. Si l'erreur Entity Already Exists (entité déjà existante) est renvoyée, cela veut dire que l'alias de l'annuaire spécifié a déjà été alloué. Choisissez un autre alias et répétez cette procédure.

Votre URL d'accès est affichée au format `<alias>.awsapps.com`.

Activation de l'authentification unique

AWS Directory Service permet à vos utilisateurs d'accéder à l'annuaire à WorkDocs partir d'un ordinateur connecté à l'annuaire sans avoir à saisir leurs informations d'identification séparément.

Avant d'activer l'authentification unique, vous devez prendre des mesures supplémentaires pour permettre aux navigateurs Web de vos utilisateurs de prendre en charge l'authentification unique. Les utilisateurs peuvent avoir besoin de modifier les paramètres de leur navigateur Web pour activer l'authentification unique.

 Note

L'authentification unique fonctionne uniquement lorsqu'elle est utilisée sur un ordinateur qui est associé à l'annuaire Directory Service . Elle ne peut pas être utilisée sur les ordinateurs qui ne sont pas joints à l'annuaire.

Si votre annuaire est un annuaire AD Connector et que le compte de service AD Connector ne dispose pas de l'autorisation d'ajouter ou de supprimer son attribut de nom principal de service, vous disposez de deux options pour les étapes 5 et 6 ci-dessous :

1. Vous pouvez continuer et vous serez invité à saisir le nom d'utilisateur et le mot de passe d'un utilisateur d'annuaire qui dispose de cette autorisation pour ajouter ou supprimer l'attribut de nom principal de service sur le compte de service AD Connector. Ces informations d'identification servent uniquement à activer l'authentification unique et ne sont pas stockées par le service. Les autorisations du compte de service AD Connector ne sont pas modifiées.
2. Vous pouvez déléguer des autorisations pour permettre au compte de service AD Connector d'ajouter ou de supprimer l'attribut du nom principal du service sur lui-même. Vous pouvez exécuter les PowerShell commandes ci-dessous à partir d'un ordinateur joint au domaine à l'aide d'un compte autorisé à modifier les autorisations sur le compte de service AD Connector. La commande ci-dessous donnera au compte de service AD Connector la possibilité d'ajouter et de supprimer un attribut de nom principal de service uniquement pour lui-même.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.Guid]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
  $RootDse.SchemaNamingContext -Filter { LDAPDisplayName -eq 'servicePrincipalName' } -
  Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
  $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
```

```
# Setting ACL allowing the AD Connector service account the ability to add and remove a
Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Pour activer ou désactiver l'authentification unique avec WorkDocs

1. Dans le volet de navigation de la [console AWS Directory Service](#), sélectionnez Directories (Annuaire).
2. Sur la page Directories (Annuaire), choisissez l'ID de votre annuaire.
3. Sur la page Directory details (Détails de l'annuaire), sélectionnez l'onglet Application management (Gestion d'applications).
4. Dans la section URL d'accès à l'application, choisissez Activer pour activer l'authentification unique pour WorkDocs.

Si vous ne voyez pas le bouton Activer, vous devez d'abord créer une URL d'accès pour pouvoir afficher cette option. Pour plus d'informations sur la création d'une URL d'accès, veuillez consulter [Création d'une URL d'accès pour AWS Managed Microsoft AD](#).

5. Dans la boîte de dialogue Activer l'authentification unique pour cet annuaire, choisissez Activer. L'authentification unique est activée pour l'annuaire.
6. Si vous souhaitez désactiver ultérieurement l'authentification unique avec WorkDocs, choisissez Désactiver, puis dans la boîte de dialogue Désactiver l'authentification unique pour ce répertoire, sélectionnez à nouveau Désactiver.

Rubriques

- [Authentification unique pour IE et Chrome](#)
- [Authentification unique pour Firefox](#)

Authentification unique pour IE et Chrome

Pour permettre aux navigateurs Microsoft Internet Explorer (IE) et Google Chrome de prendre en charge l'authentification unique, les tâches suivantes doivent être effectuées sur l'ordinateur client :

- Ajoutez votre URL d'accès (par exemple, [https ://<alias>.awsapps.com](https://<alias>.awsapps.com)) à la liste des sites approuvés pour l'authentification unique.
- Activez le script actif (JavaScript).
- Autorisez l'ouverture de session automatique.
- Activez l'authentification intégrée.

Vous ou vos utilisateurs pouvez effectuer ces tâches manuellement, ou vous pouvez modifier ces paramètres à l'aide des paramètres de politique de groupe.

Rubriques

- [Mise à jour manuelle pour authentification unique sous Windows](#)
- [Mise à jour manuelle pour authentification unique sous OS X](#)
- [Paramètres de stratégie de groupe pour authentification unique](#)

Mise à jour manuelle pour authentification unique sous Windows

Pour activer manuellement l'authentification unique sur un ordinateur Windows, effectuez les étapes suivantes sur l'ordinateur client. Certains de ces paramètres sont peut-être déjà définis correctement.

Pour activer manuellement l'authentification unique pour Internet Explorer et Chrome sous Windows

1. Pour ouvrir la boîte de dialogue Propriétés Internet, sélectionnez le menu Démarrer, tapez Internet Options dans la zone de recherche, puis sélectionnez Options Internet.
2. Ajoutez votre URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
 - a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Sécurité.
 - b. Sélectionnez Intranet local, puis Sites.
 - c. Dans la boîte de dialogue Intranet local, sélectionnez Avancé.
 - d. Ajoutez votre URL d'accès à la liste des sites Web et choisissez Fermer.
 - e. Dans la boîte de dialogue Intranet local, sélectionnez OK.
3. Pour activer les scripts actifs, effectuez les opérations suivantes :
 - a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.

- b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler la page jusqu'à Scripts et sélectionnez Activer sous Scripts actifs.
 - c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
 - a. Dans l'onglet Sécurité de la boîte de dialogue Propriétés Internet, sélectionnez Personnaliser le niveau.
 - b. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, faites défiler l'écran jusqu'à Authentification utilisateur et sélectionnez Connexion automatique uniquement dans la zone Intranet sous Connexion.
 - c. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
 - d. Dans la boîte de dialogue Paramètres de sécurité - Zone intranet locale, cliquez sur OK.
5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :
 - a. Dans la boîte de dialogue Propriétés Internet, sélectionnez l'onglet Avancé.
 - b. Faites défiler la page jusqu'à Sécurité et sélectionnez Activer l'authentification Windows intégrée.
 - c. Dans la boîte de dialogue Propriétés Internet, choisissez OK.
6. Fermez puis rouvrez votre navigateur pour que ces modifications prennent effet.

Mise à jour manuelle pour authentification unique sous OS X

Pour activer manuellement l'authentification unique pour Chrome sous OS X, effectuez les étapes suivantes sur l'ordinateur client. Vous devez disposer des droits d'administrateur sur votre ordinateur pour effectuer ces opérations.

Pour activer manuellement l'authentification unique pour Chrome sous OS X

1. Ajoutez votre URL d'accès à la [AuthServerAllowlist](#) politique en exécutant la commande suivante :

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Ouvrez les Préférences système, accédez au panneau Profils et supprimez le profil Chrome Kerberos Configuration.

3. Redémarrez Chrome et ouvrez `chrome://policy` dans Chrome pour vérifier que les nouveaux paramètres sont en place.

Paramètres de stratégie de groupe pour authentification unique

L'administrateur de domaine peut implémenter des paramètres de stratégie de groupe pour apporter les modifications d'authentification unique sur les ordinateurs clients joints au domaine.

Note

Si vous gérez les navigateurs Web Chrome sur les ordinateurs de votre domaine à l'aide des politiques Chrome, vous devez y ajouter votre URL d'[AuthServerAllowlist](#) accès. Pour plus d'informations sur la définition des politiques de Chrome, veuillez consulter la section [Policy Settings in Chrome](#) (français non garanti).

Pour activer l'authentification unique pour Internet Explorer et Chrome à l'aide des paramètres de stratégie de groupe

1. Créez un nouvel objet de stratégie de groupe en procédant comme suit :
 - a. Ouvrez l'outil de gestion des stratégies de groupe, accédez à votre domaine et sélectionnez Objets de stratégie de groupe.
 - b. Dans le menu principal, choisissez Action, puis Nouveau.
 - c. Dans la boîte de dialogue New GPO, entrez un nom descriptif pour l'objet de stratégie de groupe, tel que IAM Identity Center Policy et laissez Source Starter GPO défini sur (none). Cliquez sur OK.
2. Ajoutez l'URL d'accès à la liste des sites approuvés pour l'authentification unique en effectuant les étapes suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.
 - c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.

- d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

Action

Update

Hive

HKEY_CURRENT_USER

Chemin

Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com*<alias>*

La valeur de *<alias>* est dérivée de votre URL d'accès. Si votre URL d'accès est `https://examplecorp.awsapps.com`, l'alias est `examplecorp` et la clé de registre sera `Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\examplecorp`.

Nom de la valeur

https

Type de la valeur

REG_DWORD

Données de valeur

1

3. Pour activer les scripts actifs, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.
 - c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Autoriser les scripts actifs et choisissez Modifier.

- d. Dans la boîte de dialogue Autoriser les scripts actifs, entrez les paramètres suivants et cliquez sur OK :
 - Sélectionnez le bouton radio Activé.
 - Sous Options, définissez Autoriser les scripts actifs sur Activer.
4. Pour activer la connexion automatique, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique SSO (authentification unique), puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration informatique > Politiques > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page de sécurité > Zone intranet.
 - c. Dans la liste Zone Intranet, ouvrez le menu contextuel (clic droit) pour Options de connexion et choisissez Modifier.
 - d. Dans la boîte de dialogue Options de connexion, entrez les paramètres suivants et cliquez sur OK :
 - Sélectionnez le bouton radio Activé.
 - Sous Options, définissez les options de connexion sur Connexion automatique uniquement dans la zone Intranet.
5. Pour activer l'authentification intégrée, effectuez les opérations suivantes :
 - a. Dans l'outil de gestion des politiques de groupe, accédez à votre domaine, sélectionnez Objets de stratégie de groupe, ouvrez le menu contextuel (clic droit) de votre politique IAM Identity Center, puis choisissez Modifier.
 - b. Dans l'arborescence des politiques, accédez à Configuration utilisateur > Préférences > Paramètres Windows.
 - c. Dans la liste Paramètres Windows, ouvrez le menu contextuel (clic droit) pour Registre et choisissez Nouvel élément de Registre.
 - d. Dans la boîte de dialogue Propriétés du nouveau registre, entrez les paramètres suivants et cliquez sur OK :

Action

Update

Hive

HKEY_CURRENT_USER

Chemin

Software\Microsoft\Windows\CurrentVersion\Internet Settings

Nom de la valeur

EnableNegotiate

Type de la valeur

REG_DWORD

Données de valeur

1

6. Fermez la fenêtre de l'éditeur de gestion des politiques de groupe si elle est toujours ouverte.
7. Attribuez la nouvelle politique à votre domaine en procédant comme suit :
 - a. Dans l'arborescence Gestion des politiques de groupe, ouvrez le menu contextuel (clic droit) de votre domaine et choisissez Lier un GPO existant.
 - b. Dans la liste Objets de politique de groupe, sélectionnez votre politique IAM Identity Center et cliquez sur OK.

Ces modifications prendront effet après la prochaine mise à jour de la politique de groupe sur le client, ou la prochaine fois que l'utilisateur se connectera.

Authentification unique pour Firefox

Pour autoriser le navigateur Mozilla Firefox à prendre en charge l'authentification unique, ajoutez votre URL d'accès (par exemple, [https ://<alias>.awsapps.com](https://<alias>.awsapps.com)) à la liste des sites approuvés pour l'authentification unique. Cela peut être fait manuellement ou automatiquement à l'aide d'un script.

Rubriques

- [Mise à jour manuelle pour authentification unique](#)
- [Mise à jour automatique pour authentification unique](#)

Mise à jour manuelle pour authentification unique

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox, effectuez les étapes suivantes sur l'ordinateur client.

Pour ajouter manuellement votre URL d'accès à la liste des sites approuvés dans Firefox

1. Ouvrez Firefox et ouvrez la page `about:config`.
2. Ouvrez la préférence `network.negotiate-auth.trusted-uris` et ajoutez votre URL d'accès à la liste des sites. Utilisez une virgule (,) pour séparer plusieurs entrées.

Mise à jour automatique pour authentification unique

En tant qu'administrateur de domaine, vous pouvez utiliser un script pour ajouter votre URL d'accès aux préférences utilisateur de Firefox `network.negotiate-auth.trusted-uris` sur tous les ordinateurs de votre réseau. Pour plus d'informations, rendez-vous sur <https://support.mozilla.org/en-US/questions/939037>.

Comment associer une EC2 instance Amazon à votre Simple AD

Vous pouvez facilement joindre une EC2 instance Amazon à votre domaine Active Directory lorsque l'instance est lancée. Pour de plus amples informations, veuillez consulter [Joindre une instance Amazon EC2 Windows à votre annuaire Microsoft AD Active Directory AWS géré](#). Vous pouvez également lancer une EC2 instance et la joindre à un domaine Active Directory directement depuis la Directory Service console avec [AWS Systems Manager Automation](#).

Si vous devez joindre manuellement une EC2 instance à votre domaine Active Directory, vous devez lancer l'instance dans la région et le groupe de sécurité ou le sous-réseau appropriés, puis joindre l'instance au domaine.

Pour pouvoir vous connecter à distance à ces instances, vous devez disposer d'une connectivité IP aux instances depuis le réseau à partir duquel vous vous connectez. Dans la plupart des cas, cela nécessite qu'une passerelle Internet soit attachée à votre VPC et que l'instance possède une adresse IP publique.

Rubriques

- [Joindre une instance Amazon EC2 Windows à votre répertoire Simple AD Active Directory](#)
- [Joindre une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory](#)

- [Délégation des privilèges de connexion à un annuaire pour Simple AD](#)
- [Création d'un ensemble d'options DHCP pour Simple AD](#)

Joindre une instance Amazon EC2 Windows à votre répertoire Simple AD Active Directory

Vous pouvez lancer et joindre une EC2 Windows instance Amazon à un Simple AD. Vous pouvez également joindre manuellement une EC2 Windows instance existante à un Simple AD

Seamlessly join an EC2 Windows

Pour joindre facilement un domaine à une EC2 instance, vous devez effectuer les opérations suivantes :

Prérequis

- Créez un Simple AD Pour en savoir plus, consultez [Créez votre Simple AD](#).
- Vous aurez besoin des autorisations IAM suivantes pour rejoindre facilement une EC2 Windows instance :
 - Profil d'instance IAM avec les autorisations IAM suivantes :
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - L'utilisateur qui rejoint facilement le EC2 domaine du Simple AD a besoin des autorisations IAM suivantes :
 - Directory Service Autorisations :
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Autorisations Amazon VPC :
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - EC2 Autorisations :

- "ec2:DescribeInstances"
- "ec2:DescribeImages"
- "ec2:DescribeInstanceTypes"
- "ec2:RunInstances"
- "ec2:CreateTags"
- AWS Systems Manager Autorisations :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Lorsque votre Simple AD est créé, un groupe de sécurité est créé avec des règles entrantes et sortantes. Pour en savoir plus sur ces règles et ces ports, consultez [Qu'est-ce qui est créé avec votre Simple AD](#). Pour joindre facilement un domaine à une EC2 Windows instance, le VPC sur lequel vous lancez votre instance doit autoriser les mêmes ports autorisés dans les règles entrantes et sortantes de votre groupe de sécurité Simple AD.

- Selon les paramètres de sécurité et de pare-feu de votre réseau, il peut vous être demandé d'autoriser un trafic sortant supplémentaire. Ce trafic serait destiné au protocole HTTPS (port 443) vers les points de terminaison suivants :

Point de terminaison	Rôle
ec2messages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ssm. <i>region</i> .amazonaws.com	Endpoint pour AWS Systems Manager Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .

Point de terminaison	Rôle
ssmmessages. <i>region</i> .amazonaws.com	Crée et supprime des canaux de session avec le service Session Manager. Pour plus d'informations, consultez Points de terminaison et quotas AWS Systems Manager .
ds. <i>region</i> .amazonaws.com	Endpoint pour Directory Service. Pour de plus amples informations, veuillez consulter Disponibilité de la région pour Directory Service .

- Nous vous recommandons d'utiliser un serveur DNS qui résoudra votre nom de domaine Simple AD. Pour ce faire, vous pouvez créer un jeu d'options DHCP. Pour plus d'informations, consultez [Création d'un ensemble d'options DHCP pour Simple AD](#).
 - Si vous choisissez de ne pas créer de jeu d'options DHCP, vos serveurs DNS seront statiques et configurés par votre Simple AD.
1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
 2. Dans la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
 3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
 4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Windows.
 5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.
 6. Dans la section Application and OS Image (Amazon Machine Image) [Image de l'application et du système d'exploitation (Amazon Machine Image)], sélectionnez Windows dans le volet Quick Start (Démarrage rapide). Vous pouvez modifier Windows Amazon Machine Image (AMI) dans la liste déroulante Amazon Machine Image (AMI).
 7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.

8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante.
 - a. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés.
 - b. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée.
 - c. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez .pem. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez .ppk.
 - d. Choisissez Créer une paire de clés.
 - e. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

**Important**

C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.
10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.

14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

 Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour l'IAM instance profile (profil d'instance IAM), vous pouvez sélectionner un profil d'instance IAM existant ou en créer un nouveau. Sélectionnez un profil d'instance IAM SSMDirectory ServiceAccess auquel sont associées les politiques AWS gérées Amazon SSManaged InstanceCore et Amazon dans la liste déroulante des profils d'instance IAM. Pour en créer un nouveau, choisissez Créer un nouveau lien de profil IAM, puis procédez comme suit :
 1. Choisissez Créer un rôle.
 2. Sous Select trusted entity (Sélectionner une entité approuvée), choisissez service AWS .
 3. Sous Use case (Cas d'utilisation), choisissez EC2.
 4. Sous Ajouter des autorisations, dans la liste des politiques, sélectionnez les SSMDirectory ServiceAccess politiques Amazon SSManaged InstanceCore et Amazon. Pour filtrer la liste, tapez **SSM** dans la zone de recherche. Choisissez Suivant.

 Note

Amazon SSMDirectory ServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. Amazon SSMManged InstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section [Create an IAM instance profile for Systems Manager](#) (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

5. Sur la page Name, review, and create (Nommer, vérifier et créer), saisissez un Role name (Nom du rôle). Vous aurez besoin de ce nom de rôle pour l'associer à l' EC2instance.
 6. (Facultatif) Vous pouvez fournir une description du profil d'instance IAM dans le champ Description.
 7. Choisissez Créer un rôle.
 8. Revenez à la page Launch an instance (Lancer une instance) et choisissez l'icône d'actualisation à côté du profil d'instance IAM. Votre nouveau profil d'instance IAM doit être visible dans la liste déroulante des IAM instance profile (profil d'instance IAM). Choisissez le nouveau profil et laissez le reste de paramètres avec leurs valeurs par défaut.
16. Choisissez Launch instance (Lancer une instance).

Manually join an EC2 Windows

Pour joindre manuellement une instance Amazon EC2 Windows existante à un répertoire Simple AD Active Directory, l'instance doit être lancée à l'aide des paramètres spécifiés dans [Joindre une instance Amazon EC2 Windows à votre répertoire Simple AD Active Directory](#).

Vous aurez besoin des adresses IP des serveurs DNS Simple AD. Ces informations se trouvent sous Directory Services (Services d'annuaire) > Directories (Annuaire) > le lien Directory ID (ID de l'annuaire) de votre annuaire > Directory details (Détails de l'annuaire) puis les sections Networking & Security Réseau et sécurité.

The screenshot shows the AWS Directory Service console. On the left, the 'Directory Service' sidebar is open, with 'Directories' selected under 'Active Directory'. The main content area shows the details for directory 'd-1234567890'. The 'Directory details' section is highlighted with a red box and contains the following information:

Property	Value
Directory type	Microsoft AD
Edition	Standard
Operating system version	Windows Server 2019
Directory DNS name	corp.example.com
Directory NetBIOS name	corp
Directory administration EC2 instance(s)	-

Below the details, there are tabs for 'Networking & security', 'Scale & share', 'Application management', and 'Maintenance'. The 'Networking & security' tab is selected, and the 'Networking details' section is highlighted with a red box. It shows the VPC, Subnets, and Availability zones. The 'DNS address' is highlighted with a red box and lists the following addresses:

DNS address
192.0.2.1
198.51.100.1

Pour joindre une instance Windows à un répertoire Simple AD Active Directory

1. Connectez-vous à l'instance à l'aide d'un client RDP (Remote Desktop Protocol).
2. Ouvrez la boîte de dialogue IPv4 des propriétés TCP/ sur l'instance.
 - a. Ouvrez Network Connections (Connexions réseau).

