aws

Guide de l’administrateur

Amazon WorkMail

Version 1.0

Amazon WorkMail: Guide de l’administrateur

Table of Contents

Qu'est-ce qu'Amazon WorkMail ?

Amazon WorkMail est un service de messagerie et de calendrier professionnel sécurisé et géré qui prend en charge les clients de messagerie de bureau et mobiles existants. WorkMail Les utilisateurs d'Amazon peuvent accéder à leurs e-mails, contacts et calendriers à l'aide de Microsoft Outlook, de leur navigateur ou de leurs applications de messagerie iOS et Android natives. Vous pouvez intégrer Amazon WorkMail à votre annuaire d'entreprise existant et contrôler à la fois les clés qui chiffrent vos données et l'emplacement dans lequel elles sont stockées.

Pour obtenir la liste des régions et points de terminaison AWS pris en charge, consultez Régions et points de terminaison AWS.

Rubriques

Configuration WorkMail système requise pour Amazon

Lorsque votre WorkMail administrateur Amazon vous invite à vous connecter à votre WorkMail compte Amazon, vous pouvez vous connecter à l'aide du client WorkMail Web Amazon.

Amazon fonctionne WorkMail également avec tous les principaux appareils mobiles et systèmes d'exploitation compatibles avec le ActiveSync protocole Exchange. Cela inclut notamment les appareils iPad, iPhone, Android et Windows Phone. Les utilisateurs de macOS peuvent ajouter leur WorkMail compte Amazon à leurs applications Mail, Agenda et Contacts.

Amazon WorkMail prend en charge les versions de système d'exploitation suivantes :

- Windows — Windows 7 SP1 ou version ultérieure
- macOS — macOS 10.12 (Sierra) ou version ultérieure
- Android — Andriod 5.0 ou version ultérieure
- iPhone — iOS 5 ou version ultérieure
- Windows Phone — Windows 8.1 ou version ultérieure

- Blackberry — Système d'exploitation Blackberry 10.3.3.3216

Si vous possédez une licence Microsoft Outlook valide, vous pouvez accéder à Amazon WorkMail en utilisant les versions suivantes de Microsoft Outlook :

- Outlook 2013 ou version ultérieure
- Outlook 2013 Click-to-Run ou version ultérieure
- Outlook pour Mac 2016 ou version ultérieure

Vous pouvez accéder au client WorkMail Web Amazon à l'aide des versions de navigateur suivantes :

- Google Chrome — Version 22 ou ultérieure
- Mozilla Firefox — Version 27 ou ultérieure
- Safari — Version 7 ou ultérieure
- Internet Explorer — Version 11
- Microsoft Edge

Vous pouvez également utiliser Amazon WorkMail avec votre client IMAP préféré.

WorkMail Concepts d'Amazon

La terminologie et les concepts essentiels à votre compréhension et à votre utilisation d'Amazon WorkMail sont décrits ci-dessous.

Organisation

Une configuration de locataire pour Amazon WorkMail.

Alias

Un nom global unique pour identifier votre organisation. L'alias est utilisé pour accéder à l'application WorkMail Web Amazon (https ://*alias*.awsapps.com/mail).

Domaine

Adresse Web qui suit le @ symbole dans une adresse e-mail. Vous pouvez ajouter un domaine recevant le courrier et l'envoyant aux boîtes aux lettres de votre organisation.

Domaine de messagerie test

Un domaine est automatiquement configuré lors de l'installation et peut être utilisé pour tester Amazon WorkMail. Le domaine de messagerie de test est *alias* .awsapps.com et est utilisé comme domaine par défaut si vous ne configurez pas votre propre domaine. Le domaine de messagerie test est soumis à diverses restrictions. Pour de plus amples informations, veuillez consulter WorkMail Quotas Amazon.

Annuaire

AWS Simple AD, AWS Managed AD ou AD Connector créé dans AWS Directory Service. Si vous créez une organisation à l'aide de la configuration WorkMail rapide d'Amazon, nous créons un WorkMail répertoire pour vous. Vous ne pouvez pas afficher un WorkMail répertoire dans AWS Directory Service.