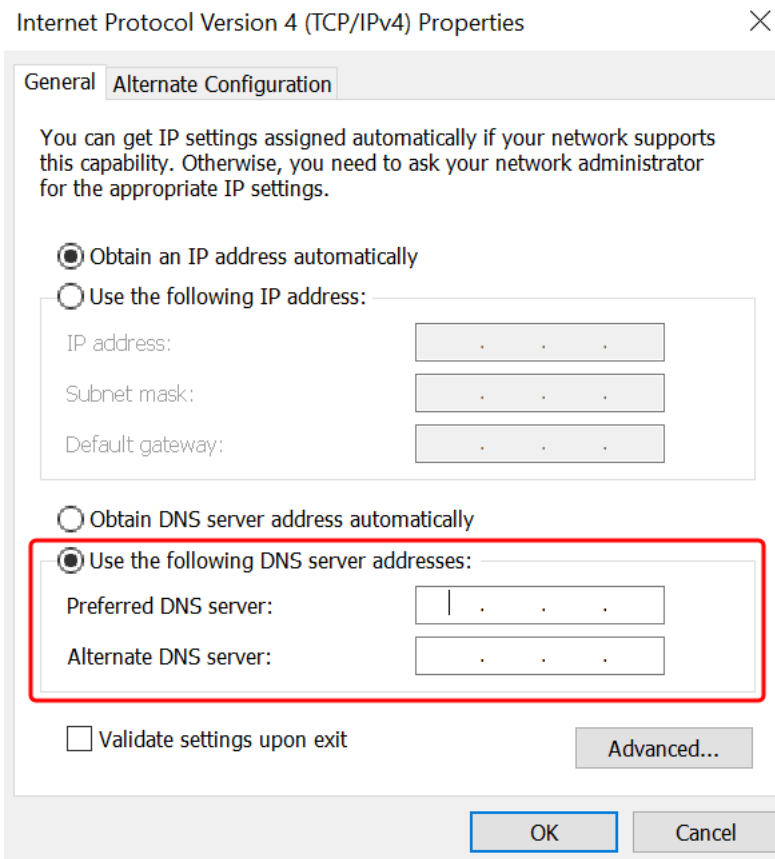
Tip

Vous pouvez ouvrir Network Connections (Connexions réseau) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. Ouvrez le menu contextuel (clic droit) pour toute connexion de réseau active, puis choisissez Properties (Propriétés).
- c. Dans la boîte de dialogue des propriétés de connexion, ouvrez (double-cliquez) Internet Protocol version 4.

3. Sélectionnez Utiliser les adresses de serveur DNS suivantes, remplacez les adresses du serveur DNS préféré et du serveur DNS alternatif par les adresses IP de vos serveurs DNS fournis par Simple AD, puis cliquez sur OK.



4. Ouvrez la boîte de dialogue System Properties (Propriétés système) de l'instance, sélectionnez l'onglet Computer Name (Nom de l'ordinateur), puis choisissez Change (Modifier).

i Tip

Vous pouvez ouvrir la boîte de dialogue System Properties (Propriétés du système) directement en exécutant ce qui suit à partir d'une invite de commande sur l'instance.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. Dans le champ Membre de, sélectionnez Domaine, entrez le nom complet de votre Simple AD Active Directory, puis cliquez sur OK.
6. Lorsque vous êtes invité à saisir le nom et le mot de passe de l'administrateur du domaine, entrez le nom d'utilisateur et le mot de passe d'un compte doté de privilèges de connexion

au domaine. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour Simple AD](#).

 Note

Vous pouvez saisir le nom complet de votre domaine ou le nom NetBIOS, suivi d'une barre oblique inverse (\), puis du nom d'utilisateur. Le nom d'utilisateur serait Administrator. Par exemple, **corp.example.com\administrator** ou **corp \administrator**.

7. Après avoir reçu le message de bienvenue dans le domaine, redémarrez l'instance pour que les modifications prennent effet.

Maintenant que votre instance a été jointe au domaine Simple AD Active Directory, vous pouvez vous connecter à distance à cette instance et installer des utilitaires pour gérer l'annuaire, tels que l'ajout d'utilisateurs et de groupes. Les outils d'administration Active Directory peuvent être utilisés pour créer des utilisateurs et des groupes. Pour de plus amples informations, veuillez consulter [Installation des outils d'administration Active Directory pour Simple AD](#).

Joindre une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory

Vous pouvez lancer et joindre une instance Amazon EC2 Linux à votre Simple AD dans le AWS Management Console. Vous pouvez également associer manuellement une instance EC2 Linux à votre Simple AD.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

 Note

Les distributions antérieures à Ubuntu 14 et à Red Hat Enterprise Linux 7 et 8 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Méthodes pour joindre un domaine à une instance EC2 Linux :

- [Associez facilement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory](#)
- [Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory](#)

Associez facilement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory

Cette procédure permet de joindre facilement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory.

Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

 Note

Les distributions antérieures à Ubuntu 14 et à Red Hat Enterprise Linux 7 et 8 ne prennent pas en charge la fonctionnalité de jonction de domaine transparente.

Prérequis

Avant de pouvoir configurer une jointure de domaine fluide à une instance Linux, vous devez suivre les procédures décrites dans cette section.

Sélectionnez votre compte de service de jonction transparente à un domaine

Vous pouvez joindre de manière transparente des ordinateurs Linux à votre domaine Simple AD. Pour ce faire, vous devez créer un compte utilisateur autorisé à créer un compte d'ordinateur pour joindre les ordinateurs au domaine. Bien que les Administrateurs de domaine ou les membres d'autres groupes puissent disposer de privilèges suffisants pour joindre des ordinateurs au domaine, nous vous le déconseillons. À titre de bonne pratique, nous vous recommandons d'utiliser un compte de service disposant des privilèges minimum nécessaires pour joindre les ordinateurs au domaine.

Pour plus d'informations sur le traitement et la délégation des autorisations à votre compte de service pour la création de comptes d'ordinateur, veuillez consulter [Délégation de privilèges à votre compte de service](#).

Créer les secrets pour stocker le compte de service de domaine

Vous pouvez l'utiliser AWS Secrets Manager pour stocker le compte de service de domaine. Pour plus d'informations, voir [Création d'un AWS Secrets Manager secret](#).

Note

Des frais sont associés à Secrets Manager. Pour plus d'informations, voir [Tarification](#) dans le guide de AWS Secrets Manager l'utilisateur.

Pour créer des secrets et stocker les informations du compte de service de domaine

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sur la page Store a new secret (Stocker un nouveau secret), procédez comme suit :
 - a. Sous Type de secret, sélectionnez Autre type de secret.
 - b. Sous Paires clé/valeur, procédez comme suit :
 - i. Dans la première case, saisissez **awsSeamlessDomainUsername**. Sur la même ligne, dans la case suivante, entrez le nom d'utilisateur de votre compte de service. Par exemple, si vous avez déjà utilisé la PowerShell commande, le nom du compte de service serait **awsSeamlessDomain**.

Note

Vous devez saisir **awsSeamlessDomainUsername** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

The screenshot shows the AWS Secrets Manager console interface. The breadcrumb navigation is [AWS Secrets Manager](#) > [Secrets](#) > Store a new secret. The left sidebar shows the steps: Step 1: Choose secret type (active), Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main content area is titled 'Choose secret type'. It has three sections: 'Secret type' with four radio button options (Credentials for Amazon RDS database, Credentials for Amazon DocumentDB database, Credentials for Amazon Redshift cluster, and Other type of secret), 'Key/value pairs' with a table, and 'Encryption key' with a dropdown menu. The 'Other type of secret' option is selected and highlighted with a red box. The 'Key/value pairs' table has two columns: 'Key/value' and 'Plaintext'. The first row has 'awsSeamlessDomainUsername' in the 'Key/value' column, which is also highlighted with a red box. Below the table is an '+ Add row' button. The 'Encryption key' section shows 'aws/secretsmanager' selected in the dropdown. At the bottom right are 'Cancel' and 'Next' buttons.

Key/value	Plaintext
awsSeamlessDomainUsername	

- ii. Choisissez Add row (Ajouter une ligne).
- iii. Sur la nouvelle ligne, dans la première case, saisissez **awsSeamlessDomainPassword**. Sur la même ligne, dans la case suivante, saisissez le mot de passe de votre compte de service.

 Note

Vous devez saisir **awsSeamlessDomainPassword** exactement tel quel. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

- iv. Sous Clé de chiffrement, laissez la valeur par défaut `aws/secretsmanager`. AWS Secrets Manager chiffre toujours le secret lorsque vous choisissez cette option. Vous pouvez également choisir une clé que vous avez créée.
 - v. Choisissez Suivant.
4. Sous Nom secret, entrez un nom secret qui inclut votre identifiant de répertoire en utilisant le format suivant, en le **`d-xxxxxxxx`** remplaçant par votre identifiant de répertoire :

```
aws/directory-services/d-xxxxxxxx/seamless-domain-join
```

Cela servira à récupérer des secrets dans l'application.

 Note

Vous devez le saisir **`aws/directory-services/d-xxxxxxxx/seamless-domain-join`** exactement tel quel, mais le **`d-xxxxxxxx`** remplacer par votre identifiant de répertoire. Assurez-vous qu'il n'y a pas d'espaces au début ni à la fin. Sinon, la jonction de domaine échouera.

Services Search [Alt+S]

AWS Secrets Manager > Secrets > Store a new secret

Step 1
[Choose secret type](#)

Step 2
Configure secret

Step 3 - optional
Configure rotation

Step 4
Review

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

`aws/directory-services/d-xxxxxxx/seamless-domain-join`

Secret name must contain only alphanumeric characters and the characters `/_+:@-`.

Description - optional

`Access to MYSQL prod database for my AppBeta`

Maximum 250 characters.

Tags - optional

No tags associated with the secret.

[Add](#)

Resource permissions - optional [Info](#)

Add or edit a resource policy to access secrets across AWS accounts.

[Edit permissions](#)

► Replicate secret - optional

Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

[Cancel](#) [Previous](#) [Next](#)

5. Laissez le reste des paramètres définis par défaut, puis choisissez Next (Suivant).
6. Sous Configure automatic rotation (Configurer la rotation automatique), choisissez Disable automatic rotation (Désactiver la rotation automatique), puis cliquez sur Next (Suivant).

Vous pouvez activer la rotation pour ce secret une fois que vous l'avez enregistré.

7. Vérifiez les paramètres, puis choisissez Store (Stocker) pour enregistrer vos modifications. La console Secrets Manager vous redirige à la liste des secrets de votre compte, où votre nouveau secret est désormais inclus.
8. Choisissez le nom du secret que vous venez de créer dans la liste et prenez note de la valeur de l'ARN secret. Vous en aurez besoin pour la section suivante.

Activer la rotation pour le secret du compte de service de domaine

Nous vous recommandons d'alterner régulièrement les secrets afin d'améliorer votre niveau de sécurité.

Pour activer la rotation pour le secret du compte de service de domaine

- Suivez les instructions de la section [Configurer la rotation automatique pour les AWS Secrets Manager secrets](#) dans le Guide de AWS Secrets Manager l'utilisateur.

Pour l'étape 5, utilisez le modèle de rotation des [informations d'identification Microsoft Active Directory](#) dans le guide de AWS Secrets Manager l'utilisateur.

Pour obtenir de l'aide, consultez la section [Résolution des problèmes AWS Secrets Manager de rotation](#) dans le Guide de AWS Secrets Manager l'utilisateur.

Créez le rôle et la politique IAM requis

Suivez les étapes préalables suivantes pour créer une politique personnalisée qui autorise un accès en lecture seule à votre secret de jonction de domaine transparent Secrets Manager (que vous avez créé précédemment) et pour créer un nouveau rôle Linux EC2 DomainJoin IAM.

Créer la politique de lecture IAM Secrets Manager

Utilisez la console IAM pour créer une politique qui accorde un accès en lecture seule à votre secret Secrets Manager.

Pour créer la politique de lecture IAM Secrets Manager

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez ensuite la console IAM à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation, Gestion des accès, sélectionnez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez-le ensuite dans la zone de texte JSON.

 Note

Assurez-vous de remplacer l'ARN de la région et de la ressource par la région et l'ARN réels du secret que vous avez créé précédemment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxx:secret:aws/directory-
services/d-xxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. Lorsque vous avez terminé, choisissez Next. Le programme de validation des politiques signale les éventuelles erreurs de syntaxe. Pour plus d'informations, veuillez consulter la section [Validating IAM policies](#) (français non garanti).
6. Sur la page Review policy (Réviser la politique), saisissez un nom pour la politique, tel que **SM-Secret-Linux-DJ-d-xxxxxxx-Read**. Vérifiez la section Summary (Récapitulatif) pour voir les autorisations accordées par votre politique. Sélectionnez Create Policy (Créer une politique) pour enregistrer vos changements. La nouvelle politique s'affiche dans la liste des politiques gérées et est prête à être attachée à une identité.

 Note

Nous vous recommandons de créer une politique par secret. Cela garantit que les instances n'ont accès qu'au secret approprié et minimise les répercussions si une instance est compromise.

Création du EC2 DomainJoin rôle Linux

Vous utilisez la console IAM pour créer le rôle que vous utiliserez pour joindre un domaine à votre EC2 instance Linux.

Pour créer le EC2 DomainJoin rôle Linux

1. Connectez-vous au en AWS Management Console tant qu'utilisateur autorisé à créer des politiques IAM. Ouvrez ensuite la console IAM à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
3. Dans le panneau de contenu, sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS .
5. Sous Cas d'utilisation, choisissez EC2, puis cliquez sur Suivant.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected from the dropdown. The 'EC2' use case is highlighted, indicating it allows EC2 instances to call AWS services on your behalf.

6. Pour Filter policies (Filtrer les politiques), procédez comme suit :
 - a. Saisissez **AmazonSSMManagedInstanceCore**. Cochez ensuite la case correspondant à cet élément de la liste.
 - b. Saisissez **AmazonSSMDirectoryServiceAccess**. Cochez ensuite la case correspondant à cet élément de la liste.
 - c. Saisissez **SM-Secret-Linux-DJ-d-xxxxxxxxxxx-Read** (ou le nom de la politique que vous avez créée dans la procédure précédente). Cochez ensuite la case correspondant à cet élément de la liste.

- d. Après avoir ajouté les trois politiques répertoriées ci-dessus, sélectionnez Créer un rôle.

 Note

Amazon SSMDirectory ServiceAccess fournit les autorisations nécessaires pour joindre des instances à un Active Directory géré par Directory Service. Amazon SSMManged InstanceCore fournit les autorisations minimales nécessaires pour utiliser le AWS Systems Manager service. Pour plus d'informations sur la création d'un rôle doté de ces autorisations, ainsi que sur les autres autorisations et politiques que vous pouvez attribuer à votre rôle IAM, veuillez consulter la section [Create an IAM instance profile for Systems Manager](#) (français non garanti) dans le Guide de l'utilisateur AWS Systems Manager .

7. Entrez un nom pour votre nouveau rôle, par exemple un autre nom que vous préférez dans le champ Nom du rôle. **LinuxEC2DomainJoin**
8. (Facultatif) Pour Role description (Description du rôle), entrez une description.
9. (Facultatif) Choisissez Ajouter une nouvelle balise à l'étape 3 : Ajouter des balises pour ajouter des balises. Les paires clé-valeur de balise sont utilisées pour organiser, suivre ou contrôler l'accès pour ce rôle.
10. Choisissez Créer un rôle.

Associez facilement une instance Linux à votre répertoire Simple AD Active Directory

Pour rejoindre facilement votre instance Linux

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le sélecteur de région de la barre de navigation, choisissez le même répertoire Région AWS que le répertoire existant.
3. Sur le EC2 tableau de bord, dans la section Launch instance, choisissez Launch instance.
4. Sur la page Lancer une instance, dans la section Nom et balises, entrez le nom que vous souhaitez utiliser pour votre EC2 instance Linux.
5. (Facultatif) Choisissez Ajouter des balises supplémentaires pour ajouter une ou plusieurs paires clé-valeur de balise afin d'organiser, de suivre ou de contrôler l'accès à cette EC2 instance.

6. Dans la section Image de l'application et du système d'exploitation (Amazon Machine Image), choisissez l'AMI Linux que vous souhaitez lancer.

 Note

L'AMI utilisée doit avoir la version 2.3.1644.0 ou supérieure AWS Systems Manager (agent SSM). Pour vérifier la version de l'agent SSM installée dans votre AMI en lançant une instance à partir de cette AMI, veuillez consulter [Getting the currently installed SSM Agent version](#) (français non garanti). Si vous devez mettre à niveau l'agent SSM, consultez la section [Installation et configuration de l'agent SSM sur des EC2 instances pour Linux](#).

SSM utilise le `aws:domainJoin` plugin pour joindre une instance Linux à un domaine Active Directory. Le plugin remplace le nom d'hôte des instances Linux par le format EC2 AMAZ-**XXXXXXX**. Pour plus d'informations sur `aws:domainJoin`, consultez la [référence du plug-in du document de AWS Systems Manager commande](#) dans le guide de AWS Systems Manager l'utilisateur.

7. Dans la section Type d'instance, choisissez le type d'instance que vous souhaitez utiliser dans la liste déroulante Type d'instance.
8. Dans la section Paire de clés (connexion), vous pouvez choisir de créer une nouvelle paire de clés ou choisir une paire de clés existante. Pour créer une nouvelle paire de clés, choisissez Créer une paire de clés. Entrez le nom de la paire de clés et sélectionnez une option pour le type de paire de clés et le format de fichier de clé privée. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez .pem. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez .ppk. Choisissez Créer une paire de clés. Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Enregistrez le fichier de clé privée en lieu sûr.

 Important

C'est votre seule occasion d'enregistrer le fichier de clé privée.

9. Sur la page Lancer une instance, dans la section Paramètres réseau, choisissez Modifier. Choisissez le VPC dans lequel votre répertoire a été créé dans la liste déroulante VPC obligatoire.

10. Choisissez l'un des sous-réseaux publics de votre VPC dans la liste déroulante Sous-réseau. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.

Pour obtenir plus d'informations sur la manière de se connecter à une passerelle Internet, veuillez consulter la section [Connect to the internet using an internet gateway](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

11. Sous Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

Pour plus d'informations sur l'adressage IP public et privé, consultez la section [Adressage IP des EC2 instances Amazon](#) dans le guide de EC2 l'utilisateur Amazon.

12. Pour les paramètres Firewall (security groups) [Pare-feu (groupes de sécurité)], vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
13. Pour les paramètres Configure storage (Configurer le stockage), vous pouvez utiliser les paramètres par défaut ou les modifier selon vos besoins.
14. Choisissez la section Advanced details (Détails avancés), puis sélectionnez votre domaine dans la liste déroulante Domain join directory (Annuaire de jonction de domaines).

Note

Après avoir choisi le répertoire de jointure du domaine, vous pouvez voir :

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

Cette erreur se produit si l'assistant de EC2 lancement identifie un document SSM existant présentant des propriétés inattendues. Vous pouvez effectuer l'une des actions suivantes :

- Si vous avez déjà modifié le document SSM et que les propriétés sont attendues, choisissez Fermer et lancez l' EC2 instance sans aucune modification.
- Cliquez sur le lien Supprimer le document SSM existant ici pour supprimer le document SSM. Cela permettra de créer un document SSM avec les propriétés

correctes. Le document SSM sera automatiquement créé lorsque vous lancerez l' EC2 instance.

15. Pour le profil d'instance IAM, choisissez le rôle IAM que vous avez créé précédemment dans la section Conditions préalables Étape 2 : Création du rôle Linux. EC2 DomainJoin
16. Choisissez Launch instance (Lancer une instance).

Note

Si vous effectuez une jonction de domaine transparente avec SUSE Linux, un redémarrage est nécessaire pour que les authentifications fonctionnent. Pour redémarrer SUSE depuis le terminal Linux, tapez `sudo reboot`.

Joindre manuellement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory

Outre les instances Amazon EC2 Windows, vous pouvez également joindre certaines instances Amazon EC2 Linux à votre répertoire Simple AD Active Directory. Les distributions et les versions d'instance Linux suivantes sont prises en charge :

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64 bits x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64 bits x86)
- Ubuntu Server 18.04 LTS et Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- Serveur SUSE Linux Enterprise 15 SP1

Note

D'autres distributions et versions Linux peuvent fonctionner, mais n'ont pas été testées.

Prérequis

Avant de pouvoir joindre une instance Amazon Linux, CentOS, Red Hat ou Ubuntu à votre annuaire, l'instance doit d'abord être lancée comme indiqué dans [Associez facilement une instance Amazon EC2 Linux à votre répertoire Simple AD Active Directory](#).

Important

Certaines des procédures suivantes peuvent rendre votre instance inaccessible ou non utilisable si elles ne sont pas effectuées correctement. Par conséquent, nous vous conseillons vivement de faire une sauvegarde ou de prendre un instantané de votre instance avant d'exécuter ces procédures.

Pour joindre une instance Linux à votre annuaire

Suivez les étapes pour votre instance Linux spécifique à l'aide de l'un des onglets suivants :

Amazon Linux

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance Amazon Linux - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les paquets Amazon Linux requis sur votre instance Linux.

Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

Note

Pour vous aider à déterminer la version d'Amazon Linux que vous utilisez, consultez la section [Identification des images Amazon Linux](#) dans le guide de EC2 l'utilisateur Amazon pour les instances Linux.

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un compte du *example.com* domaine doté de privilèges de connexion au domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.

a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- b. Définissez le paramètre PasswordAuthentication sur yes.

```
PasswordAuthentication yes
```

- c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

- a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

- b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

CentOS

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que votre instance CentOS 7 est à jour.

```
sudo yum -y update
```

4. Installez les paquets CentOS 7 obligatoires sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés. Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un compte du *example.com* domaine doté de privilèges de connexion au domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.
 - a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Red hat

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que l'instance Red Hat - 64 bits est à jour.

```
sudo yum -y update
```

4. Installez les packages Red Hat obligatoires sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés. Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -v -U join_account example.com --install=/  
  
join_account
```

AMAccountNom s d'un compte du *example.com* domaine doté de privilèges d'adhésion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.

```
...  
* Successfully enrolled machine in realm
```

6. Définissez le service SSH pour permettre l'authentification du mot de passe.
 - a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

7. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste sudoers en effectuant les étapes suivantes :

a. Ouvrez le fichier sudoers avec la commande suivante :

```
sudo visudo
```

b. Ajoutez les éléments suivants en bas du fichier sudoers et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « \<space> » pour créer le caractère d'espace Linux.)

Ubuntu

1. Connectez-vous à l'instance à l'aide d'un client SSH.
2. Configurez l'instance Linux pour utiliser les adresses IP des serveurs DNS Directory Service fournis. Pour cela, vous pouvez la configurer dans le jeu d'options DHCP lié au VPC ou la définir manuellement sur l'instance. Si vous souhaitez le configurer manuellement, consultez l'article [Comment attribuer un serveur DNS statique à une EC2 instance Amazon privée](#) dans le centre de AWS connaissances pour obtenir des conseils sur la configuration du serveur DNS persistant pour votre distribution et votre version Linux spécifiques.
3. Assurez-vous que l'instance Ubuntu - 64 bits est à jour.

```
sudo apt-get update
```

```
sudo apt-get -y upgrade
```

4. Installez les packages Ubuntu obligatoires sur votre instance Linux.

 Note

Certains de ces packages peuvent être déjà installés.

Au fur et à mesure que vous installez les packages, plusieurs fenêtres de configuration contextuelles peuvent apparaître. Vous pouvez généralement laisser les champs de ces écrans vides.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Désactivez la résolution DNS inversée et définissez le domaine par défaut sur le nom de domaine complet de votre domaine. Les instances Ubuntu doivent pouvoir faire l'objet d'une résolution inverse dans le DNS pour qu'un domaine puisse fonctionner. Sinon, vous devez désactiver la résolution DNS inverse dans `/etc/krb5.conf` de la façon suivante :

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Joignez l'instance à l'annuaire avec la commande suivante.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

AMAccountNom s d'un compte du *example.com* domaine doté de privilèges d'adhésion à un domaine. À l'invite, saisissez le mot de passe du compte. Pour obtenir plus d'informations sur la délégation de ces privilèges, veuillez consulter [Délégation des privilèges de connexion à un annuaire pour AWS Managed Microsoft AD](#).

example.com

Nom DNS complet de votre annuaire.


```
...  
* Successfully enrolled machine in realm
```

7. Définissez le service SSH pour permettre l'authentification du mot de passe.

- a. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte.

```
sudo vi /etc/ssh/sshd_config
```

- b. Définissez le paramètre `PasswordAuthentication` sur `yes`.

```
PasswordAuthentication yes
```

- c. Redémarrez le service SSH.

```
sudo systemctl restart sshd.service
```

Autrement :

```
sudo service sshd restart
```

8. Une fois que l'instance a redémarré, connectez-vous y avec un client SSH et ajoutez le groupe d'administrateurs du domaine à la liste `sudoers` en effectuant les étapes suivantes :

- a. Ouvrez le fichier `sudoers` avec la commande suivante :

```
sudo visudo
```

- b. Ajoutez les éléments suivants en bas du fichier `sudoers` et enregistrez-le.

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'exemple ci-dessus utilise « `\<space>` » pour créer le caractère d'espace Linux.)

 Note

Lors de l'utilisation de Simple AD, si vous créez un compte d'utilisateur sur une instance Linux avec l'option « Force user to change password at first login », cet utilisateur ne pourra pas

modifier initialement son mot de passe à l'aide de la commande `kpasswd`. Pour modifier le mot de passe la première fois, un administrateur de domaine doit mettre à jour le mot de passe utilisateur à l'aide des outils de gestion Active Directory.

Gérer des comptes à partir d'une instance Linux

Pour gérer des comptes dans Simple AD à partir d'une instance Linux, vous devez mettre à jour des fichiers de configuration spécifiques sur votre instance Linux comme suit :

1. Définissez `krb5_use_kdcinfo` sur `False` dans le fichier `/etc/sss/sss.conf`. Exemples :

```
[domain/example.com]
krb5_use_kdcinfo = False
```

2. Pour que la configuration soit appliquée, vous devez redémarrer le service `sssd` :

```
$ sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
$ sudo service sssd start
```

3. Si vous allez gérer les utilisateurs à partir d'une instance Linux CentOS, vous devez également modifier le fichier `/etc/smb.conf` pour inclure :

```
[global]
workgroup = EXAMPLE.COM
realm = EXAMPLE.COM
netbios name = EXAMPLE
security = ads
```

Restriction de l'accès de connexion à un compte

Comme tous les comptes sont définis dans Active Directory, par défaut, tous les utilisateurs de l'annuaire peuvent se connecter à l'instance. Vous pouvez autoriser uniquement certains utilisateurs à se connecter à l'instance à l'aide de la commande `ad_access_filter` dans `sss.conf`. Exemples :

```
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

memberOf

Indique que les utilisateurs ne peuvent accéder qu'à l'instance s'ils sont membres d'un groupe spécifique.

cn

Nom canonique du groupe disposant d'un accès. Dans cet exemple, le nom du groupe est *admins*.

ou

Il s'agit de l'unité d'organisation dans laquelle se trouve le groupe ci-dessus. Dans cet exemple, l'OU est *Testou*.

dc

Il s'agit du composant de domaine de votre domaine. Dans cet exemple, *example*.

dc

Il s'agit d'un composant de domaine supplémentaire. Dans cet exemple, *com*.

Vous devez ajouter manuellement `ad_access_filter` à votre `/etc/sss/sss.conf`.

Ouvrez le fichier `/etc/sss/sss.conf` dans un éditeur de texte.

```
sudo vi /etc/sss/sss.conf
```

Une fois l'opération effectuée, votre commande `sss.conf` pourrait ressembler à ce qui suit :

```
[sss]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
```

```
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Pour que la configuration soit appliquée, vous devez redémarrer le service sssd :

```
sudo systemctl restart sssd.service
```

Vous pouvez également utiliser :