Utilisateur

Un utilisateur créé dans le AWS Directory Service. L'utilisateur peut être créé dans un rôle USER ou REMOTE_USER. Lorsqu'un utilisateur est créé et activé avec le rôle USER, il reçoit sa propre boîte aux lettres à laquelle il peut accéder. Lorsqu'un utilisateur est désactivé, il ne peut pas accéder à Amazon WorkMail.

Les utilisateurs créés et activés avec le rôle REMOTE_USER sont répertoriés dans le carnet d'adresses, mais aucune boîte aux lettres n'est disponible sur Amazon. WorkMail Le REMOTE_USER peut avoir la boîte aux lettres hébergée en dehors d'Amazon, WorkMail mais il sera toujours répertorié comme tout autre utilisateur dont la boîte aux lettres figure dans le carnet d' WorkMail adresses Amazon et pourra consulter le calendrier de chacun pour trouver des informations gratuites ou occupées.

Groupe

Un groupe utilisé dans AWS Directory Service. Un groupe peut être utilisé comme liste de distribution ou groupe de sécurité sur Amazon WorkMail. Les groupes ne disposent pas de leur propre boîte aux lettres.

Ressource

Une ressource représente une salle de réunion ou un équipement pouvant être réservé par WorkMail les utilisateurs d'Amazon.

Politique relative aux appareils mobiles

Les différentes règles de politique informatique qui contrôlent les fonctions de sécurité et le comportement d'un dispositif mobile.

Services AWS connexes

Les services suivants sont utilisés conjointement avec Amazon WorkMail :

- AWS Directory Service—Vous pouvez intégrer Amazon WorkMail à un AWS Simple AD, AWS Managed AD ou AD Connector existant. Créez un répertoire dans le, AWS Directory Service puis activez Amazon WorkMail pour ce répertoire. Après avoir configuré cette intégration, vous pouvez choisir les utilisateurs que vous souhaitez activer pour Amazon dans la liste des utilisateurs WorkMail de votre annuaire existant, et les utilisateurs peuvent se connecter à l'aide de leurs informations d'identification Active Directory existantes. Pour plus d'informations, consultez le Guide AWS Directory Service d'administration.
- Amazon Simple Email Service : Amazon WorkMail utilise Amazon SES pour envoyer tous les e-mails sortants. Le domaine de messagerie de test et vos domaines peuvent être gérés dans la console Amazon SES. Les e-mails sortants envoyés depuis Amazon sont gratuits WorkMail. Pour plus d'informations, consultez le guide du développeur d'Amazon Simple Email Service.
- Gestion des identités et des accès AWS AWS Management Console —Nécessite votre nom d'utilisateur et votre mot de passe afin que tout service que vous utilisez puisse déterminer si vous êtes autorisé à accéder à ses ressources. Nous vous recommandons d'éviter d'utiliser les informations d'identification du compte AWS pour y accéder, AWS car les informations d'identification du AWS compte ne peuvent en aucun cas être révoquées ou limitées. Nous vous recommandons plutôt de créer un utilisateur IAM et de l'ajouter à un groupe IAM doté d'autorisations administratives. Vous pouvez ensuite accéder à la console à l'aide des informations d'identification de l'utilisateur IAM.

  Si vous êtes inscrit à AWS, mais que vous n'avez pas créé d'utilisateur IAM pour vous-même, vous pouvez le faire avec la console IAM. Pour plus d'informations, consultez la section Création d'utilisateurs IAM individuels dans le guide de l'utilisateur IAM.
- AWS Key Management Service—Amazon WorkMail est intégré AWS KMS pour le chiffrement des données des clients. La gestion des clés peut être effectuée depuis la AWS KMS console. Pour plus d'informations, consultez la section Que AWS Key Management Service contient le guide du AWS Key Management Service développeur ?

WorkMail Tarifs Amazon

Avec Amazon WorkMail, il n'y a aucun frais initial ni engagement. Vous ne payez que pour les comptes d'utilisateurs actifs. Pour des informations plus spécifiques sur la tarification, consultez la rubrique Tarification.