```
sudo service sssd restart
```

Cartographie des identifiants

Le mappage des identifiants peut être effectué par deux méthodes afin de maintenir une expérience unifiée entre l'identifiant utilisateur (UID) UNIX/Linux et l'identifiant de groupe (GID) et les identités Windows et Active Directory Security Identifier (SID). Ces méthodes sont les suivantes :

1. Centralisée
2. Distribué

Note

Le mappage centralisé de l'identité utilisateur dans Active Directory nécessite une interface de système d'exploitation portable ou POSIX.

Cartographie centralisée de l'identité des utilisateurs

Active Directory ou un autre service LDAP (Lightweight Directory Access Protocol) fournit un UID et un GID aux utilisateurs de Linux. Dans Active Directory, ces identifiants sont stockés dans les attributs des utilisateurs si l'extension POSIX est configurée :

- UID - Le nom d'utilisateur Linux (chaîne)

- Numéro UID : numéro d'identification utilisateur Linux (entier)
- Numéro GID : numéro d'identification du groupe Linux (entier)

Pour configurer une instance Linux afin d'utiliser l'UID et le GID d'Active Directory, définissez-les `ldap_id_mapping = False` dans le fichier `sssd.conf`. Avant de définir cette valeur, vérifiez que vous avez ajouté un UID, un numéro UID et un numéro GID aux utilisateurs et aux groupes dans Active Directory.

Cartographie distribuée de l'identité des utilisateurs

Si Active Directory ne possède pas l'extension POSIX ou si vous choisissez de ne pas gérer de manière centralisée le mappage des identités, Linux peut calculer les valeurs UID et GID. Linux utilise l'identifiant de sécurité (SID) unique de l'utilisateur pour garantir la cohérence.

Pour configurer le mappage d'ID utilisateur distribué, définissez-le `ldap_id_mapping = True` dans le fichier `sssd.conf`.

Problèmes courants

Si vous le configurez `ldap_id_mapping = False`, le démarrage du service SSSD échouera parfois. La raison de cet échec est due au fait que les modifications UIDs ne sont pas prises en charge. Nous vous recommandons de supprimer le cache SSSD chaque fois que vous passez du mappage d'ID aux attributs POSIX ou des attributs POSIX au mappage d'ID. Pour plus de détails sur le mappage des identifiants et les paramètres `ldap_id_mapping`, consultez la page de manuel `sssd-ldap (8)` sur la ligne de commande Linux.

Connect à l'instance Linux

Lorsqu'un utilisateur se connecte à l'instance à l'aide d'un client SSH, il est invité à indiquer son nom d'utilisateur. L'utilisateur peut entrer le nom d'utilisateur au format `username@example.com` ou au format `EXAMPLE\username`. La réponse ressemblera à la suivante, selon la distribution Linux que vous utilisez :

Amazon Linux, Red Hat Enterprise Linux et CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:

- zypper command for package management
- yast command for configuration management

Management and Config: <https://www.suse.com/suse-in-the-cloud-basics>

Documentation: <https://www.suse.com/documentation/sles-15/>

Forum: <https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud>

Have a lot of fun...

Ubuntu Linux

login as: admin@example.com

admin@example.com@10.24.34.0's password:

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

System information as of Sat Apr 18 22:03:35 UTC 2020

System load:	0.01	Processes:	102
Usage of /:	18.6% of 7.69GB	Users logged in:	2
Memory usage:	16%	IP address for eth0:	10.24.34.1
Swap usage:	0%		

Délégation des privilèges de connexion à un annuaire pour Simple AD

Pour joindre un ordinateur à votre annuaire, vous devez disposer d'un compte doté des privilèges de jonction des ordinateurs à l'annuaire.

Avec Simple AD, les membres du groupe Administrateurs de domaine ont les privilèges nécessaires pour joindre les ordinateurs à l'annuaire.

Cependant, en tant que bonne pratique, vous devez utiliser un compte disposant uniquement des privilèges minimum nécessaires. La procédure suivante montre comment créer un nouveau groupe

appelé **Joiners** et déléguer les privilèges à ce groupe qui sont nécessaires pour joindre des ordinateurs à l'annuaire.

Vous devez effectuer cette procédure sur un ordinateur qui est joint à votre annuaire et qui dispose du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Vous devez également être connecté en tant qu'administrateur de domaine.

Pour déléguer des privilèges de jonction pour Simple AD

1. Ouvrez Utilisateurs et ordinateurs Active Directory, puis sélectionnez votre domaine dans l'arborescence de navigation.
2. Dans l'arborescence de navigation de gauche, ouvrez le menu contextuel (clic droit) Utilisateurs, choisissez Nouveau, puis Groupe.
3. Dans la zone Nouvel objet - groupe, saisissez ce qui suit et choisissez OK.
 - Pour Nom du groupe, tapez **Joiners**.
 - Pour Étendue du groupe, choisissez Global.
 - Pour Type de groupe, choisissez Sécurité.
4. Dans l'arborescence de navigation, sélectionnez la racine de votre domaine. À partir du menu Action, choisissez Déléguer le contrôle.
5. Sur la page Delegation of Control Wizard, choisissez Next, puis choisissez Add.
6. Dans la zone Select Users, Computers, or Groups, saisissez Joiners, puis choisissez OK. Si vous trouvez plusieurs objets, sélectionnez le groupe Joiners créé précédemment. Choisissez Suivant.
7. Sur la page Tâches à déléguer, sélectionnez Créer une tâche personnalisée à déléguer, puis choisissez Suivant.
8. Sélectionnez Only the following objects in the folder, puis Computer objects.
9. Sélectionnez Créer les objets sélectionnés dans ce dossier et Supprimer les objets sélectionnés dans ce dossier. Ensuite, sélectionnez Suivant.

Delegation of Control Wizard ✕

Active Directory Object Type 

Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

☐ Site Settings objects

☐ Sites Container objects

☐ Subnet objects

☐ Subnets Container objects

☐ Trusted Domain objects

☒ User objects

☒ Create selected objects in this folder

☒ Delete selected objects in this folder

< Back Next > Cancel Help

10. Sélectionnez Lecture et Ecriture, puis choisissez Suivant.

Delegation of Control Wizard ✕

Permissions 

Select the permissions you want to delegate.

Show these permissions:

☒ General

☒ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

☐ Full Control

☒ Read

☐ Write

☐ Create All Child Objects

☐ Delete All Child Objects

☐ Read All Properties

< Back Next > Cancel Help

11. Vérifiez les informations de la page Fin de l'Assistant Délégation de contrôle, puis choisissez Terminer.
12. Créez un utilisateur avec un mot de passe fort et ajoutez-le au groupe Joiners. L'utilisateur disposera alors de privilèges suffisants pour se connecter Directory Service à l'annuaire.

Création d'un ensemble d'options DHCP pour Simple AD

AWS vous recommande de créer un ensemble d'options DHCP pour votre Directory Service répertoire et d'attribuer le jeu d'options DHCP au VPC dans lequel se trouve votre répertoire. Cela permet à toutes les instances de ce VPC de pointer vers le domaine spécifié, et aux serveurs DNS de résoudre leurs noms de domaine.

Pour en savoir plus sur les jeux d'options DHCP, veuillez consulter la section [DHCP options sets](#) (français non garanti) dans le Guide de l'utilisateur Amazon VPC.

Pour créer un jeu d'options DHCP défini pour votre annuaire

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez DHCP Options Sets, puis sélectionnez Create DHCP options set.
3. Dans la page Créer un jeu d'options DHCP, saisissez les valeurs suivantes pour votre annuaire :

Nom

Une balise facultative pour le jeu d'options.

Nom de domaine

Nom complet de votre annuaire, par exemple corp.example.com.

Serveurs de noms de domaine

Les adresses IP des serveurs DNS du répertoire AWS que vous avez fourni.

 Note

Vous pouvez trouver ces adresses en accédant au volet de navigation de la [console AWS Directory Service](#), en sélectionnant Directories (Annuaire), puis en choisissant l'ID d'annuaire correct.

Serveurs NTP

Laissez ce champ vide.

Serveur de nom NetBIOS

Laissez ce champ vide.

Type de nœud NetBIOS

Laissez ce champ vide.

4. Choisissez Créer un jeu d'options DHCP. Le nouveau jeu d'options DHCP apparaît dans votre liste d'options DHCP.
5. Notez l'ID du nouveau jeu d'options DHCP (dopt-**xxxxxxxxxx**). Vous l'utilisez pour associer le nouveau jeu d'options à votre VPC.

Pour modifier le jeu d'options DHCP associé à un VPC

Vous ne pouvez pas modifier un jeu d'options DHCP après l'avoir créé. Si vous voulez que votre VPC utilise un jeu différent d'options DHCP, vous devez créer un nouveau jeu et l'associer à votre VPC. Vous pouvez également configurer votre VPC pour ne pas utiliser d'options DHCP du tout.

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, sélectionnez Votre VPCs.
3. Sélectionnez le VPC, puis choisissez Actions, Modifier les paramètres du VPC.
4. Pour le jeu d'options DHCP, sélectionnez-en un ou choisissez No DHCP options set (Aucun jeu d'option DHCP), puis sélectionnez Save (Enregistrer).

Pour modifier le jeu d'options DHCP associé à un VPC à l'aide de la ligne de commande, consultez ce qui suit :

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Gestion des utilisateurs et des groupes dans Simple AD

Les utilisateurs représentent des individus ou des entités individuelles qui ont accès à votre annuaire. Les groupes sont très utiles pour octroyer ou refuser des privilèges à des groupes d'utilisateurs, plutôt que d'appliquer ces privilèges à chaque utilisateur. Si un utilisateur change d'organisation, déplacez-le dans un autre groupe. Il reçoit alors automatiquement les privilèges nécessaires pour la nouvelle organisation.

Pour créer des utilisateurs et des groupes dans un Directory Service annuaire, vous devez utiliser n'importe quelle instance (locale ou EC2) jointe à votre Directory Service annuaire, et être connecté en tant qu'utilisateur disposant des privilèges nécessaires pour créer des utilisateurs et des groupes. Vous devrez également installer les outils Active Directory sur votre EC2 instance afin de pouvoir ajouter vos utilisateurs et vos groupes à l'aide du composant logiciel enfichable Utilisateurs et ordinateurs Active Directory. Pour plus d'informations sur la configuration d'une EC2 instance et l'installation des outils nécessaires, consultez [Comment associer une EC2 instance Amazon à votre Simple AD](#).

Note

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, mais il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section [Préauthentification](#) sur Microsoft TechNet.

Les rubriques suivantes expliquent comment créer et gérer des utilisateurs et des groupes.

Rubriques

- [Installation des outils d'administration Active Directory pour Simple AD](#)
- [Création d'un utilisateur Simple AD](#)
- [Supprimer un utilisateur Simple AD](#)
- [Réinitialisation d'un mot de passe utilisateur Simple AD](#)
- [Création d'un groupe Simple AD](#)

- [Ajouter un utilisateur Simple AD à un groupe](#)

Installation des outils d'administration Active Directory pour Simple AD

Pour gérer votre Active Directory à partir d'une instance Amazon EC2 Windows Server, vous devez installer les services de domaine Active Directory et les outils Active Directory Lightweight Directory Services sur l'instance. Utilisez la procédure suivante pour installer ces outils sur une instance de EC2 Windows serveur.

Prérequis

Avant de commencer cette procédure, effectuez les opérations suivantes :

1. Créez un répertoire Active Directory Simple AD. Pour de plus amples informations, veuillez consulter [Créez votre Simple AD](#).
2. Lancez une instance de EC2 Windows serveur et joignez-la à votre répertoire Simple AD Active Directory. L' EC2 instance a besoin des politiques suivantes pour créer des utilisateurs et des groupes : **AmazonSSMManagedInstanceCore** et **AmazonSSMDirectoryServiceAccess**. Pour de plus amples informations, veuillez consulter [Joindre une instance Amazon EC2 Windows à votre répertoire Simple AD Active Directory](#).
3. Vous aurez besoin des informations d'identification de votre administrateur de domaine Active Directory. Ces informations d'identification ont été créées lors de la création du Simple AD. Si vous avez suivi la procédure décrite dans [Créez votre Simple AD](#), votre nom d'utilisateur d'administrateur inclut votre nom NetBIOS, **.corp\administrator**

Pour installer les outils d'administration Active Directory sur une instance EC2 Windows Server

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la EC2 console Amazon, choisissez Instances, sélectionnez l'instance Windows Server, puis sélectionnez Connect.
3. Dans la page Se connecter à l'instance, sélectionnez Client RDP.
4. Dans l'onglet Client RDP, sélectionnez Télécharger le fichier Bureau à distance, puis choisissez Obtenir le mot de passe pour récupérer votre mot de passe.
5. Dans le champ Obtenir le mot de passe Windows, sélectionnez Chargement du fichier de clé privée. Choisissez le fichier de clé privée .pem associé à l'instance Windows Server. Après avoir chargé le fichier de clé privée, sélectionnez Déchiffrer le mot de passe.

6. Dans la boîte de dialogue de sécurité Windows, copiez vos informations d'identification d'administrateur local pour que l'ordinateur Windows Server puisse se connecter. Le nom d'utilisateur peut être dans les formats suivants : **NetBIOS-Name\administrator** ou **DNS-Name\administrator**. Par exemple, **corp\administrator** ce serait le nom d'utilisateur si vous avez suivi la procédure dans [Créez votre Simple AD](#).
7. Une fois connecté à l'instance Windows Server, ouvrez le Gestionnaire de serveur dans le menu Démarrer en choisissant Gestionnaire de serveur.
8. Dans le tableau de bord du Gestionnaire de serveur, choisissez Ajouter des rôles et des fonctionnalités.
9. Dans l'Assistant Ajout de rôles et de fonctionnalités, choisissez Type d'installation, sélectionnez Installation basée sur un rôle ou une fonctionnalité, puis choisissez Suivant.
10. Sous Sélection de serveur, vérifiez que le serveur local est sélectionné, puis choisissez Fonctionnalités dans le volet de navigation de gauche.
11. Dans l'arborescence Fonctionnalités, sélectionnez et ouvrez Outils d'administration de serveur distant, Outils d'administration de rôles et Outils AD DS et AD LDS. Lorsque les outils AD DS et AD LDS sont sélectionnés, le module Active Directory pour, les outils AD DS PowerShell, les composants logiciels enfichables et les outils de ligne de commande AD LDS sont sélectionnés. Faites défiler la page vers le bas et sélectionnez Outils du serveur DNS, puis cliquez sur Suivant.

Select features

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

- ☐ Remote Differential Compression
- ☒ Remote Server Administration Tools
 - ☐ Feature Administration Tools
 - ☒ Role Administration Tools
 - ☒ AD DS and AD LDS Tools
 - ☒ Active Directory module for Windows PowerShell
 - ☒ AD DS Tools
 - ☒ AD LDS Snap-Ins and Command-Line Tools
 - ☐ Hyper-V Management Tools
 - ☐ Remote Desktop Services Tools
 - ☐ Windows Server Update Services Tools
 - ☐ Active Directory Certificate Services Tools
 - ☐ Active Directory Rights Management Services
 - ☐ DHCP Server Tools
 - ☒ DNS Server Tools
 - ☐ Fax Server Tools
 - ☐ File Services Tools
 - ☐ Network Controller Management Tools
 - ☐ Network Policy and Access Services Tools

Description

Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

< Previous

Next >

Install

Cancel

12. Passez en revue les informations, puis choisissez Installer. Lorsque l'installation des fonctionnalités est terminée, les outils Active Directory Domain Services et Active Directory Lightweight Directory Services sont disponibles sur l'écran Démarrer dans le dossier Outils d'administration.

Création d'un utilisateur Simple AD

Utilisez la procédure suivante pour créer un utilisateur avec une EC2 instance Amazon jointe à votre annuaire Simple AD. Avant de créer des utilisateurs, vous devez suivre les procédures décrites dans la section [Installation des outils d'administration Active Directory](#).

Note

Lors de l'utilisation de Simple AD, si vous créez un compte d'utilisateur sur une instance Linux avec l'option « Force user to change password at first login », cet utilisateur ne pourra pas modifier initialement son mot de passe à l'aide de la commande `kpasswd`. Pour modifier le

mot de passe la première fois, un administrateur de domaine doit mettre à jour le mot de passe utilisateur à l'aide des outils de gestion Active Directory.

Pour créer un utilisateur

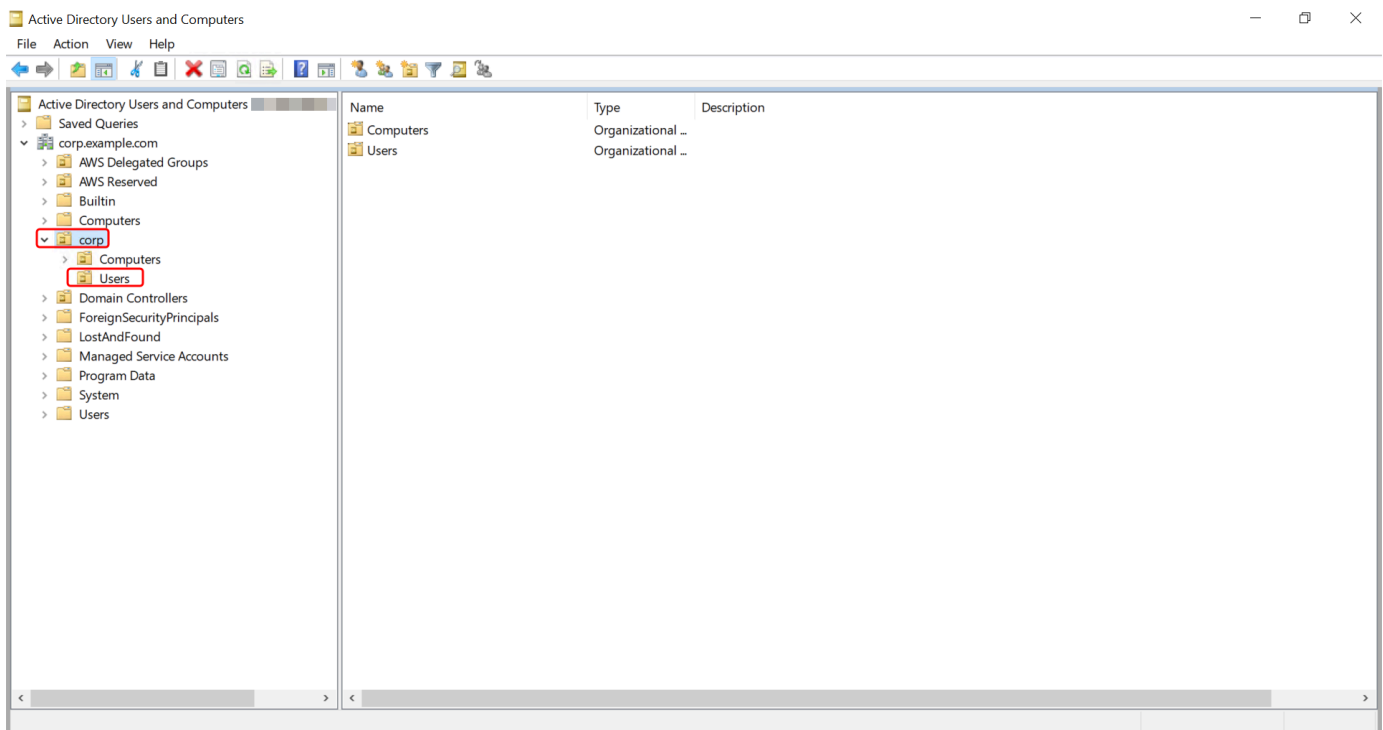
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous le nom NetBIOS de votre répertoire ou dans laquelle vous souhaitez enregistrer votre utilisateur (par exemple, **corp\Users**). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré.](#)



4. Dans le menu Action, choisissez Nouveau, puis sélectionnez Utilisateur pour ouvrir l'assistant de création d'utilisateurs.
5. Sur la première page de l'assistant, entrez les valeurs des champs suivants, puis sélectionnez Suivant.
 - Prénom
 - Nom
 - Nom de connexion de l'utilisateur
6. Sur la deuxième page de l'assistant, entrez un mot de passe temporaire dans Mot de passe et Confirmer le mot de passe. Assurez-vous que l'utilisateur doit modifier le mot de passe lors de sa prochaine connexion. Aucune autre option ne doit être sélectionnée. Choisissez Suivant.
7. Sur la troisième page de l'assistant Nouvel utilisateur, vérifiez que les informations du nouvel utilisateur sont correctes, puis choisissez Terminer. Le nouvel utilisateur s'affiche dans le dossier Utilisateurs.

Supprimer un utilisateur Simple AD

Suivez la procédure ci-dessous pour supprimer un utilisateur dont l'instance Amazon EC2 Windows est jointe à votre annuaire Simple AD.

Pour supprimer un utilisateur

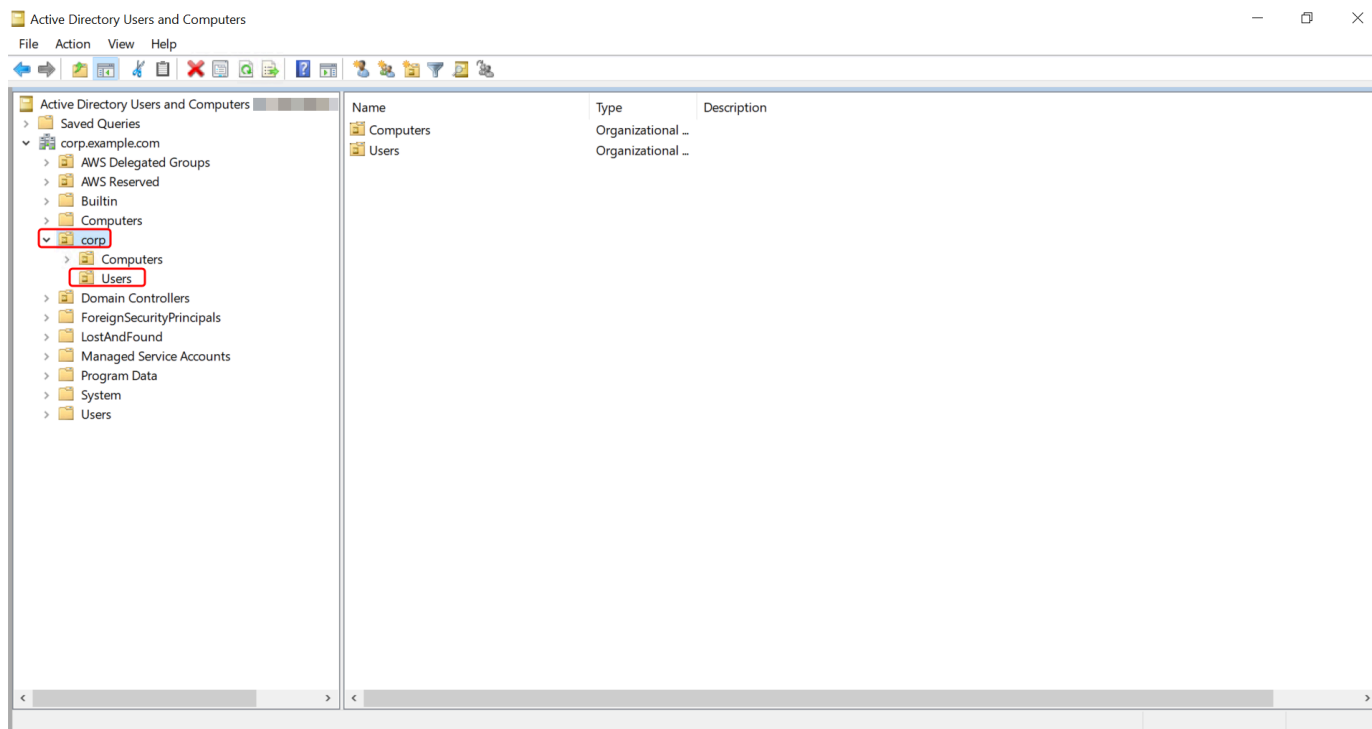
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu Démarrer de Windows. Un raccourci vers cet outil se trouve dans le dossier Outils d'administration de Windows.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez l'unité d'organisation contenant l'utilisateur que vous souhaitez supprimer (par exemple, **corp\Users**).



4. Sélectionnez l'utilisateur que vous souhaitez supprimer. Dans le menu Action, sélectionnez Supprimer.
5. Une boîte de dialogue vous demande de confirmer que vous souhaitez supprimer l'utilisateur. Choisissez Oui pour supprimer l'utilisateur. Cette action supprime définitivement l'utilisateur sélectionné.

Réinitialisation d'un mot de passe utilisateur Simple AD

Les utilisateurs doivent respecter les politiques de mot de passe définies dans Active Directory. Parfois, cela peut prendre le dessus sur les utilisateurs, y compris l'administrateur Active Directory, et ils oublient leur mot de passe. Dans ce cas, vous pouvez rapidement réinitialiser le mot de passe de l'utilisateur en indiquant Directory Service s'il réside dans Simple AD.

Vous devez être connecté en tant qu'utilisateur avec les autorisations nécessaires pour réinitialiser les mots de passe. Pour plus d'informations sur les autorisations, consultez [Vue d'ensemble de la gestion des autorisations d'accès à vos Directory Service ressources](#).

Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de votre Active Directory, sauf dans les cas suivants :

- Vous pouvez réinitialiser le mot de passe de n'importe quel utilisateur de l'unité organisationnelle (UO) en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre Active Directory. Par exemple, si vous avez suivi la procédure décrite dans [Créez votre Simple AD](#), votre nom NetBIOS serait CORP et les mots de passe des utilisateurs que vous pourriez réinitialiser seraient membres de l' Corp/Users UO.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur en dehors de l'unité d'organisation en fonction du nom NetBIOS que vous avez utilisé lors de la création de votre Active Directory. Pour plus d'informations sur la structure de l'UO de Simple AD, consultez [Qu'est-ce qui est créé avec votre Simple AD](#).
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur membre de deux domaines. Vous ne pouvez pas non plus réinitialiser le mot de passe d'un utilisateur membre du groupe Administrateurs du domaine ou du groupe Administrateurs d'entreprise, à l'exception de l'utilisateur administrateur.
- Vous ne pouvez pas réinitialiser le mot de passe d'un utilisateur membre du groupe Administrateurs du domaine ou du groupe Administrateurs d'entreprise, à l'exception de l'utilisateur administrateur.

Vous pouvez utiliser l'une des méthodes suivantes pour réinitialiser le mot de passe d'un utilisateur :

- AWS Management Console
- AWS CLI

AWS Management Console

1. Dans le volet de navigation de la [Directory Service console](#), sous Active Directory, choisissez Directories, puis sélectionnez Active Directory dans la liste où vous souhaitez réinitialiser un mot de passe utilisateur.
2. Sur la page des détails de l'annuaire, choisissez Actions, puis Réinitialiser le mot de passe utilisateur.
3. Dans la boîte de dialogue Réinitialiser le mot de passe utilisateur, dans Nom d'utilisateur, tapez le nom d'utilisateur de l'utilisateur dont le mot de passe doit être modifié.
4. Entrez un mot de passe dans Nouveau mot de passe et Confirmer le mot de passe, puis choisissez Réinitialiser le mot de passe.

AWS CLI

1. Pour installer le AWS CLI, voir [Installer ou mettre à jour la dernière version du AWS CLI](#).
2. Ouvrez le AWS CLI.
3. Tapez la commande suivante et remplacez l'ID de répertoire, le nom d'utilisateur **jane.doe** et le mot de passe **P@ssw0rd** par votre ID Active Directory et les informations d'identification souhaitées. Consultez [reset-user-password](#) le manuel de référence des AWS CLI commandes pour plus d'informations.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

Création d'un groupe Simple AD

Utilisez la procédure suivante pour créer un groupe de sécurité avec une EC2 instance Amazon jointe à votre annuaire Simple AD. Avant de créer des groupes de sécurité, vous devez suivre les procédures décrites dans la section [Installation des outils d'administration Active Directory](#).

Pour créer un groupe

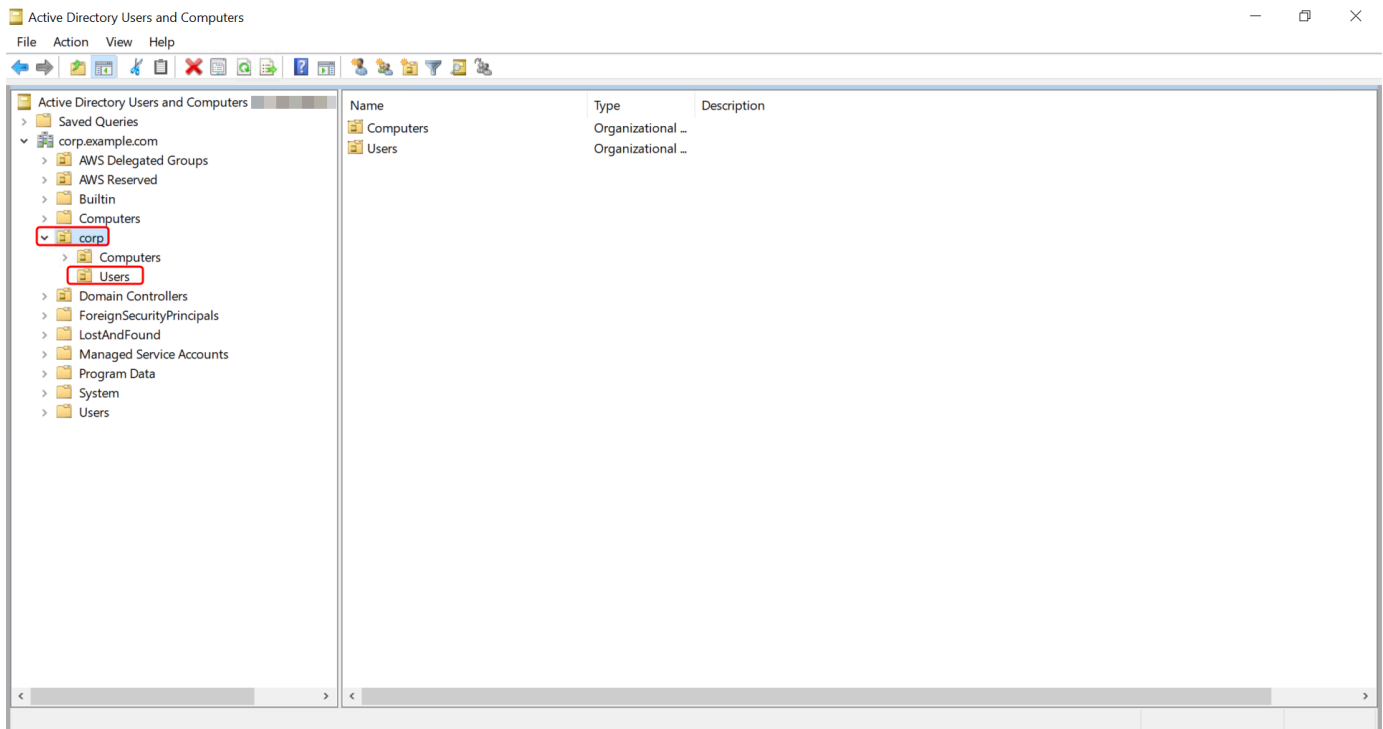
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence du répertoire, sélectionnez une unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous souhaitez stocker votre groupe (par exemple, Corp\Users). Pour plus d'informations sur la structure de l'UO utilisée par les annuaires dans AWS, consultez [Qu'est-ce qui est créé avec votre Microsoft AD AWS géré](#).



4. Dans le menu Action, cliquez sur Nouveau, puis sur Groupe pour ouvrir l'assistant de création de nouveaux groupes.
5. Tapez le nom du groupe dans Nom du groupe, sélectionnez une étendue de groupe qui répond à vos besoins, puis sélectionnez Sécurité pour le type de groupe. Pour plus d'informations sur l'étendue des groupes Active Directory et les groupes de sécurité, veuillez consulter la section [Groupes de sécurité Active Directory](#) dans la documentation de Microsoft Windows Server.
6. Cliquez sur OK. Le nouveau groupe de sécurité apparaîtra dans le dossier Utilisateurs.

Ajouter un utilisateur Simple AD à un groupe

Suivez la procédure ci-dessous pour ajouter un utilisateur à un groupe de sécurité avec une EC2 instance jointe à votre annuaire Simple AD.

Pour ajouter un utilisateur à un groupe

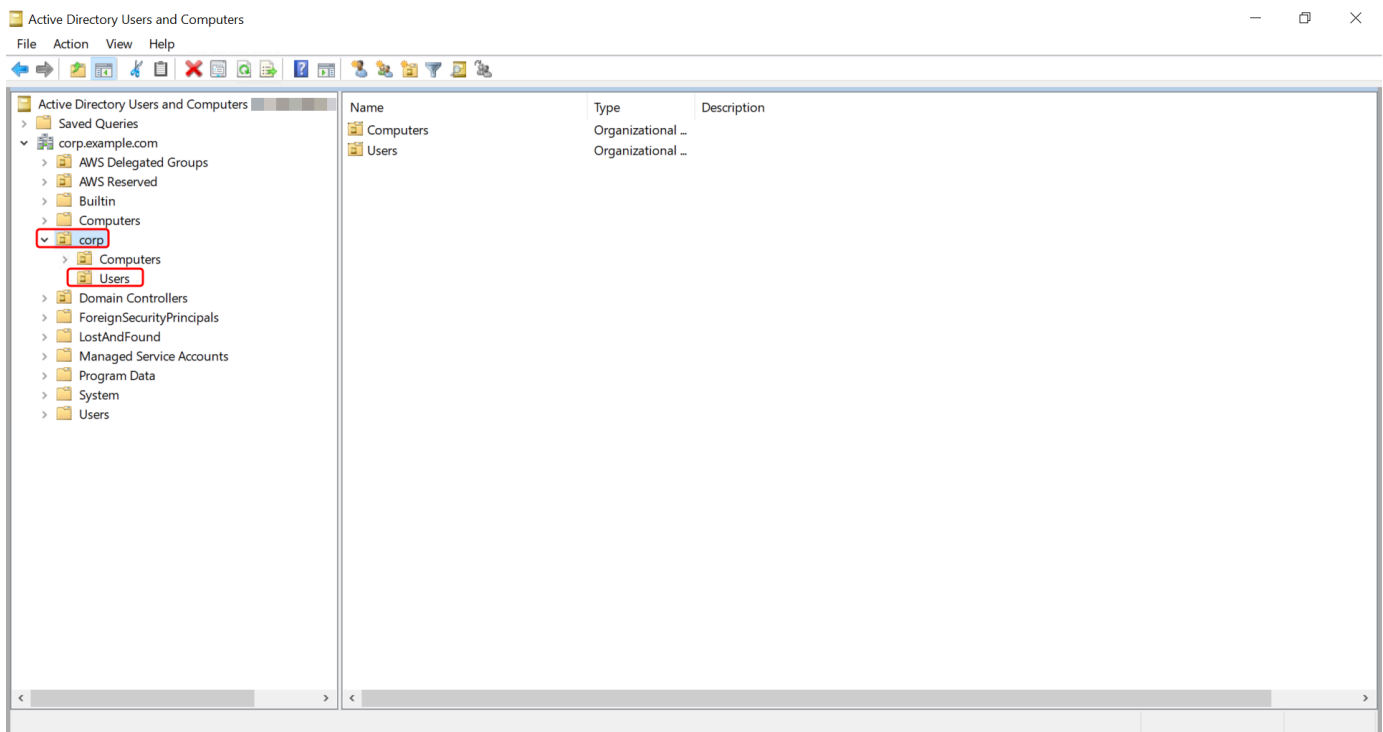
1. Connectez-vous à l'instance où les outils d'administration Active Directory ont été installés.
2. Ouvrez l'outil Utilisateurs et ordinateurs Active Directory. Il existe un raccourci vers cet outil dans le dossier Outils d'administration.

Tip

Vous pouvez exécuter ce qui suit à partir d'une invite de commande sur l'instance pour ouvrir directement la boîte à outils Utilisateurs et ordinateurs Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Dans l'arborescence de l'annuaire, sélectionnez l'unité d'organisation sous l'unité d'organisation du nom NetBIOS de votre annuaire dans laquelle vous avez enregistré votre groupe, puis sélectionnez le groupe auquel vous souhaitez ajouter un utilisateur en tant que membre.



4. Dans le menu Action, cliquez sur Propriétés pour ouvrir la boîte de dialogue des propriétés du groupe.
5. Sélectionnez l'onglet Membres, puis cliquez sur Ajouter.
6. Pour Entrez les noms des objets à sélectionner, tapez le nom d'utilisateur que vous souhaitez ajouter et cliquez sur OK. Le nom sera affiché dans la liste Membres. Cliquez à nouveau sur OK pour mettre à jour les membres du groupe.
7. Vérifiez que l'utilisateur est désormais membre du groupe en le sélectionnant dans le dossier Utilisateurs et en cliquant sur Propriétés dans le menu Action pour ouvrir la boîte de dialogue des

propriétés. Sélectionnez l'onglet Membre de. Le nom du groupe doit apparaître dans la liste des groupes auxquels appartient l'utilisateur.

Quotas Simple AD

En général, vous ne devez pas ajouter plus de 500 utilisateurs à un petit annuaire Simple AD et pas plus de 5 000 à un grand annuaire Simple AD. Pour des options de dimensionnement plus flexibles et des fonctionnalités Active Directory supplémentaires, pensez plutôt à utiliser AWS Directory Service pour Microsoft Active Directory (Standard Edition ou Enterprise Edition).

Voici les quotas par défaut pour Simple AD. Sauf indication contraire, chaque quota est spécifique à une région.

Quotas Simple AD

Ressource	Quota par défaut
Annuaire Simple AD	10
Instantanés manuels *	5 par Simple AD

* Le quota d'instantanés manuels ne peut pas être modifié.

Note

Vous ne pouvez pas associer d'adresse IP publique à votre AWS Elastic Network Interface (ENI).

Résolution des problèmes de Simple AD

Les informations suivantes peuvent vous aider à résoudre certains problèmes courants que vous pouvez rencontrer lors de la création ou de l'utilisation de Simple AD Active Directory.

Rubriques

- [Récupération d'un mot de passe](#)
- [Je reçois un message d'erreur « KDC ne peut pas répondre à l'option demandée » lors de l'ajout d'un utilisateur à Simple AD](#)

- [Je ne parviens pas à mettre à jour le nom DNS ou l'adresse IP d'une instance jointe à mon domaine \(mise à jour dynamique DNS\)](#)
- [Je ne parviens pas à me connecter à SQL Server à l'aide d'un compte SQL Server](#)
- [Mon Simple AD est bloqué dans l'état « Demandé »](#)
- [Je reçois un message d'erreur « AZ constrained » lorsque je crée un Simple AD](#)
- [Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon Simple AD](#)
- [Ressources supplémentaires](#)
- [Résolution des messages d'état de l'annuaire Simple AD](#)

Récupération d'un mot de passe

Si un utilisateur oublie un mot de passe ou rencontre des difficultés pour se connecter à votre annuaire Simple AD, vous pouvez réinitialiser son mot de passe à l'aide du AWS Management Console, PowerShell ou du AWS CLI.

Pour de plus amples informations, veuillez consulter [Réinitialisation d'un mot de passe utilisateur Simple AD](#).

Je reçois un message d'erreur « KDC ne peut pas répondre à l'option demandée » lors de l'ajout d'un utilisateur à Simple AD

Cela peut se produire lorsque le client Samba CLI n'envoie pas correctement les net commandes à tous les contrôleurs de domaine. Si ce message d'erreur s'affiche lorsque vous utilisez la net ads commande pour ajouter un utilisateur à votre annuaire Simple AD, utilisez l'-S argument et spécifiez l'adresse IP de l'un de vos contrôleurs de domaine. Si l'erreur persiste, essayez l'autre contrôleur de domaine. Vous pouvez également utiliser les outils d'administration d'Active Directory pour ajouter des utilisateurs à votre annuaire. Pour de plus amples informations, veuillez consulter [Installation des outils d'administration Active Directory pour Simple AD](#).

Je ne parviens pas à mettre à jour le nom DNS ou l'adresse IP d'une instance jointe à mon domaine (mise à jour dynamique DNS)

Les mises à jour dynamiques DNS ne sont pas prises en charge dans les domaines Simple AD. En revanche, vous pouvez effectuer les modifications directement en connectant votre annuaire à l'aide du Gestionnaire DNS sur une instance qui est jointe à votre domaine.

Je ne parviens pas à me connecter à SQL Server à l'aide d'un compte SQL Server

Un message d'erreur peut s'afficher si vous essayez d'utiliser SQL Server Management Studio (SSMS) avec un compte SQL Server pour vous connecter à SQL Server exécuté sur une EC2 instance Amazon Windows 2012 R2. Le problème se produit lorsque SSMS s'exécute en tant qu'utilisateur de domaine et peut entraîner l'erreur `Login failed for user`, même lorsque des informations d'identification valides sont fournies. Il s'agit d'un problème connu et AWS nous nous efforçons activement de le résoudre.

Pour contourner ce problème, vous pouvez vous connecter à SQL Server avec Windows l'authentification au lieu de l'authentification SQL. Vous pouvez également lancer SSMS en tant qu'utilisateur local et non utilisateur de domaine Simple AD.

Mon Simple AD est bloqué dans l'état « Demandé »

Si vous possédez un Simple AD qui est resté actif pendant `Requested` plus de cinq minutes, essayez de supprimer le répertoire et de le recréer. Si le problème persiste, contactez le [Centre AWS Support](#).

Je reçois un message d'erreur « AZ constrained » lorsque je crée un Simple AD

Certains AWS comptes créés avant 2012 peuvent avoir accès à des zones de disponibilité dans les régions de l'est des États-Unis (Virginie du Nord), de l'ouest des États-Unis (Californie du Nord) ou de l'Asie-Pacifique (Tokyo) qui ne prennent pas en charge Directory Service les annuaires. Si vous voyez une erreur comme celle-ci lors de la création d'un annuaire, choisissez un sous-réseau dans une autre zone de disponibilité et essayez de recréer l'annuaire.

Certains de mes utilisateurs ne peuvent pas s'authentifier avec mon Simple AD

Vos comptes d'utilisateur doivent avoir une pré-authentification Kerberos activée. Il s'agit du paramètre par défaut pour les nouveaux comptes d'utilisateur, et il ne doit pas être modifié. Pour plus d'informations sur ce paramètre, consultez la section [Préauthentification](#) sur Simple AD. TechNet

Ressources supplémentaires

Les ressources suivantes peuvent vous aider à résoudre les problèmes pendant que vous travaillez avec AWS.

- [AWS Centre de connaissances](#) : recherchez d'autres ressources FAQs et liens vers d'autres ressources pour vous aider à résoudre les problèmes.
- [AWS Centre de support](#) : bénéficiez d'une assistance technique.
- [AWS Premium Support Center](#) : bénéficiez d'un support technique haut de gamme.

Rubriques

- [Résolution des messages d'état de l'annuaire Simple AD](#)

Résolution des messages d'état de l'annuaire Simple AD

Lorsqu'un Simple AD est défaillant ou inutilisable, le message d'état du répertoire contient des informations supplémentaires. Le message d'état est affiché dans la Directory Service console ou renvoyé dans le [DirectoryDescription.StageReason](#) membre par l'[DescribeDirectories](#) API. Pour plus d'informations sur le statut de l'annuaire, veuillez consulter [Comprendre le statut de votre annuaire Microsoft AD AWS géré](#).

Voici les messages de statut d'un annuaire Simple AD :

Rubriques

- [L'interface réseau Elastic \(ENI\) du service d'annuaire n'est pas connectée](#)
- [Problèmes détectés par l'instance](#)
- [L'utilisateur Directory Service réservé critique est absent de l'annuaire](#)
- [L'utilisateur Directory Service réservé critique doit appartenir au groupe des administrateurs de domaine](#)
- [L'utilisateur Directory Service réservé critique est désactivé](#)
- [The main domain controller does not have all FSMO roles](#)
- [Domain controller replication failures](#)

L'interface réseau Elastic (ENI) du service d'annuaire n'est pas connectée

Description

L'interface ELASTIC Network (ENI) critique créée en votre nom lors de la création de l'annuaire afin d'établir une connectivité réseau avec votre VPC n'est pas attachée à l'instance d'annuaire. AWS les applications soutenues par ce répertoire ne fonctionneront pas. Votre annuaire ne peut pas se connecter à votre réseau sur site.

Résolution des problèmes

Si l'ENI est détachée, mais existe toujours, contactez Support. Si l'ENI est supprimée, il n'y a aucun moyen de résoudre le problème et votre annuaire est définitivement inutilisable. Vous devez supprimer votre annuaire et en créer un nouveau.

Problèmes détectés par l'instance

Description

Une erreur interne a été détectée par l'instance. Cela signifie généralement que le service de surveillance tente activement de récupérer les instances endommagées.

Résolution des problèmes

Dans la plupart des cas, il s'agit d'un problème temporaire et le répertoire finit par revenir à l'état actif. Si le problème persiste, contactez Support pour obtenir de l'aide.

L'utilisateur Directory Service réservé critique est absent de l'annuaire

Description

Lorsqu'un Simple AD est créé, il Directory Service crée un compte de service dans l'annuaire portant le nom `AWSAdminD-xxxxxxxxxx`. Cette erreur est générée lorsque ce compte de service est introuvable. Sans ce compte, Directory Service ne peut pas exécuter de fonctions administratives sur l'annuaire, ce qui rend l'annuaire inutilisable.

Résolution des problèmes

Pour résoudre ce problème, restaurez l'annuaire pour revenir à un instantané précédent ayant été créé avant la suppression du compte de service. Des instantanés automatiques de votre annuaire Simple AD sont pris une fois par jour. Si l'instantané a été pris plus de cinq jours après

la suppression de ce compte, vous ne pourrez pas restaurer l'annuaire à l'état d'existence du compte. Si vous n'êtes pas en mesure de restaurer l'annuaire à partir d'un instantané où le compte existait, votre annuaire peut devenir définitivement hors d'usage. Si tel est le cas, vous devez supprimer votre annuaire et en créer un nouveau.

L'utilisateur Directory Service réservé critique doit appartenir au groupe des administrateurs de domaine

Description

Lorsqu'un Simple AD est créé, il Directory Service crée un compte de service dans l'annuaire portant le nom `AWSAdminD-xxxxxxxxxx`. Cette erreur est générée lorsque ce compte de service n'est pas un membre du groupe `Domain Admins`. L'appartenance à ce groupe est nécessaire pour lui donner Directory Service les privilèges nécessaires pour effectuer des opérations de maintenance et de restauration, telles que le transfert de rôles FSMO, l'adhésion à un domaine de nouveaux contrôleurs de répertoire et la restauration à partir de snapshots.

Résolution des problèmes

Utilisez l'outil Utilisateurs et ordinateurs Active Directory pour ajouter à nouveau le compte de service au groupe `Domain Admins`.

L'utilisateur Directory Service réservé critique est désactivé

Description

Lorsqu'un Simple AD est créé, il Directory Service crée un compte de service dans l'annuaire portant le nom `AWSAdminD-xxxxxxxxxx`. Cette erreur est générée lorsque ce compte de service est désactivé. Ce compte doit être activé afin de Directory Service pouvoir effectuer des opérations de maintenance et de restauration sur le répertoire.

Résolution des problèmes

Utilisez l'outil Utilisateurs et ordinateurs Active Directory pour réactiver le compte de service.

The main domain controller does not have all FSMO roles

Description

Tous les rôles FSMO ne sont pas détenus par le contrôleur d'annuaire Simple AD. Directory Service ne peut pas garantir le comportement et la fonctionnalité si les rôles FSMO ne font pas partie du contrôleur d'annuaire Simple AD approprié.

Résolution des problèmes

Utilisez les outils Active Directory pour redéplacer les rôles FSMO vers le contrôleur de l'annuaire actif original. Pour plus d'informations sur le déplacement des rôles FSMO, rendez-vous sur <https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles>.
in-ad-ds Si cela ne résout pas le problème, veuillez nous contacter Support pour obtenir de l'aide.

Domain controller replication failures

Description

Les contrôleurs d'annuaire Simple AD n'effectuent pas de réplication entre eux. Cela peut être causé par un ou plusieurs des problèmes suivants :

- Les groupes de sécurité des contrôleurs d'annuaire n'ont pas les ports corrects ouverts.
- Le réseau ACLs est trop restrictif.
- La table de routage du VPC n'achemine pas correctement le trafic réseau entre les contrôleurs d'annuaire.
- Une autre instance a été promue à un contrôleur de domaine dans l'annuaire.

Résolution des problèmes

Pour plus d'informations sur vos besoins en matière de réseau VPC, veuillez consulter AWS Managed Microsoft AD [Conditions préalables à la création d'un Microsoft AWS AD géré](#), AD Connector [Conditions préalables requises pour AD Connector](#) ou Simple AD [Prérequis pour Simple AD](#). Si votre annuaire comporte un contrôleur de domaine inconnu, vous devez le rétrograder. Si la configuration réseau de votre VPC est correcte, mais que l'erreur persiste, veuillez contacter le Support pour obtenir de l'aide.

Sécurité dans AWS Directory Service

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 Directory Service, consultez la section [AWS Services concernés par programme de conformité](#).
- **Sécurité dans le cloud** — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation Directory Service. Les rubriques suivantes expliquent comment procéder à la configuration Directory Service 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 Directory Service ressources.

Rubriques de sécurité

Les rubriques de sécurité suivantes sont disponibles dans cette section :

- [Gestion des identités et des accès pour Directory Service](#)
- [Connexion et surveillance AWS Directory Service](#)
- [Validation de conformité pour AWS Directory Service](#)
- [Résilience dans AWS Directory Service](#)
- [Sécurité de l'infrastructure dans AWS Directory Service](#)

Rubriques de sécurité supplémentaires

Les rubriques de sécurité supplémentaires suivantes sont disponibles dans ce guide :

Comptes, trusts et accès aux AWS ressources

- [AWS Compte administrateur Microsoft AD géré et autorisations de groupe](#)
- [Comptes de service administrés de groupe](#)
- [Création d'une relation de confiance entre votre Microsoft AD AWS géré et votre AD autogéré](#)
- [Délégation Kerberos contrainte](#)
- [Octroi aux utilisateurs et aux groupes de AWS Managed Microsoft AD d'accéder aux AWS ressources avec des rôles IAM](#)
- [Autorisation pour AWS les applications et les services utilisant Directory Service](#)

Sécurisation de votre annuaire

- [Sécurisez votre Microsoft AD AWS géré](#)
- [Sécurisation de votre annuaire AD Connector](#)

Journalisation et surveillance

- [Surveillez votre Microsoft AD AWS géré](#)
- [Surveillance de votre annuaire AD Connector](#)

Résilience

- [Application de correctifs et maintenance pour AWS Managed Microsoft AD](#)

Gestion des identités et des accès pour Directory Service

L'accès à Directory Service nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder à AWS des ressources, telles qu'un Directory Service annuaire. Les sections suivantes fournissent des informations détaillées sur la manière dont vous pouvez utiliser [AWS Identity and Access Management \(IAM\)](#) et vous aider Directory Service à sécuriser vos ressources en contrôlant qui peut y accéder :

- [Authentification](#)
- [Contrôle d'accès](#)

Authentification

Découvrez comment accéder à l' AWS aide des [identités IAM](#).

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais vous ne pouvez pas créer de Directory Service ressources ou y accéder sans autorisation. Par exemple, vous devez être autorisé à créer un Directory Service répertoire ou à créer un instantané de répertoire.

Les sections suivantes décrivent comment gérer les autorisations pour Directory Service. Nous vous recommandons de lire d'abord la présentation.

- [Vue d'ensemble de la gestion des autorisations d'accès à vos Directory Service ressources](#)
- [Utilisation de politiques basées sur l'identité \(politiques IAM\) pour Directory Service](#)
- [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#)

Vue d'ensemble de la gestion des autorisations d'accès à vos Directory Service ressources

Chaque AWS ressource est détenue par un AWS compte. Par conséquent, les autorisations de création ou d'accès aux ressources sont régies par des politiques d'autorisation. Toutefois, un administrateur de compte, c'est-à-dire un utilisateur disposant d'autorisations d'administrateur, peut associer des autorisations aux ressources. Ils ont également la possibilité d'associer des politiques d'autorisations aux identités IAM, telles que les utilisateurs, les groupes et les rôles, et certains services, tels que AWS Lambda la prise en charge de l'attachement de politiques d'autorisations aux ressources.

Note

Pour plus d'informations sur le rôle d'administrateur de compte, consultez les [meilleures pratiques IAM](#) dans le guide de l'utilisateur IAM.

Rubriques

- [Directory Service ressources et opérations](#)
- [Présentation de la propriété des ressources](#)
- [Gestion de l'accès aux ressources](#)
- [Spécification des éléments d'une politique : actions, effets, ressources et principaux](#)
- [Spécification de conditions dans une politique](#)

Directory Service ressources et opérations

Dans Directory Service, la ressource principale est un répertoire. Comme il Directory Service prend en charge les ressources de capture instantanée d'annuaire, vous pouvez créer des instantanés uniquement dans le contexte d'un répertoire existant. Cet instantané est appelé sous-ressource.

Ces ressources sont associées à des noms de ressources Amazon (ARNs) uniques, comme indiqué dans le tableau suivant.

Type de ressource	Format ARN
Annuaire	arn:aws:ds: <i>region</i> : <i>account-id</i> :directory/ <i>external-directory-id</i>
Instantané	arn:aws:ds: <i>region</i> : <i>account-id</i> :snapshot/ <i>external-snapshot-id</i>

Directory Service inclut deux espaces de noms de service en fonction du type d'opérations que vous effectuez.

- L'espace ds de noms du service fournit un ensemble d'opérations permettant de travailler avec les ressources appropriées. Pour obtenir la liste des opérations disponibles, veuillez consulter [Directory Service Actions](#) (français non garanti).
- L'espace ds-data de noms du service fournit un ensemble d'opérations aux objets Active Directory. Pour obtenir la liste des opérations disponibles, consultez la section [Directory Service Data API Reference](#).

Présentation de la propriété des ressources

Le propriétaire d'une ressource est le AWS compte qui a créé une ressource. En d'autres termes, le propriétaire de la ressource est le AWS compte de l'entité principale (le compte root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande qui crée la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte root de votre AWS compte pour créer une Directory Service ressource, telle qu'un répertoire, votre AWS compte est le propriétaire de cette ressource.
- Si vous créez un utilisateur IAM dans votre AWS compte et que vous accordez des autorisations pour créer Directory Service des ressources à cet utilisateur, celui-ci peut également créer des Directory Service ressources. Cependant, votre AWS compte, auquel appartient l'utilisateur, est propriétaire des ressources.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer Directory Service des ressources, toute personne pouvant assumer ce rôle peut créer des Directory Service ressources. Votre AWS compte, auquel appartient le rôle, est propriétaire des Directory Service ressources.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

Note

Cette section décrit l'utilisation d'IAM dans le contexte de Directory Service. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, veuillez consulter la section [What is IAM?](#) (français non garanti) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, veuillez consulter [IAM JSON policy reference](#) (français non garanti) dans le Guide de l'utilisateur IAM.

Les politiques associées à une identité IAM sont appelées politiques basées sur l'identité (politiques IAM) et les politiques associées à une ressource sont appelées politiques basées sur les ressources. Directory Service prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

- [Politiques basées sur une identité \(politiques IAM\)](#)
- [Politiques basées sur les ressources](#)

Politiques basées sur une identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associer une politique d'autorisation à un utilisateur ou à un groupe de votre compte : un administrateur de compte peut utiliser une politique d'autorisation associée à un utilisateur particulier pour autoriser cet utilisateur à créer une Directory Service ressource, telle qu'un nouveau répertoire.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes.

Pour plus d'informations sur l'utilisation d'IAM pour déléguer des autorisations, veuillez consulter la section [Access management](#) (français non garanti) dans le Guide de l'utilisateur IAM.

La politique d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `Describe`. Ces actions affichent des informations sur une Directory Service ressource, telle qu'un répertoire ou un instantané. Notez que le caractère générique (*) dans l'`Resource` élément indique que les actions sont autorisées pour toutes les Directory Service ressources détenues par le compte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