WorkMail Ressources Amazon

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

- Cours et ateliers — Liens vers des cours spécialisés et basés sur des rôles, ainsi que des ateliers à votre rythme pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Centre pour développeurs : découvrez les didacticiels, téléchargez des outils et découvrez les événements AWS destinés aux développeurs.
- AWS Outils de développement : liens vers des outils de développement SDKs, des boîtes à outils IDE et des outils de ligne de commande pour le développement et la gestion d' AWS applications.
- Centre de ressources pour la mise en route : découvrez comment configurer votre application Compte AWS, rejoindre la AWS communauté et lancer votre première application.
- Tutoriels pratiques — Suivez les step-by-step didacticiels pour lancer votre première application sur AWS.
- AWS Livres blancs : liens vers une liste complète de livres AWS blancs techniques, traitant de sujets tels que l'architecture, la sécurité et l'économie, rédigés par des architectes de AWS solutions ou d'autres experts techniques.
- AWS Support Centre — Le centre de création et de gestion de vos AWS Support dossiers. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des informations techniques FAQs, l'état de santé des services et AWS Trusted Advisor.
- Support— La principale page Web contenant des informations sur Support un one-on-one canal d'assistance à réponse rapide pour vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS , à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

Conditions préalables

Pour agir en tant qu' WorkMail administrateur Amazon, vous avez besoin d'un compte AWS. Si vous n'avez pas encore souscrit à AWS, effectuez les tâches suivantes.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif
- Accorder des autorisations aux utilisateurs IAM pour Amazon WorkMail

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pasCompte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à unCompte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWSvous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratifCompte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécuriséAWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS.
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d'AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center.
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWSutilisateur.

Attribution d’un accès à d’autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d’autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center.
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center.

Accorder des autorisations aux utilisateurs IAM pour Amazon WorkMail

Par défaut, les utilisateurs IAM ne sont pas autorisés à gérer les WorkMail ressources Amazon. Vous devez joindre une politique gérée par AWS (AmazonWorkMailFullAccessou AmazonWorkMailReadOnlyAccess) ou créer une politique gérée par le client qui accorde explicitement ces autorisations aux utilisateurs IAM. Vous attachez ensuite la stratégie aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon WorkMail.

Sécurité sur Amazon WorkMail

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. AWSvous 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 Amazon WorkMail, consultez la section AWSServices 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 l'utilisation d'Amazon WorkMail. Les rubriques suivantes expliquent comment configurer Amazon pour répondre WorkMail à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS qui vous aident à surveiller et à sécuriser vos WorkMail ressources Amazon.

Rubriques

Protection des données sur Amazon WorkMail

Le modèle de responsabilité AWS partagée de s'applique à la protection des données sur Amazon WorkMail. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous lesAWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée d'AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécurité AWS.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avecAWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennentServices AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Amazon WorkMail ou une autre entreprise

Services AWS à l'aide de la consoleAWS CLI, de l'API ou AWSSDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Comment Amazon WorkMail utilise AWS KMS

Amazon chiffre de WorkMail manière transparente tous les messages dans les boîtes aux lettres de toutes les WorkMail organisations Amazon avant qu'ils ne soient écrits sur le disque, et déchiffre les messages de manière transparente lorsque les utilisateurs y accèdent. Vous ne pouvez pas désactiver le chiffrement. Pour protéger les clés de chiffrement qui protègent les messages, Amazon WorkMail est intégré à AWS Key Management Service (AWS KMS).

Amazon propose WorkMail également une option permettant aux utilisateurs d'envoyer des e-mails signés ou chiffrés. Cette fonctionnalité de chiffrement n'utilise pas AWS KMS. Pour de plus amples informations, veuillez consulter Activation d'un e-mail signé ou chiffré.