```
}
```

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec Directory Service, consultez [Utilisation de politiques basées sur l'identité \(politiques IAM\) pour Directory Service](#). 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.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez associer une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. Directory Service ne prend pas en charge les politiques basées sur les ressources.

Spécification des éléments d'une politique : actions, effets, ressources et principaux

Pour chaque Directory Service ressource, le service définit un ensemble d'opérations d'API. Pour de plus amples informations, veuillez consulter [Directory Service ressources et opérations](#). Pour obtenir la liste des opérations d'API disponibles, veuillez consulter [Directory Service Actions](#) (français non garanti).

Pour accorder des autorisations pour ces opérations d'API Directory Service, définissez un ensemble d'actions que vous pouvez spécifier dans une politique. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments de base 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 les Directory Service ressources, vous utilisez toujours le caractère générique (*) dans les politiques IAM. Pour de plus amples informations, veuillez consulter [Directory Service ressources et opérations](#).
- **Action** : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, l'autorisation `ds:DescribeDirectories` permet à l'utilisateur d'effectuer l'opération Directory Service `DescribeDirectories`.
- **Effet** – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique. Il peut s'agir d'un accord ou d'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 les ressources, vous spécifiez l'utilisateur, le compte, le service ou toute autre entité pour lequel vous souhaitez recevoir des autorisations (s'applique uniquement aux politiques basées sur les ressources). Directory Service ne prend pas en charge les politiques basées sur les ressources.

Pour plus d'informations sur la syntaxe des politiques IAM et pour obtenir des descriptions, veuillez consulter [IAM JSON policy reference](#) (français non garanti) dans le manuel Guide de l'utilisateur IAM.

Pour consulter un tableau présentant toutes les actions d' Directory Service API et les ressources auxquelles elles s'appliquent, consultez [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de la politique d'accès pour spécifier les conditions définissant quand 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.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à Directory Service. Cependant, il existe des clés de AWS condition que vous pouvez utiliser selon les besoins. Pour obtenir la liste complète des AWS clés, consultez la section [Clés de condition globales disponibles](#) dans le guide de l'utilisateur IAM.

AWS politiques gérées pour AWS Directory Service

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients.

Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

Les sections suivantes décrivent les politiques AWS gérées spécifiques à Directory Service. Vous pouvez associer ces politiques aux utilisateurs de votre compte.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSDirectoryServiceFullAccess

Vous pouvez associer la politique `AWSDirectoryServiceFullAccess` à vos identités IAM. Pour consulter les autorisations complètes associées à cette politique, reportez-vous [AWSDirectoryServiceFullAccess](#) à la référence des politiques AWS gérées.

Cette politique accorde des autorisations administratives qui permettent au principal d'avoir un accès complet à toutes les Directory Service actions. Les principaux titulaires de ces autorisations peuvent créer, configurer et gérer des annuaires, notamment Simple AD, AD Connector et Managed Microsoft AD. Ils peuvent également gérer le partage d'annuaires, les relations de confiance et les configurations de surveillance. Cette politique inclut des autorisations pour gérer l'infrastructure réseau sous-jacente requise pour les services d'annuaire.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ds`— Permet aux principaux un accès complet à toutes les Directory Service actions.
- `ec2`— Permet aux principaux de gérer les interfaces réseau, les groupes de sécurité et de décrire les ressources VPC requises pour les opérations d'annuaire.
- `sns`— Permet aux principaux de créer et de gérer des rubriques SNS pour la surveillance des annuaires, en particulier les rubriques dont le nom commence par « »`DirectoryMonitoring`.

- `iam`— Permet aux principaux de répertorier les rôles IAM pour les opérations de service d'annuaire.
- `organizations`— Permet aux directeurs de gérer l'intégration des AWS Organisations et l'accès aux enable/disable services pour les services d'annuaire.

AWS politique gérée : `AWSDirectoryServiceReadOnlyAccess`

Vous pouvez associer la politique `AWSDirectoryServiceReadOnlyAccess` à vos identités IAM. Pour consulter les autorisations complètes associées à cette politique, reportez-vous [AWSDirectoryServiceReadOnlyAccess](#) à la référence des politiques AWS gérées.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs de consulter les informations dans Directory Service. Les directeurs auxquels cette politique est attachée ne peuvent effectuer aucune mise à jour des annuaires ou de leurs configurations. Par exemple, les principaux disposant de ces autorisations peuvent consulter les détails des annuaires, les relations de confiance et les configurations de surveillance, mais ne peuvent pas créer de nouveaux annuaires ni modifier les annuaires existants. Ils peuvent également consulter les ressources EC2 réseau associées et les rubriques SNS associées aux annuaires.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ds`— Permet aux utilisateurs d'effectuer des actions en lecture seule qui renvoient des informations d'annuaire. Cela inclut les opérations d'API qui commencent par `Check`, `Describe`, `Get`, `List`, ou `Verify`.
- `ec2`— Permet aux utilisateurs de décrire les interfaces réseau, les sous-réseaux et les services d'annuaire VPCs associés.
- `sns`— Permet aux utilisateurs de répertorier et d'obtenir des informations sur les sujets et les abonnements SNS utilisés pour la surveillance des annuaires.
- `organizations`— Permet aux utilisateurs de décrire les AWS Organizations comptes et les configurations d'accès aux services liés aux services d'annuaire.

AWS politique gérée : AWSDirectoryServiceDataFullAccess

Vous pouvez associer la politique `AWSDirectoryServiceDataFullAccess` à vos identités IAM. Pour consulter les autorisations complètes associées à cette politique, reportez-vous [AWSDirectoryServiceDataFullAccess](#) à la référence des politiques AWS gérées.

Cette politique accorde des autorisations administratives qui permettent un accès complet principal aux opérations relatives aux données du Directory Service. Les administrateurs disposant de ces autorisations peuvent créer, mettre à jour et supprimer des utilisateurs et des groupes Active Directory au sein d'annuaires gérés. Ils peuvent gérer les appartenances aux groupes, activer ou désactiver des utilisateurs et effectuer des opérations complètes de gestion des utilisateurs et des groupes. Cette politique est conçue pour les administrateurs qui doivent gérer des objets Active Directory par programmation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ds`— Permet aux principaux d'accéder aux données du répertoire via l'API Directory Service Data.
- `ds-data`— Permet aux principaux d'accéder à toutes les opérations relatives aux données du service d'annuaire, notamment à la création, à la mise à jour et à la suppression d'utilisateurs et de groupes, à la gestion des appartenances aux groupes et à la recherche d'objets de répertoire.

AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess

Vous pouvez associer la politique `AWSDirectoryServiceDataReadOnlyAccess` à vos identités IAM. Pour consulter les autorisations complètes associées à cette politique, reportez-vous [AWSDirectoryServiceDataReadOnlyAccess](#) à la référence des politiques AWS gérées.

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs d'afficher et de rechercher des objets Active Directory dans des annuaires gérés. Les directeurs auxquels cette politique est attachée ne peuvent apporter aucune modification aux utilisateurs, aux groupes ou aux adhésions aux groupes. Par exemple, les administrateurs disposant de ces autorisations peuvent rechercher des utilisateurs et des groupes, consulter les détails des utilisateurs et des groupes et répertorier les appartenances aux groupes, mais ne peuvent pas créer, modifier ou supprimer des objets d'annuaire.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ds`— Permet aux principaux d'accéder aux données du répertoire via l'API Directory Service Data.
- `ds-data`— Permet aux utilisateurs d'effectuer des actions en lecture seule qui renvoient des informations sur les objets du répertoire. Cela inclut les opérations d'API qui commencent par `DescribeList`, ou `Search`.

AWSDirectoryServiceServiceRolePolicy

Vous ne pouvez pas associer la `AWSDirectoryServiceServiceRolePolicy` politique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet à AWS Directory Service d'effectuer des actions en votre nom. Pour voir les autorisations de cette stratégie, consultez [AWSDirectoryServiceServiceRolePolicy](#) dans le AWS Guide de référence des stratégies gérées par.

Cette politique accorde des autorisations qui permettent Directory Service de surveiller et d'évaluer les contrôleurs de domaine autogérés dans les environnements Active Directory hybrides. Le service utilise ces autorisations pour exécuter des évaluations de santé automatisées, exécuter des PowerShell scripts pour les tests de compatibilité et recueillir des informations de configuration réseau afin de garantir une connectivité hybride appropriée et des capacités de restauration automatique.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `ssm`— Permet au service d'envoyer des PowerShell commandes aux contrôleurs de domaine locaux et de récupérer les résultats d'exécution des commandes à des fins de surveillance et d'évaluation.
- `ec2`— Permet au service de décrire les ressources réseau telles que les sous-réseaux VPCs, les groupes de sécurité et les interfaces réseau afin de valider les configurations de connectivité hybrides.

IAM et Directory Service mises à jour des politiques AWS gérées

Consultez les informations relatives aux mises à jour apportées à l'IAM et aux politiques AWS gérées depuis que le service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur les pages IAM et Historique des Directory Service documents.

Modifier	Description	Date
AWSDirectoryServiceServiceRolePolicy : nouvelle politique	Directory Service a ajouté une nouvelle politique permettant de AWS surveiller les contrôleurs de domaine autogérés d'un client.	30 juillet 2025
AWS Politique gérée par : AWSDirectoryServiceDataReadOnlyAccess : nouvelle politique	Directory Service a ajouté une nouvelle politique permettant à un utilisateur ou à un groupe d'accéder à l'affichage et à la recherche d'utilisateurs, de membres et de groupes AD.	17 septembre 2024
AWS politique gérée : AWSDirectoryServiceDataFullAccess : nouvelle politique	Directory Service a ajouté une nouvelle politique permettant à un utilisateur ou à un groupe d'accéder à la gestion d'objets intégrée avec Directory Service Data pour créer, gérer et afficher les utilisateurs, les membres et les groupes AD.	17 septembre 2024
Directory Service a commencé à suivre les modifications	Directory Service a commencé à suivre les modifications apportées AWS à ses politiques gérées.	17 septembre 2024

Utilisation de politiques basées sur l'identité (politiques IAM) pour Directory Service

Cette rubrique fournit des exemples de stratégies basées sur l'identité dans lesquelles un administrateur de compte peut associer des stratégies d'autorisation à des identités IAM (utilisateurs, groupes et rôles). Ces exemples illustrent les politiques IAM dans Directory Service. Vous devez modifier et créer vos propres politiques en fonction de vos besoins et de votre environnement.

⚠ Important

Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options disponibles pour gérer l'accès à vos Directory Service ressources. Pour de plus amples informations, veuillez consulter [Vue d'ensemble de la gestion des autorisations d'accès à vos Directory Service ressources](#).

Les sections de cette rubrique couvrent les sujets suivants :

- [Autorisations requises pour utiliser la Directory Service console](#)
- [AWS politiques gérées \(prédéfinies\) pour Directory Service](#)
- [Exemples de politiques gérées par le client](#)
- [Utilisation des balises avec des politiques IAM](#)

Un exemple de politique d'autorisation est exposé ci-dessous.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDsEc2IamGetRole",
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "iam:GetRole"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
  },
  {
    "Sid": "AllowPassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::111122223333:role/Your-Role-Name",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "cloudwatch.amazonaws.com"
      }
    }
  }
]
}