Rubriques

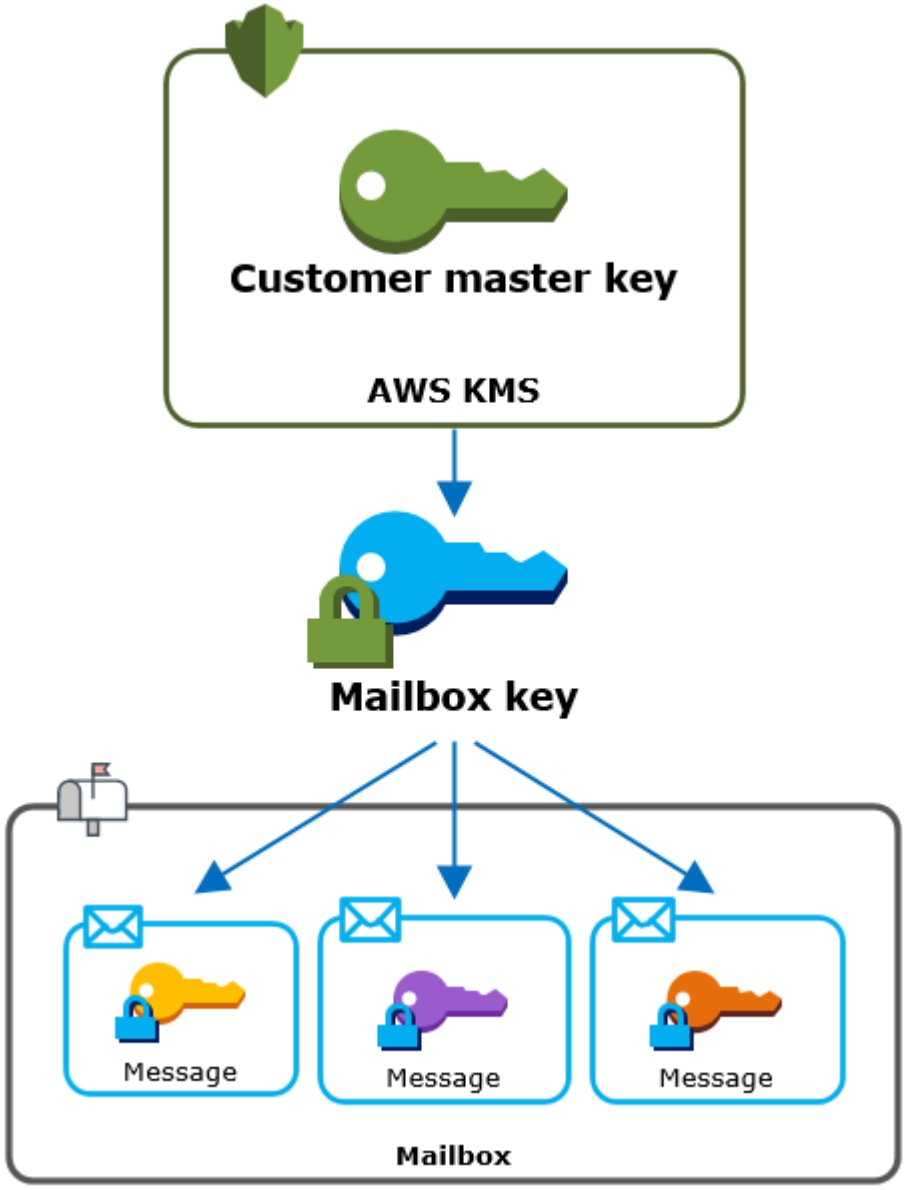
WorkMail Chiffrement Amazon

Dans Amazon WorkMail, chaque organisation peut contenir plusieurs boîtes aux lettres, une pour chaque utilisateur de l'organisation. Tous les messages, y compris les e-mails et les éléments de calendrier, sont stockés dans la boîte de réception de l'utilisateur.

Pour protéger le contenu des boîtes aux lettres de vos WorkMail organisations Amazon, Amazon WorkMail chiffre tous les messages des boîtes aux lettres avant qu'ils ne soient écrits sur le disque. Aucune des informations fournies par le client n'est stockée en texte brut.