```

Les trois instructions de la politique accordent les autorisations suivantes :

- La première instruction autorise la création d'un Directory Service répertoire. Comme les autorisations Directory Service ne sont pas prises en charge au niveau des ressources, la politique spécifie un caractère générique (*) comme Resource valeur.
- La deuxième déclaration accorde des autorisations pour accéder aux actions IAM, afin que Directory Service vous puissiez lire et créer des rôles IAM en votre nom. Le caractère générique (*) à la fin de la valeur Resource signifie que l'instruction accepte les autorisations pour les actions IAM sur n'importe quel rôle IAM. Pour limiter cette autorisation à un rôle spécifique, remplacez le caractère générique (*) dans la ressource ARN par un nom de rôle spécifique. Pour plus d'informations, veuillez consulter [IAM Actions](#) (français non garanti).
- La troisième déclaration accorde des autorisations à un ensemble spécifique de ressources dans Amazon EC2 qui sont nécessaires pour Directory Service permettre la création, la configuration et

la destruction de ses répertoires. Remplacez l'ARN du rôle par votre rôle. Pour plus d'informations, consultez [Amazon EC2 Actions](#).

Vous ne voyez aucun Principal élément dans la politique, car dans une stratégie basée sur l'identité, vous ne spécifiez pas le principal qui obtient l'autorisation. Quand vous attachez la stratégie à un utilisateur, l'utilisateur est le mandataire implicite. Lorsque vous attachez une politique d'autorisation à un rôle IAM, le principal identifié dans la politique d'approbation de ce rôle obtient les autorisations.

Pour consulter un tableau présentant toutes les actions d' Directory Service API et les ressources auxquelles elles s'appliquent, consultez [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

Autorisations requises pour utiliser la Directory Service console

Pour qu'un utilisateur puisse utiliser la Directory Service console, il doit disposer des autorisations répertoriées dans la politique précédente ou des autorisations accordées par le rôle d'accès complet du service d'annuaire ou le rôle de lecture seule du service d'annuaire, décrits dans [AWS politiques gérées \(prédéfinies\) pour Directory Service](#).

Si vous créez une politique IAM plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les utilisateurs dotés de cette politique IAM.

AWS politiques gérées (prédéfinies) pour Directory Service

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM prédéfinies ou gérées qui sont créées et administrées par AWS. Les politiques gérées accordent les autorisations nécessaires pour les cas d'utilisation courants, ce qui vous permet de décider des autorisations dont vous avez besoin. Pour de plus amples informations, veuillez consulter [AWS politiques gérées pour AWS Directory Service](#).

Exemples de politiques gérées par le client

Dans cette section, vous trouverez des exemples de politiques utilisateur qui accordent des autorisations pour diverses Directory Service actions.

 Note

Tous les exemples utilisent la région de l'Ouest des États-Unis (Oregon) (us-west-2) et contiennent un récit fictif. IDs

Exemples

- [Exemple 1 : Autoriser un utilisateur à effectuer n'importe quelle action de description sur n'importe quelle Directory Service ressource](#)
- [Exemple 2 : Permettre à un utilisateur de créer un annuaire](#)

Exemple 1 : Autoriser un utilisateur à effectuer n'importe quelle action de description sur n'importe quelle Directory Service ressource

La politique d'autorisation suivante autorise un utilisateur à exécuter toutes les actions qui commencent par Describe dans un Microsoft AD AWS géré avec l'ID de répertoire d-1234567890 dans le Compte AWS 111122223333. Ces actions affichent des informations sur une ressource Directory Service, telle qu'un annuaire ou un instantané. Assurez-vous de remplacer le numéro Région AWS de compte par la région que vous souhaitez utiliser et par votre numéro de compte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
    }
  ]
}
```

Exemple 2 : Permettre à un utilisateur de créer un annuaire

La politique d'autorisations suivante accorde des autorisations pour permettre à un utilisateur de créer un annuaire et toutes les autres ressources connexes, telles que les instantanés et les

approbations. Pour ce faire, des autorisations d'accès à certains EC2 services Amazon sont également requises.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ds:DescribeDirectories"
      ],
      "Resource": "arn:aws:ds:*:111122223333:"
    }
  ]
}
```

Utilisation des balises avec des politiques IAM

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans les politiques IAM que vous utilisez pour la plupart des actions d'API. Directory Service Vous bénéficiez ainsi d'un meilleur contrôle sur les ressources qu'un utilisateur peut créer, modifier ou utiliser. Vous pouvez utiliser l'élément `Condition` (également appelé bloc `Condition`) avec les clés et valeurs de contexte de condition suivantes dans une politique IAM pour contrôler l'accès des utilisateurs (autorisations) en fonction des balises d'une ressource :

- Utilisez `aws:ResourceTag/tag-key: tag-value` pour accorder ou refuser aux utilisateurs des actions sur des ressources ayant des balises spécifiques.
- Utilisez `aws:ResourceTag/tag-key: tag-value` pour exiger qu'une balise spécifique soit utilisée (ou ne soit pas utilisée) lorsque vous effectuez une demande d'API pour créer ou modifier une ressource qui autorise les balises.
- Utilisez `aws:TagKeys: [tag-key, ...]` pour exiger qu'un ensemble de clés de balise spécifique soit utilisé (ou ne soit pas utilisé) lorsque vous effectuez une demande d'API pour créer ou modifier une ressource qui autorise les balises.

Note

Les clés et les valeurs de contexte de condition dans une politique IAM s'appliquent uniquement aux actions Directory Service dans lesquelles un identifiant pour une ressource pouvant être balisée est un paramètre obligatoire.

La section [Contrôle de l'accès à l'aide de balises](#) dans le Guide d'utilisateur IAM contient des informations supplémentaires sur l'utilisation des balises. La section [Référence de politique JSON IAM](#) de ce guide fournit la syntaxe détaillée, des descriptions, ainsi que des exemples des éléments, des variables et de la logique d'évaluation des politiques JSON dans IAM.

La politique de balises suivante permet de créer un Directory Service répertoire tant que les balises suivantes sont utilisées :

- Environnement : production
- Propriétaire : Infrastructure Team
- Centre de coûts : 1234

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Environment": "Production",
          "aws:RequestTag/Owner": "Infrastructure-Team",
          "aws:RequestTag/CostCenter": "12345"
        }
      }
    }
  ]
}
```

La politique de balises suivante permet de mettre à jour et de supprimer des Directory Service répertoires tant que les balises suivantes sont utilisées :

- Projet : Atlas
- Département : Ingénierie
- Environnement : mise en scène

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:DeleteDirectory",
        "ds:UpdateDirectory"
      ]
    }
  ]
}
```



```

    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/Project": "Atlas",
            "aws:ResourceTag/Department": "Engineering",
            "aws:ResourceTag/Environment": "Staging"
        }
    }
}
]
}

```

La politique de balises suivante refuse le balisage des ressources Directory Service lorsque la ressource possède l'une des balises suivantes :

- Production
- Sécurité
- Confidentiel

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ds:AddTagsToResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": ["Production", "Security", "Confidential"]
        }
      }
    }
  ]
}

```

Pour plus d'informations ARNs, consultez [Amazon Resource Names \(ARNs\) et AWS Service Namespaces](#).

La liste suivante des opérations d' Directory Service API prend en charge les autorisations au niveau des ressources basées sur des balises :

- [AcceptSharedDirectory](#)
- [AddIpRoutes](#)
- [AddTagsToResource](#)
- [CancelSchemaExtension](#)
- [CreateAlias](#)
- [CreateComputer](#)
- [CreateConditionalForwarder](#)
- [CreateSnapshot](#)
- [CreateLogSubscription](#)
- [CreateTrust](#)
- [DeleteConditionalForwarder](#)
- [DeleteDirectory](#)
- [DeleteLogSubscription](#)
- [DeleteSnapshot](#)
- [DeleteTrust](#)
- [DeregisterEventTopic](#)
- [DescribeConditionalForwarders](#)
- [DescribeDomainControllers](#)
- [DescribeEventTopics](#)
- [DescribeSharedDirectories](#)
- [DescribeSnapshots](#)
- [DescribeTrusts](#)
- [DisableRadius](#)
- [DisableSso](#)
- [EnableRadius](#)

- [EnableSso](#)
- [GetSnapshotLimits](#)
- [ListIpRoutes](#)
- [ListSchemaExtensions](#)
- [ListTagsForResource](#)
- [RegisterEventTopic](#)
- [RejectSharedDirectory](#)
- [RemovelpRoutes](#)
- [RemoveTagsForResource](#)
- [ResetUserPassword](#)
- [RestoreFromSnapshot](#)
- [ShareDirectory](#)
- [StartSchemaExtension](#)
- [UnshareDirectory](#)
- [UpdateConditionalForwarder](#)
- [UpdateNumberOfDomainControllers](#)
- [UpdateRadius](#)
- [UpdateTrust](#)
- [VerifyTrust](#)

Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions

Lorsque vous configurez des politiques d'autorisation d'écriture et de [Contrôle d'accès](#) que vous pouvez attacher à une entité IAM (politiques basées sur une identité), vous pouvez utiliser le tableau [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#) comme référence. Chaque entrée d'API du inclut les éléments suivants :

- Le nom de chaque opération d'API
- Action ou actions correspondantes à chaque opération d'API dans lesquelles vous pouvez accorder des autorisations pour effectuer l'action
- La AWS ressource dans 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. Pour indiquer une action, utilisez le préfixe `ds:` suivi du nom de l'opération d'API (par exemple, `ds:CreateDirectory`). Certaines AWS applications peuvent nécessiter l'utilisation d'opérations d'API non publiques telles que `ds:AuthorizeApplication`, `ds:CheckAlias`, `ds:CreateIdentityPoolDirectory`, `ds:GetAuth` et `ds:UnauthorizeApplication` dans leurs politiques.

Certains ne Directory Service APIs peuvent être appelés que via le AWS Management Console. Ils ne sont pas publics APIs, dans le sens où ils ne peuvent pas être appelés par programmation, et ils ne sont fournis par aucun SDK. Ils acceptent les informations d'identification des utilisateurs. Ces opérations d'API incluent `ds:DisableRoleAccess`, `ds:EnableRoleAccess`, et `ds:UpdateDirectory`.

Vous pouvez utiliser des clés de condition AWS globales dans vos politiques Directory Service et celles relatives aux données du Directory Service pour exprimer des conditions. Pour obtenir la liste complète des AWS clés, consultez la section [Clés de condition globale disponibles](#) dans le guide de l'utilisateur IAM.

Directory Service API et autorisations requises pour les actions

AWS API Directory Service Data et autorisations requises pour les actions

Note

Pour spécifier une action, utilisez le `ds-data:` préfixe suivi du nom de l'opération d'API (par exemple, `ds-data:AddGroupMember`).

Opérations de l'API de données du Directory Service	Autorisations requises (Action d'API)	Ressources
AddGroupMember	<code>ds-data:AddGroupMember</code>	*
CreateGroup	<code>ds-data:CreateGroup</code>	*
CreateUser	<code>ds-data:CreateUser</code>	*
DeleteGroup	<code>ds-data>DeleteGroup</code>	*

Opérations de l'API de données du Directory Service	Autorisations requises (Action d'API)	Ressources
DeleteUser	ds-data:DeleteUser	*
DescribeGroup	ds-data:DescribeGroup	*
DescribeUser	ds-data:DescribeUser	*
DisableUser	ds-data:DisableUser	*
ListGroup	ds-data:ListGroup	*
ListGroupMembers	ds-data:ListGroupMembers	*
ListGroupsForMember	ds-data:ListGroups ForMember	*
ListUsers	ds-data:ListUsers	*
RemoveGroupMember	ds-data:RemoveGroupMember	*
SearchGroups	ds-data:DescribeGroup ds-data:SearchGroups	*
SearchUsers	ds-data:DescribeUser ds-data:SearchUsers	*
UpdateGroup	ds-data:UpdateGroup	*
UpdateUser	ds-data:UpdateUser	*

Rubriques connexes

- [Contrôle d'accès](#)

Clés de condition des données du Directory Service

Utilisez les clés de condition [des données du Directory Service](#) pour ajouter des instructions spécifiques aux utilisateurs et à l'accès au niveau du groupe. Cela permet aux utilisateurs de décider quels principaux peuvent effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément Condition, ou bloc Condition, vous permet de spécifier les conditions dans lesquelles une instruction est en vigueur. L'élément Condition est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que égal (=) ou inférieur à (<), pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments de condition dans une instruction ou plusieurs clés dans un seul élément de condition, vous les AWS évaluez à l'aide d'une opération logique ET. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération OR logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées. Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un utilisateur IAM à accéder à une ressource uniquement si celle-ci est associée à son nom d'utilisateur. Pour plus d'informations, consultez la section [Condition comportant plusieurs clés ou valeurs](#) dans le guide de l'utilisateur IAM.

Pour obtenir la liste des actions prenant en charge ces clés de condition, consultez la section [Actions définies par les données du AWS Directory Service](#) dans le Service Authorization Reference.

Note

Pour plus d'informations sur les autorisations au niveau des ressources basées sur des balises, consultez. [Utilisation des balises avec des politiques IAM](#)

ds-data : Nom SAMAccount

Fonctionne avec [les opérateurs de chaînes](#).

Utilisez cette clé pour autoriser ou interdire explicitement à un rôle IAM d'effectuer des actions sur des utilisateurs et des groupes spécifiques.

Important

Lorsque vous utilisez SAMAccountName ou MemberName, nous vous recommandons de spécifier ds-data:Identifier comme SAMAccountName. Cela empêche les futurs

identifiants pris en charge par AWS Directory Service DataSID, tels que ceux qui enfreignent les autorisations existantes.

La politique suivante interdit au principal IAM de décrire l'utilisateur joe ou le groupe joegroup.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDescribe",
      "Effect": "Deny",
      "Action": "ds-data:Describe*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe",
            "joegroup"
          ],
          "ds-data:identifiant": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

 Note

Cette clé de condition ne tient pas compte des majuscules et minuscules. Vous devez utiliser [StringEqualsIgnoreCase](#) ou [StringNotEqualsIgnoreCase](#) conditionner des opérateurs pour comparer les valeurs des chaînes, quelles que soient les majuscules.

DS-Data : identifiant

Fonctionne avec [les opérateurs de chaînes](#).

Utilisez cette clé pour définir l'identifiant à utiliser dans les autorisations de politique IAM. Actuellement, seul SAMAccountName est pris en charge.

La politique suivante permet au principal IAM de mettre à jour l'utilisateur joe.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateJoe",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe"
          ],
          "ds-data:identifiant": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

données DS : MemberName

Fonctionne avec [les opérateurs de chaînes](#).

Utilisez cette touche pour définir les membres sur lesquels des opérations peuvent être effectuées.

 Important

Lorsque vous utilisez `MemberName` ou `SAMAccountName`, nous vous recommandons de spécifier `ds-data:Identifier` comme `SAMAccountName`. Cela empêche les futurs identifiants pris en charge par Directory Service DataSID, tels que ceux qui enfreignent les autorisations existantes.

La politique suivante autorise le directeur IAM à agir à l'égard des membres `AddGroupMember` `joe` de n'importe quel groupe.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddJoe",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "joe"
        }
      }
    }
  ]
}
```

 Note

Cette clé de condition ne distingue pas les majuscules et minuscules. Vous devez utiliser [StringEqualsIgnoreCase](#) ou [StringNotEqualsIgnoreCase](#) conditionner des opérateurs pour comparer les valeurs des chaînes, quelles que soient les majuscules.

données DS : MemberRealm

Fonctionne avec [les opérateurs de chaînes](#).

Utilisez cette clé pour vérifier si la `ds-data:MemberRealm` valeur de la politique correspond au domaine membre indiqué dans la demande.

Note

Cette clé de condition ne distingue pas les majuscules et minuscules. Vous devez utiliser [StringEqualsIgnoreCase](#) ou [StringNotEqualsIgnoreCase](#) conditionner des opérateurs pour comparer les valeurs des chaînes, quelles que soient les majuscules.

La politique suivante permet au principal IAM d'appeler un `AddGroupMember` membre bob dans le domaine `ONE.TRU1.AMAZON.COM`.

Note

L'exemple suivant utilise uniquement la clé de `ds-data:MemberName` contexte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "addbob",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "bob",
          "ds-data:MemberRealm": "one.tru1.amazon.com"
        }
      }
    }
  ]
}
```

```
}
```

DS-Data : Realm

Fonctionne avec [les opérateurs de chaînes](#).

Utilisez cette clé pour vérifier si la `ds-data:Realm` valeur de la politique correspond au domaine qu'un principal IAM peut utiliser pour envoyer des demandes à Directory Service Data APIs.

Note

Cette clé de condition ne distingue pas les majuscules et minuscules. Vous devez utiliser [StringEqualsIgnoreCase](#) ou [StringNotEqualsIgnoreCase](#) conditionner des opérateurs pour comparer les valeurs des chaînes, quelles que soient les majuscules.

La politique suivante interdit au principal IAM d'appeler `ListUsers` le domaine `one.tru1.amazon.com`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyTrustedList",
      "Effect": "Deny",
      "Action": "ds-data:ListUsers",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:Realm": [
            "one.tru1.amazon.com"
          ]
        }
      }
    }
  ]
}
```

Autorisation pour AWS les applications et les services utilisant Directory Service

Cette rubrique décrit l'autorisation pour les AWS applications et les services utilisant AWS Directory Service des données de AWS Directory Service.

Autoriser une AWS application sur un Active Directory

Directory Service accorde des autorisations spécifiques aux applications sélectionnées afin de s'intégrer parfaitement à votre Active Directory lorsque vous autorisez une AWS application. AWS les applications ne bénéficient que de l'accès nécessaire à leurs cas d'utilisation spécifiques. Voici un ensemble d'autorisations internes accordées aux applications et aux administrateurs d'applications après autorisation :

Note

L'`ds:AuthorizationApplicationautorisation` est requise pour autoriser une nouvelle AWS application pour un Active Directory. Les autorisations relatives à cette action ne doivent être accordées qu'aux administrateurs qui configurent les intégrations avec Directory Service.

- Accès en lecture aux données des utilisateurs, des groupes, des unités organisationnelles, des ordinateurs ou des autorités de certification Active Directory dans toutes les unités organisationnelles (UO) des annuaires AWS Managed Microsoft AD, Simple AD, AD Connector, ainsi que dans les domaines approuvés pour AWS Managed Microsoft AD si une relation de confiance l'autorise.
- Accès en écriture aux utilisateurs, aux groupes, aux membres de groupes, aux ordinateurs ou aux données d'autorité de certification dans votre unité organisationnelle de AWS Managed Microsoft AD. Accès en écriture à toutes les UO de Simple AD.
- Authentification et gestion de session des utilisateurs d'Active Directory pour tous les types d'annuaires.

Certaines applications Microsoft AD AWS gérées, telles qu'Amazon RDS et Amazon FSx s'intègrent via une connexion réseau directe à votre Active Directory. Dans ce cas, les interactions d'annuaire utilisent des protocoles Active Directory natifs tels que LDAP et Kerberos. Les autorisations de ces AWS applications sont contrôlées par un compte utilisateur d'annuaire créé dans l'unité

organisationnelle AWS réservée (UO) lors de l'autorisation de l'application, qui inclut la gestion du DNS et l'accès complet à une unité d'organisation personnalisée créée pour l'application. Pour utiliser ce compte, l'application doit être autorisée à agir ds: `GetAuthorizedApplicationDetails` via les informations d'identification de l'appelant ou un rôle IAM.

Pour plus d'informations sur les autorisations d' Directory Service API, consultez [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

Pour plus d'informations sur l'activation AWS des applications et des services pour AWS Managed Microsoft AD, consultez [Accès aux AWS applications et aux services depuis votre Microsoft AD AWS géré](#). Pour plus d'informations sur l'activation AWS des applications et des services pour Simple AD, consultez [Accès aux AWS applications et aux services depuis votre Simple AD](#). Pour plus d'informations sur l'activation AWS des applications et des services pour AD Connector, consultez [Accès aux AWS applications et aux services depuis AD Connector](#).

Annulation de l'autorisation d'une AWS application sur un Active Directory

L' `ds:UnauthorizedApplication` autorisation est requise pour supprimer les autorisations permettant à une AWS application d'accéder à un Active Directory. Suivez la procédure fournie par l'application pour le désactiver.

AWS autorisation d'application avec Directory Service Data

Pour les annuaires Microsoft AD AWS gérés, l'API Directory Service Data (ds-data) fournit un accès programmatique aux tâches de gestion des utilisateurs et des groupes. Le modèle d'autorisation des AWS applications est distinct des contrôles d'accès aux données du service de répertoire, ce qui signifie que les politiques d'accès aux actions relatives aux données du service de répertoire n'ont aucune incidence sur l'autorisation des AWS applications. Le fait de refuser l'accès à un répertoire dans ds-data n'interrompra pas l'intégration de l' AWS application ni les cas d'utilisation des applications. AWS

Lorsque vous rédigez des politiques d'accès pour les annuaires Microsoft AD AWS gérés qui autorisent AWS les applications, sachez que les fonctionnalités relatives aux utilisateurs et aux groupes peuvent être disponibles en appelant une AWS application ou une API de données de service de répertoire autorisée. Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon Quick Suite et Amazon Chime proposent tous des actions de gestion des utilisateurs et des groupes dans leur. APIs Contrôlez l'accès à cette fonctionnalité de AWS l'application à l'aide de politiques IAM.

Exemples

Les extraits suivants montrent les méthodes incorrectes et correctes pour refuser des DeleteUser fonctionnalités lorsque AWS des applications, telles qu' WorkDocs Amazon WorkMail, sont autorisées dans l'annuaire.

Incorrect

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser"
    ],
    "Resource": "*"
  }]
}
```

Correct

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser",
      "workmail:DeleteUser",
      "workdocs:DeleteUser"
    ],
    "Resource": "*"
  }]
}
```

Utilisation des rôles liés aux services pour Directory Service

AWS Directory Service utilise des AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Directory Service. Les rôles liés au service sont prédéfinis par Directory Service 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 Directory Service car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Directory Service définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Directory Service peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation, qui ne peuvent être rattachées à aucune autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela vous évite de perdre l'accès à vos Directory Service ressources car vous ne pouvez pas supprimer par inadvertance les autorisations d'accès aux ressources.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez [Services AWS qui fonctionnent avec IAM](#).

Rubriques

- [Autorisations de rôle liées à un service pour Directory Service](#)
- [Création d'un rôle lié à un service pour Directory Service](#)
- [Modification d'un rôle lié à un service pour Directory Service](#)
- [Supprimer un rôle lié à un service pour Directory Service](#)
- [Régions prises en charge pour les rôles Directory Service liés à un service](#)

Autorisations de rôle liées à un service pour Directory Service

Directory Service utilise le rôle lié au service nommé `AWSServiceRoleForDirectoryService`— Permet de surveiller AWS les contrôleurs de domaine autogérés du client.

Le rôle lié à un service `AWSServiceRoleForDirectoryService` approuve les services suivants pour endosser le rôle :

- `ds.amazonaws.com`

La politique d'autorisations de rôle nommée `AWSDirectoryServiceServiceRolePolicy` Directory Service permet d'effectuer les actions suivantes sur les ressources spécifiées. Pour les autorisations de politique complètes, voir [AWSDirectoryServiceServiceRolePolicy](#) la référence des politiques AWS gérées.

- `ec2`— Permet au service de décrire les ressources réseau telles que les sous-réseaux VPCs, les groupes de sécurité et les interfaces réseau afin de valider les configurations de connectivité hybrides :
 - `ec2:DescribeAvailabilityZones`
 - `ec2:DescribeDhcpOptions`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`
 - `ec2:DescribeSecurityGroups`
 - `ec2:DescribeSubnets`
 - `ec2:DescribeVpcs`
- `ssm`— Permet au service d'envoyer et de surveiller les PowerShell guilabels aux contrôleurs de domaine locaux à des fins de surveillance et d'évaluation :
 - `ssm:Sendguilabel`
 - `ssm:Listguilabels`
 - `ssm:GetguilabelInvocation`
 - `ssm:DescribeInstanceInformation`
 - `ssm:GetConnectionStatus`

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles 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 Directory Service

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous autorisez le client AWS à surveiller les contrôleurs de domaine autogérés dans le AWS Management Console, le ou l' AWS API AWS CLI, vous Directory Service créez le rôle lié au service pour vous. Pour plus d'informations sur cette modification, consultez la section [Mises à jour des politiques](#).

 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. De même, si vous utilisiez le Directory Service service avant le 1er janvier 2017, date à laquelle il a commencé à prendre en charge les rôles liés au service, vous avez Directory Service créé le `AWSServiceRoleForDirectoryService` rôle dans votre compte. Pour en savoir plus, voir [Un nouveau rôle est apparu dans mon Compte AWS](#).

Modification d'un rôle lié à un service pour Directory Service

Directory Service ne vous permet pas de modifier le rôle `AWSServiceRoleForDirectoryService` 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 [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Directory Service

Si vous n'avez plus besoin d'utiliser une fonction 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 les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

 Note

Si le Directory Service service utilise le rôle au moment où vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer Directory Service les ressources utilisées par `AWSServiceRoleForDirectoryService`

- Pour supprimer votre répertoire, consultez [Suppression de votre Microsoft AD AWS géré](#).

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForDirectoryServiceservice`. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles Directory Service liés à un service

Directory Service ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Toutefois, Directory Service utilise le `AWSServiceRoleForDirectoryService` rôle uniquement dans les Régions AWS cas où vous pouvez vous inscrire à des annuaires hybrides.

Support régional optionnel à l'annuaire hybride

Nom de la région	Identité de la région	soutien à l'inscription
USA Est (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Europe (Stockholm)	eu-north-1	Oui
Moyen-Orient (Bahreïn)	me-south-1	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Europe (Paris)	eu-west-3	Oui
Asie-Pacifique (Jakarta)	ap-southeast-3	Oui
Afrique (Le Cap)	af-south-1	Oui
Europe (Irlande)	eu-west-1	Oui
Moyen-Orient (EAU)	me-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui

Nom de la région	Identité de la région	soutien à l'inscription
Asie-Pacifique (Hong Kong)	ap-east-1	Oui
Asie-Pacifique (Hyderabad)	ap-south-2	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Europe (Londres)	eu-west-2	Oui
Asie-Pacifique (Melbourne)	ap-southeast-4	Oui
Europe (Milan)	eu-south-1	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Espagne)	eu-south-2	Oui
Europe (Zurich)	eu-central-2	Oui

Connexion et surveillance AWS Directory Service

La bonne pratique consiste à surveiller votre organisation pour vous assurer que les modifications sont journalisées. Cela vous permet de vous assurer que tout changement inattendu peut être étudié et que les modifications indésirables peuvent être annulées. AWS Directory Service prend actuellement en charge les deux AWS services suivants, afin que vous puissiez surveiller votre organisation et les activités qui s'y déroulent.

- Amazon CloudWatch - Vous pouvez utiliser CloudWatch Events avec le type d'annuaire AWS Managed Microsoft AD. Pour de plus amples informations, veuillez consulter [Activation du transfert de CloudWatch journaux Amazon Logs pour AWS Managed Microsoft AD](#). En outre, vous pouvez utiliser CloudWatch les métriques pour surveiller les performances du contrôleur de domaine.

Pour de plus amples informations, veuillez consulter [Déterminer quand ajouter des contrôleurs de domaine avec des CloudWatch métriques](#).

- AWS CloudTrail
 - Vous pouvez l'utiliser CloudTrail avec tous les types de Directory Service répertoires. Pour de plus amples informations, veuillez consulter [Enregistrement des appels AWS Directory Service d'API à l'aide de AWS CloudTrail](#).
 - Vous pouvez l'utiliser CloudTrail avec AWS Managed Microsoft AD dans l'API Directory Service Data. Pour de plus amples informations, veuillez consulter [Journalisation AWS des appels d'API de données du Directory Service à l'aide de AWS CloudTrail](#).

Enregistrement des appels AWS Directory Service d'API à l'aide de AWS CloudTrail

L'API AWS Managed Microsoft AD est intégrée à AWS CloudTrail un service qui capture les appels d'API effectués par ou pour le compte de AWS Managed Microsoft AD dans votre Compte AWS répertoire et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. CloudTrail capture les appels d'API depuis la console AWS Managed Microsoft AD et depuis les appels de code vers AWS Managed Microsoft AD APIs. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer quelle demande a été envoyée à AWS Managed Microsoft AD, l'adresse IP source à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite, etc. Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

AWS Informations Microsoft AD gérées dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Managed Microsoft AD, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements survenus dans votre environnement Compte AWS, y compris ceux relatifs AWS à Managed Microsoft AD, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au

compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Vue d'ensemble de la création d'un journal d'activité](#)
- [CloudTrail Services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Lorsque la CloudTrail journalisation est activée dans votre Compte AWS compte, tous les appels d'API effectués aux actions AWS Managed Microsoft AD sont suivis dans des fichiers journaux. AWS Les enregistrements Microsoft AD gérés sont écrits avec les autres enregistrements AWS de service dans un fichier journal. CloudTrail détermine à quel moment créer et écrire dans un nouveau fichier en fonction d'une période et de la taille du fichier. Tous les appels effectués vers l' Directory Service API ou les appels CLI sont enregistrés par CloudTrail.

Chaque entrée du journal contient des informations sur la personne qui a généré la demande. Les informations d'identité utilisateur contenues dans le journal vous aident à déterminer si la demande a été faite avec les informations d'identification de l'utilisateur root ou IAM, avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré, ou par un autre AWS service. Pour plus d'informations, reportez-vous au champ `userIdentity` dans le [Guide de référence des événements CloudTrail](#).

Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez, mais vous pouvez également définir des règles de cycle de vie Amazon S3 pour archiver ou supprimer automatiquement les fichiers journaux. Par défaut, vos fichiers journaux sont chiffrés à l'aide du chiffrement côté serveur (SSE) d'Amazon S3.

Vous pouvez choisir de CloudTrail publier des notifications Amazon SNS lorsque de nouveaux fichiers journaux sont livrés si vous souhaitez agir rapidement lors de la livraison des fichiers journaux. Pour de plus amples informations, veuillez consulter [Configuration des notifications Amazon SNS](#).

Vous pouvez également agréger les fichiers journaux Microsoft AD AWS gérés provenant de plusieurs AWS régions Comptes AWS dans un seul compartiment Amazon S3. Pour plus d'informations, consultez la section [Agrégation de fichiers CloudTrail journaux dans un seul compartiment Amazon S3](#).

Comprendre les entrées de fichiers journaux Microsoft AD AWS gérées

CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal, chaque entrée étant composée de plusieurs événements au format JSON. Une entrée de journal représente une demande individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, sur tous les paramètres, sur la date et l'heure de l'action, etc. Il n'est pas garanti que les entrées du journal soient dans un ordre particulier, c'est-à-dire qu'elles ne constituent pas une trace ordonnée des appels d'API publics.

Les informations sensibles, telles que les mots de passe, les jetons d'authentification, les commentaires sur les fichiers et le contenu des fichiers, sont consignées dans les entrées de journal.

L'exemple suivant montre un exemple d'entrée de CloudTrail journal pour AWS Managed Microsoft AD :

```
{
  "Records" : [
    {
      "eventVersion" : "1.02",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "<user_id>",
        "arn" : "<user_arn>",
        "accountId" : "<account_id>",
        "accessKeyId" : "<access_key_id>",
        "userName" : "<username>"
      },
      "eventTime" : "<event_time>",
      "eventSource" : "ds.amazonaws.com",
      "eventName" : "CreateDirectory",
      "awsRegion" : "<region>",
      "sourceIPAddress" : "<IP_address>",
      "userAgent" : "<user_agent>",
      "requestParameters" :
      {
        "name" : "<name>",
        "shortName" : "<short_name>",
        "vpcSettings" :
        {
          "vpcId" : "<vpc_id>",
          "subnetIds" : [
```

```

        "<subnet_id_1>",
        "<subnet_id_2>"
    ]
},
"type" : "<size>",
"setAsDefault" : <option>,
"password" : "****OMITTED****"
},
"responseElements" :
{
    "requestId" : "<request_id>",
    "directoryId" : "<directory_id>"
},
"requestID" : "<request_id>",
"eventID" : "<event_id>",
"eventType" : "AwsApiCall",
"recipientAccountId" : "<account_id>"
}
]
}

```

Journalisation AWS des appels d'API de données du Directory Service à l'aide de AWS CloudTrail

AWS Directory Service Data s'intègre AWS CloudTrail à un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Directory Service Data. CloudTrail capture tous les appels d'API pour les données du Directory Service sous forme d'événements. Les appels capturés incluent des appels provenant de la console Directory Service Data et des appels de code vers les opérations de l'API Directory Service Data. Si vous créez un suivi, vous pouvez activer la diffusion continue d'événements CloudTrail vers un compartiment Amazon S3, y compris des événements pour Directory Service Data. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Directory Service Data, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur les données du service de répertoire dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité événementielle prise en charge (événements de gestion) se produit dans Directory Service

Data, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements de gestion des 90 derniers jours dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#). La consultation de l'historique des événements est gratuite.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements relatifs à Directory Service Data, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les actions relatives aux données du service de répertoire sont enregistrées CloudTrail et documentées dans le manuel de [référence de l'API de données du service de répertoire](#). Par exemple, les appels au `AddGroupMember`, `DescribeUser` et les `SearchGroups` actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (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.

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#) .

Comprendre les entrées du fichier journal de données du Directory Service

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'[CreateUser](#) action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T18:22:38Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-05-30T19:17:03Z",
  "eventSource": "ds.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "ap-northeast-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
  "requestParameters": {
```

```
"directoryId": "d-1234567890",
"sAMAccountName": "johnsmith",
"clientToken": "example_token"
"emailAddress": "HIDDEN_DUE_TO_SECURITY_REASONS",
"givenName": "HIDDEN_DUE_TO_SECURITY_REASONS",
"surname": "HIDDEN_DUE_TO_SECURITY_REASONS",
"otherAttributes": {
  "physicalDeliveryOfficeName": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "telephoneNumber": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "streetAddress": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "displayName": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "homePhone": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "postalCode": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "description": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  }
},
"clientToken": "createUserToken4"
},
"responseElements": {
  "directoryId": "d-1234567890",
  "sID": "S-1-5-21-1234567890-123456789-123456789-1234",
  "sAMAccountName": "johnsmith"
},
"additionalEventData": {
  "SID": "S-1-5-21-1234567890-123456789-123456789-1234"
},
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": false,
"resources": [
  {
```

```

        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444",
"eventCategory": "Management",
"tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
}
},

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'[ListUsers](#) action.

Les actions qui ne créent ni ne modifient un objet renvoient une réponse nulle.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T18:22:52Z",
    "eventSource": "ds.amazonaws.com",

```

```

    "eventName": "ListUsers",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-users",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1244",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'[ListGroups](#) action.

Note

L'`NextToken` élément est supprimé de toutes les entrées du journal.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",

```

```
"principalId": "1234567890abcdef0:admin-role",
"arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
"accountId": "111222333444",
"accessKeyId": "021345abcdef6789",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::111222333444:role/AdAdmin",
    "accountId": "111222333444",
    "userName": "AdAdmin"
  },
  "attributes": {
    "creationDate": "2023-05-30T18:22:38Z",
    "mfaAuthenticated": "false"
  }
},
"eventTime": "2023-05-30T18:29:15Z",
"eventSource": "ds.amazonaws.com",
"eventName": "ListGroup",
"awsRegion": "ap-northeast-2",
"sourceIPAddress": "10.24.34.0",
"userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-groups",
"requestParameters": {
  "directoryId": "d-1234567890",
  "nextToken": "REDACTED",
  "maxResults": 1
},
"responseElements": null,
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": true,
"resources": [
  {
    "accountId": "111222333444",
    "type": "AWS::DirectoryService::MicrosoftAD",
    "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444",
```

```
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
}
}
```

Entrées de journal pour les erreurs d'exception

L'exemple suivant montre une entrée de CloudTrail journal pour une erreur d'accès refusé. Pour obtenir de l'aide concernant cette erreur, consultez la section [Résolution des messages d'erreur relatifs au refus d'accès](#) dans le Guide de l'utilisateur IAM.

Note

Le journal des accès refusés n'affiche pas les paramètres des demandes.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-31T23:25:49Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-05-31T23:38:18Z",
```

```

    "eventSource": "ds.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
    "errorCode": "AccessDenied",
    "errorMessage": "User: arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-
role is not authorized to perform: ds-data:CreateUser on resource: arn:aws:ds:ap-
northeast-2:111222333444:directory/d-1234567890 because no identity-based policy allows
the ds-data:CreateUser action",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
  }
}

```

L'exemple suivant montre une entrée de CloudTrail journal pour une erreur Resource Not Found.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",

```

```

    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T20:41:50Z",
        "mfaAuthenticated": "false"
      }
    },
    "eventTime": "2023-05-30T21:10:16Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "DescribeUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.describe-user",
    "errorCode": "ResourceNotFoundException",
    "errorMessage": "User not found in directory d-1234567890.",
    "requestParameters": {
      "directoryId": "d-1234567890",
      "sAMAccountName": "nonExistingUser",
      "otherAttributes": [
        "co",
        "givenName",
        "sn",
        "telephoneNumber"
      ]
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
      }
    ]
  }

```



```
],  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "111222333444"  
  "eventCategory": "Management",  
  "tlsDetails": {  
    "tlsVersion": "TLSv1.3",  
    "cipherSuite": "TLS_AES_128_GCM_SHA256",  
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"  
  }  
}
```

Validation de conformité pour AWS Directory Service

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](#).

Résilience dans AWS Directory Service

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Outre l'infrastructure AWS mondiale, Directory Service offre la possibilité de prendre des instantanés manuels des données à tout moment pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour de plus amples informations, veuillez consulter [Restauration de votre Microsoft AD AWS géré à l'aide de snapshots](#).

Sécurité de l'infrastructure dans AWS Directory Service

En tant que service géré, AWS Directory Service il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). 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 Directory Service via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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 la confusion des 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 avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition [aws:SourceAccount](#) globale [aws:SourceArn](#) et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui, Directory Service pour Microsoft Active Directory, octroient un autre service à la ressource. Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de

compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations. Si vous utilisez les deux clés de contexte de condition globale et que la valeur `aws:SourceArn` contient l'ID de compte, la valeur `aws:SourceAccount` et le compte dans la valeur `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'ils sont utilisés dans la même instruction de politique. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Dans l'exemple suivant, la valeur de `aws:SourceArn` doit être un groupe de CloudWatch journaux.

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 suivant montre comment utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans AWS Managed Microsoft AD pour éviter le problème de confusion des adjoints.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:111122223333:log-group:/aws/
directoryservice/Log_Group_Name:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/Directory_Name"
```

```

    },
    "StringEquals": {
        "aws:SourceAccount": "111122223333"
    }
}
}
}

```

Dans l'exemple suivant, la valeur de `aws:SourceArn` doit être une rubrique SNS de votre compte. Par exemple, vous pouvez utiliser quelque chose comme `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` « `ap-southeast-1` » correspondant à votre région, « `123456789012` » à votre identifiant client et « `_d-966739499f` » au nom de rubrique Amazon SNS que vous avez créé. `DirectoryMonitoring`

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 suivant montre comment utiliser les clés contextuelles `aws:SourceArn` et les clés de contexte de condition `aws:SourceAccount` globale dans AWS Managed Microsoft AD pour éviter le problème de confusion des adjoints.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
      "SNS:GetTopicAttributes",
      "SNS:SetTopicAttributes",
      "SNS:AddPermission",
      "SNS:RemovePermission",
      "SNS:DeleteTopic",
      "SNS:Subscribe",

```

```

        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish"
    ],
    "Resource": [
        "arn:aws:sns:us-east-1:111122223333:SNS_TOPIC_NAME"
    ],
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ds:us-east-1:111122223333:directory/EXTERNAL_DIRECTORY_ID"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
}

```

L'exemple suivant montre une politique d'approbations IAM pour un rôle auquel l'accès à la console a été délégué. La valeur de `aws:SourceArn` doit être une ressource d'annuaire de votre compte. Pour plus d'informations, consultez la section [Types de ressources définis par Directory Service](#). Par exemple, vous pouvez utiliser `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`, où 123456789012 correspond à votre identifiant client et d-1234567890 à votre identifiant d'annuaire.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-east-1:111122223333:directory/YOUR_DIRECTORY_ID"
            }
        }
    }
}

```

```
    },
    "StringEquals": {
        "aws:SourceAccount": "111122223333"
    }
}
}
```

Directory Service API et interface : points de terminaison Amazon VPC utilisant AWS PrivateLink

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC Directory Service et Directory Service Data. APIs Cela vous permet d'accéder Directory Service aux données du Service d'annuaire APIs comme si elles se trouvaient dans votre VPC, sans passer par une passerelle Internet, un périphérique NAT, une connexion VPN ou Direct Connect une connexion. Les instances de votre Amazon VPC n'ont pas besoin d'adresses IP publiques pour accéder aux données Directory Service du Directory Service. APIs

Pour établir une connexion privée, vous créez une interface Amazon VPC endpoint qui AWS PrivateLink alimente. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par les demandeurs, qui servent de point d'entrée pour le trafic destiné aux données AWS Directory Service de AWS Directory Service.

Pour plus d'informations, consultez la section [Accès Services AWS par AWS PrivateLink le biais](#) du AWS PrivateLink guide.

Considérations relatives Directory Service aux données du Directory Service

Avec Directory Service and Directory Service Data, vous pouvez appeler des actions d'API via les points de terminaison de l'interface. Pour plus d'informations sur les prérequis à prendre en compte avant de créer un point de terminaison d'interface, consultez la section [Accès et Service AWS utilisation d'un point de terminaison Amazon VPC d'interface](#) dans AWS PrivateLink le Guide.

Directory Service et disponibilité des données du Directory Service

Directory Service prend en charge les points de terminaison d'interface suivants : Régions AWS

- USA Est (Virginie du Nord)
- AWS GovCloud (USA Est)
- AWS GovCloud (US-Ouest)

Directory Service Data prend en charge les points de terminaison d'interface partout Régions AWS où ils sont disponibles. Pour plus d'informations sur Régions AWS ce support Directory Service et les données du Directory Service, consultez [la section Disponibilité des régions pour Directory Service](#).

Création d'une interface (point de terminaison Amazon VPC) pour Directory Service les données du Directory Service

Vous pouvez créer un point de terminaison d'interface pour Directory Service et les données du service de répertoire APIs à l'aide de la console Amazon VPC ou du AWS Command Line Interface (AWS CLI).

Exemple : Directory Service

Créez un point de terminaison d'interface pour Directory Service APIs utiliser le nom de service suivant :

```
com.amazonaws.region.ds
```

Exemple : données du Directory Service

Créez un point de terminaison d'interface pour Directory Service Data APIs en utilisant le nom de service suivant :

```
com.amazonaws.region.ds-data
```

Pour plus d'informations sur la création d'un point de terminaison d'interface, consultez la section [Accès et Service AWS utilisation d'un point de terminaison Amazon VPC](#) dans le AWS PrivateLink Guide.

Créez une politique de point de terminaison Amazon VPC pour votre interface (point de terminaison Amazon VPC)

Une stratégie de point de terminaison est une politique de ressources IAM que vous attachez à un point de terminaison d'interface.

 Note

Si vous n'associez pas de politique de point de terminaison à votre point de terminaison d'interface, AWS PrivateLink associe une politique de point de terminaison par défaut à votre point de terminaison d'interface en votre nom. Pour plus d'informations, consultez [Concepts AWS PrivateLink](#).

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux (Comptes AWS utilisateurs IAM et rôles IAM) qui peuvent effectuer des actions
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être effectuées

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 .

Vous pouvez contrôler l'accès APIs depuis votre Amazon VPC en attachant une politique de point de terminaison personnalisée à votre point de terminaison d'interface.

Exemple : politique de point de terminaison Amazon VPC pour les actions d'API Directory Service

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux Directory Service actions répertoriées à tous les principaux sur toutes les ressources.

Remplacez *action-1* *action-2*, et *action-3* par les autorisations requises pour Directory Service APIs ce que vous souhaitez inclure dans votre politique. Pour obtenir une liste complète, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds:action-1",
        "ds:action-2",
```



```
        "ds:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple : politique de point de terminaison Amazon VPC pour les actions de l'API Directory Service Data

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux actions de données du service de répertoire répertoriées pour tous les principaux sur toutes les ressources.

Remplacez *action-1**action-2*, et *action-3* par les autorisations requises pour les données de Directory Service APIs que vous souhaitez inclure dans votre politique. Pour obtenir une liste complète, veuillez consulter [Directory Service Autorisations d'API : référence aux actions, aux ressources et aux conditions](#).

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds-data:action-1",
        "ds-data:action-2",
        "ds-data:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

Contrat de niveau de service pour Directory Service

Directory Service est un service à haute disponibilité qui repose sur une infrastructure AWS gérée. Il est soutenu par un accord de niveau de service (SLA) qui définit notre politique de disponibilité des services.

- Le SLA s'applique à AWS Managed Microsoft AD, AD Connector et Simple AD.
- Le SLA traite des crédits de service, des exclusions du SLA et définit des termes tels que « répertoire couvert », « pourcentage de disponibilité mensuel » et « demandes ».
- Pour plus d'informations, veuillez consulter [Service level agreement for Directory Service](#) (français non garanti).

Disponibilité de la région pour Directory Service

Le tableau suivant propose une liste décrivant les points de terminaison spécifiques à la région pris en charge par type d'annuaire.

Nom de la région	Région	Point de terminaison	Protocole	AWS Managed Microsoft AD (Standard et Enterprise)	AWS Managed Microsoft AD (hybride)	AD Connector	Simple AD
USA Est (Virginie du Nord)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui
USA Est (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
USA Ouest (Californie du Nord)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
USA Ouest (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui

Nom de la région	Région	Point de terminaison	Protocole	AWS Managed Microsoft AD (éditions Standard et Enterprise)	AWS Managed Microsoft AD (édition hybride)	AD Connect	Simple AD
Afrique (Le Cap)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 O	 O	 O	 Non
Asie-Pacifique (Hong Kong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 O	 O	 O	 Non
Asie-Pacifique (Taïpei)	ap-east-2	ds.ap-east-2.amazonaws.com	HTTPS	 O	 N	 O	 Non
Asie-Pacifique (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 O	 O	 O	 Non
Asie-Pacifique (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 O	 O	 O	 Non

Nom de la région	Région	Point de terminaison	Protoco	AWS Microso AD géré (éditions Standard et Enterprise)	AWS Microso AD géré (édition hybride)	AD Con	Simple AD
Asie-Pacifique (Malaisie)	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	 Oui	 Non	 Oui	 Non
Asie-Pacifique (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Asie-Pacifique (Thaïlande)	ap-southeast-7	ds.ap-southeast-7.amazonaws.com	HTTPS	 Oui	 Non	 Oui	 Non
Asie-Pacifique (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Asie-Pacifique (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré (éditions Standard et Enterprise)	AWS Microsoft AD géré (édition hybride)	AD Connect	Simple AD
Asie-Pacifique (Séoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Asie-Pacifique (Singapour)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui
Asie-Pacifique (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui
Canada (Centre)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Canada Ouest (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 Oui	 Non	 Oui	 Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré (éditions Standard et Enterprise)	AWS Microsoft AD géré (édition hybride)	AD Connect	Simple AD
Chine (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 Oui	 Non	 Oui	 Non
Chine (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 Oui	 Non	 Oui	 Non
Europe (Francfort)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Europe (Irlande)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Oui
Europe (Londres)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Europe (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non

Nom de la région	Région	Point de terminaison	Protoco	AWS Microso AD géré (éditions Standard et Enterprise)	AWS Microso AD géré (édition hybride)	AD Con	Simple AD
Europe (Espagne)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	 O	 O	 O	 Non
Europe (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	 O	 O	 O	 Non
Europe (Zurich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 O	 O	 O	 Non
Israël (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 O	 N	 O	 Non
Mexique (centre)	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	 O	 N	 O	 Non
Moyen-Orient (Bahreïn)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 O	 O	 O	 Non
Moyen-Orient (EAU)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 O	 O	 O	 Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Managed Microsoft AD (éditions Standard et Enterprise)	AWS Managed Microsoft AD (édition hybride)	AD Connect	Simple AD
Amérique du Sud (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 Oui	 Oui	 Oui	 Non
AWS GovCloud (US-Ouest)	us-gov-west-1	ds.us-gov-west-1.amazonaws.com	HTTPS	 Oui	 Non	 Oui	 Non
AWS GovCloud (USA Est)	us-gov-east-1	ds.us-gov-east-1.amazonaws.com	HTTPS	 Oui	 Non	 Oui	 Non

Pour plus d'informations sur l'utilisation Directory Service dans la région AWS GovCloud (ouest des États-Unis) et dans la région AWS GovCloud (est des États-Unis), consultez la section [Points de terminaison du service](#) dans le guide de l'AWS GovCloud (US) utilisateur.

Pour plus d'informations sur l'utilisation Directory Service dans les régions de Pékin et du Ningxia, consultez [Endpoints et ARNs pour Amazon Web Services en Chine](#) dans Getting started with in AWS China.

Pour plus d'informations sur les points de terminaison FIPS pris en charge par Directory Service Data, consultez la section [Points de terminaison et quotas des données de service d'annuaire](#) dans le Références générales AWS Guide de référence.

Pris en charge Régions AWS pour les données du Directory Service

Le tableau suivant fournit une liste des points de terminaison spécifiques à une région pris en charge par Directory Service Data par type d'annuaire.

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Contr	Simple AD
USA Est (Ohio)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	 O	 N	 Non
USA Est (Virginie du Nord)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	 O	 N	 Non
USA Ouest (Californie du Nord)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	 O	 N	 Non
USA Ouest (Oregon)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	 O	 N	 Non
Asie-Paci	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	 O	 N	 Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Contr	Simple AD
Asie-Pacifique (Hong Kong)						
Asie-Pacifique (Mumbai)	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	 Oui	 Non	 Non
Asie-Pacifique (Osaka)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	 Oui	 Non	 Non
Asie-Pacifique (Séoul)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	 Oui	 Non	 Non
Asie-Pacifique (Singapour)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	 Oui	 Non	 Non
Asie-Pacifique (Sydney)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	 Oui	 Non	 Non

Nom de la région	Région	Point de terminaison	Protocole	AWS Microsoft AD géré	AD Contr	Simple AD
Asie-Pacifique (Tokyo)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	 O	 N	 Non
Canada (Centre)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	 O	 N	 Non
Europe (Francfort)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	 O	 N	 Non
Europe (Irlande)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	 O	 N	 Non
Europe (Londres)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	 O	 N	 Non
Europe (Paris)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	 O	 N	 Non
Europe (Stockholm)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	 O	 N	 Non
Amérique du Sud (São Paulo)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	 O	 N	 Non

Pour plus d'informations sur les points de terminaison FIPS pris en charge par Directory Service Data, consultez la section [Points de terminaison et quotas des données de service d'annuaire](#) dans le Références générales AWS Guide de référence.

Compatibilité du navigateur pour AWS Directory Service

AWS les applications et services tels qu'Amazon WorkSpaces WorkMail, Amazon Connect, Amazon Chime WorkDocs, etc. nécessitent des AWS IAM Identity Center informations de connexion valides provenant d'un navigateur compatible avant de pouvoir y accéder. Le tableau suivant décrit uniquement les navigateurs et les versions de navigateur compatibles pour les connexions.

Navigateur	Version	Compatibilité
Microsoft Edge	Les 3 dernières versions	Compatible
Mozilla Firefox	Les 3 dernières versions	Compatible
Google Chrome	Les 3 dernières versions	Compatible
Apple Safari	Les 3 dernières versions	Compatible

Maintenant que vous avez vérifié que vous utilisez une version compatible de votre navigateur, nous vous recommandons de consulter également la section ci-dessous pour vérifier que votre navigateur a été configuré pour utiliser le paramètre Transport Layer Security (TLS) requis par AWS.

Qu'est-ce que TLS ?

TLS est un protocole utilisé par des navigateurs Web et d'autres applications pour échanger des données en toute sécurité sur un réseau. TLS permet de s'assurer qu'une connexion à un point de terminaison distant correspond au point de terminaison prévu via le chiffrement et la vérification d'identité du point de terminaison. À ce jour, les versions de TLS disponibles sont TLS 1.0, 1.1, 1.2 et 1.3.

Quelles sont les versions de TLS prises en charge par l'IAM Identity Center ?

AWS les applications et les services prennent en charge les protocoles TLS 1.1, 1.2 et 1.3 pour les connexions sécurisées. À compter du 30 octobre 2019, TLS 1.0 n'est plus pris en charge. Il est donc important que tous les navigateurs soient configurés pour prendre en charge TLS 1.1 ou version

ultérieure. En d'autres termes, vous ne serez pas en mesure de vous connecter à des applications et services AWS si vous y accédez alors que TLS 1.0 est activé. Pour obtenir de l'aide relative à cette modification, contactez votre administrateur.

Comment puis-je activer les versions de TLS prises en charge dans mon navigateur

Cela dépend de votre navigateur. Généralement, vous devez accéder aux paramètres avancés dans les paramètres de votre navigateur. Par exemple, dans Internet Explorer, vous trouverez différentes options TLS sous Propriétés Internet, dans l'onglet Avancé, puis dans la section Sécurité. Consultez le site d'aide du fabricant de votre navigateur pour obtenir des instructions spécifiques.

Historique du document

Le tableau suivant décrit les modifications significatives apportées depuis la publication du Guide de l'administrateur AWS Directory Service .

Modification	Description	Date
Support de type réseau à double pile	AWS Directory Service prend désormais en charge la mise à niveau du type de réseau d'annuaire IPv4 vers un réseau à double pile (IPv4 et IPv6). Cette fonctionnalité fournit un espace d'adressage plus large et permet IPv6 la connectivité de vos annuaires . Vous pouvez également mettre à jour vos annuaires AD Connector et Simple AD grâce à la prise en charge du double stack.	30 septembre 2025
Nouveau rôle lié à un AWS service	Directory Service ajoute un nouveau rôle lié au AWS service AWSServiceRoleForDirectoryService et une nouvelle politique AWS gérée AWSDirectoryServiceServiceRolePolicy. La politique permet AWS de surveiller les contrôleurs de domaine gérés par le client.	30 juillet 2025
AWS Microsoft AD géré (édition hybride)	AWS Managed Microsoft AD (Hybrid Edition) connecte votre Active Directory autogéré à AWS Directory Service pour Microsoft Active Directory,	30 juillet 2025

créant ainsi un environnement d'identité intégré couvrant à la fois votre infrastructure et le AWS Cloud.

[Rubrique de journalisation et de surveillance mise à jour - nouvelles sections](#)

Des sections AWS Directory Service et des données de AWS Directory Service ont été incluses dans la rubrique consacrée à la journalisation et à la surveillance.

18 septembre 2024

[Nouvelle API et nouveaux attributs de données du Directory Service](#)

AWS Directory Service Data fournit une gestion intégrée des objets. Vous pouvez désormais rechercher et mettre à jour des objets avec une [liste des attributs AD pris en charge](#).

18 septembre 2024

[AWS politiques gérées - nouvelles politiques](#)

AWS Directory Service Data ajoute de nouvelles politiques AWS gérées : AWSDirectoryServiceDataFullAccess et AWSDirectoryServiceDataReadOnlyAccess. Les politiques accordent l'accès à la gestion des objets de Directory Service Data.

18 septembre 2024

[Paramètres d'authentification basés sur des certificats](#)

Ajout de contenu concernant deux nouveaux paramètres de sécurité pour AWS Managed Microsoft AD.

11 avril 2023

[AWS PrivateLink](#)

Ajout de contenu concernant AWS PrivateLink.

31 mars 2023

Points de terminaison d'un VPC Simple AD	Ajout de contenu indiquant quels points de terminaison d'un VPC ne doivent pas être configurés.	25 août 2021
Points de terminaison d'un VPC AD Connector	Ajout de contenu indiquant quels points de terminaison d'un VPC ne doivent pas être configurés.	25 août 2021
Prendre en charge des cartes intelligentes	Ajout de contenu sur la prise en charge des cartes à puce et d'Amazon WorkSpaces Application Manager dans la AWS GovCloud région (ouest des États-Unis)	1er décembre 2020
Réinitialisation du mot de passe	Ajout de contenu expliquant comment réinitialiser les mots de passe des utilisateurs à AWS Management Console l'aide PowerShell AWS CLI des	2 janvier 2019
Partage d'annuaire	Ajout de contenu expliquant comment utiliser le partage d'annuaires avec AWS Managed Microsoft AD.	25 septembre 2018
Contenu migré vers le nouveau Guide du développeur Amazon Cloud Directory	Le contenu d'Amazon Cloud Directory a été déplacé de ce guide vers le nouveau Guide du développeur Amazon Cloud Directory .	21 juin 2018

Révision de la table des matières du Guide de l'administrateur terminée	Contenu réorganisé pour répondre plus directement aux besoins du client. Du nouveau contenu a également été ajouté lorsqu'il était nécessaire.	5 avril 2018
AWS groupes délégués	Ajout de la liste des groupes AWS délégués pouvant être affectés aux utilisateurs locaux.	8 mars 2018
Stratégies de mot de passe affinées	Ajout de nouveau contenu sur les politiques de mot de passe.	5 juillet 2017
Contrôleurs de domaine supplémentaires	Ajout de contenu expliquant comment ajouter d'autres contrôleurs de domaine à votre annuaire dans AWS Managed Microsoft AD.	30 juin 2017
Didacticiels	Ajout de nouveaux didacticiels pour tester un environnement de laboratoire Microsoft AD AWS géré.	21 juin 2017
MFA avec AWS Microsoft AD géré	Ajout de contenu sur l'utilisation du MFA avec Managed AWS Microsoft AD.	13 février 2017
Amazon Cloud Directory	Ajout de contenu concernant un nouveau type d'annuaire.	26 janvier 2017
Extensions de schéma	Ajout de contenu sur les extensions de schéma avec AWS Directory Service pour Microsoft Active Directory.	14 novembre 2016

<u>Réorganisation majeure du guide de Directory Service l'administrateur</u>	Contenu réorganisé pour répondre plus directement aux besoins du client.	14 novembre 2016
<u>Notifications SNS</u>	Ajout de contenu sur les notifications SNS.	25 février 2016
<u>Autorisation et authentification</u>	Ajout de contenu expliquant comment utiliser IAM avec Directory Service.	25 février 2016
<u>AWS Microsoft AD géré</u>	Ajout de contenu sur AWS Managed Microsoft AD et de guides combinés en un seul guide.	17 novembre 2015
<u>Permettre aux instances Linux d'être jointes à un annuaire Simple AD</u>	Ajout de contenu expliquant comment joindre une instance Linux à un annuaire Simple AD.	23 juillet 2015
<u>Séparation de manuel</u>	Divisez le Guide de l'administrateur Directory Service en guides distincts.	14 juillet 2015
<u>Prise en charge de l'authentification unique</u>	Ajout de contenu sur la prise en charge de l'authentification unique.	31 mars 2015
<u>Nouveau guide</u>	Il s'agit de la première version du Guide de l'utilisateur AWS Directory Service .	21 octobre 2014

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.