Chaque message est chiffré sous une clé de chiffrement de données unique. La clé du message est protégée par une clé de boîte de réception, qui est une clé de chiffrement unique utilisée uniquement pour cette boîte de réception. La clé de la boîte aux lettres est cryptée sous une clé principale AWS KMS du client (CMK) pour l'organisation qui ne sort jamais AWS KMS non chiffrée. Le schéma

suivant illustre la relation entre les messages chiffrés, les clés des messages chiffrés, la clé de la boîte de réception chiffrée et la clé CMK de l'organisation dans AWS KMS.



Configuration d'une clé CMK pour l'organisation

Lorsque vous créez une WorkMail organisation Amazon, vous avez la possibilité de sélectionner une clé principale AWS KMS client (CMK) pour l'organisation. Cette clé CMK protège toutes les clés de boîte de réception de cette organisation.

Vous pouvez sélectionner la clé CMK AWS gérée par défaut pour Amazon WorkMail, ou vous pouvez sélectionner une clé CMK gérée par le client que vous possédez et gérez. Pour plus d'informations, consultez la section customer master keys (CMKs) dans le manuel du AWS Key Management

Service développeur. Vous pouvez sélectionner la même clé CMK ou une clé CMK différente pour chacune de vos organisations, mais vous ne pouvez pas modifier la clé CMK une fois que vous l'avez sélectionnée.

> **Important**
>
> Amazon ne WorkMail prend en charge que le système symétrique CMKs. Vous ne pouvez pas utiliser une clé CMK asymétrique. Pour savoir si une clé CMK est symétrique ou asymétrique, consultez la section Identification de la symétrie et de l'asymétrie CMKs dans le manuel du développeur. AWS Key Management Service

Pour trouver la clé CMK de votre organisation, utilisez l'entrée du AWS CloudTrail journal qui enregistre les appels adressés àAWS KMS.

Clé de chiffrement unique pour chaque boîte de réception

Lorsque vous créez une boîte aux lettres, Amazon WorkMail génère une clé de chiffrement symétrique AES (Advanced Encryption Standard) 256 bits unique pour la boîte aux lettres, connue sous le nom de clé de boîte aux lettres, en dehors de. AWS KMS Amazon WorkMail utilise la clé de boîte aux lettres pour protéger les clés de chiffrement de chaque message contenu dans la boîte aux lettres.

Pour protéger la clé de boîte aux lettres, Amazon WorkMail appelle AWS KMS pour chiffrer la clé de boîte aux lettres sous la clé CMK de l'organisation. Ensuite, il stocke la clé de la boîte de réception chiffrée dans la boîte de réception des métadonnées.

> **Note**
>
> Amazon WorkMail utilise une clé de chiffrement de boîte aux lettres symétrique pour protéger les clés de message. Auparavant, Amazon WorkMail protégeait chaque boîte aux lettres à l'aide d'une paire de clés asymétrique. Il utilise la clé publique pour chiffrer chaque clé de message et la clé privée pour la déchiffrer. La clé privée de la boîte de réception a été protégée par la clé CMK de l'organisation. Les anciennes boîtes aux lettres peuvent utiliser une paire de clés de boîte aux lettres asymétrique. Cette modification n'a pas d'incidence sur la sécurité de la boîte de réception ou de ses messages.

Chiffrer chaque message

Lorsqu'un utilisateur ajoute un message à une boîte aux lettres, Amazon WorkMail génère une clé de chiffrement symétrique AES 256 bits unique pour le message en dehors de. AWS KMS Il utilise cette clé de message pour chiffrer le message. Amazon WorkMail chiffre la clé du message sous la clé de la boîte aux lettres et stocke la clé de message chiffrée avec le message. Ensuite, il chiffre la clé de la boîte de réception sous la clé CMK de l'organisation.

Création d'une boîte de réception

Lorsqu'Amazon WorkMail crée une boîte aux lettres, il utilise le processus suivant pour préparer la boîte aux lettres afin qu'elle contienne des messages chiffrés.

- Amazon WorkMail génère une clé de chiffrement symétrique AES 256 bits unique pour la boîte aux lettres en dehors d'AWS KMS.
- Amazon WorkMail lance l'opération AWS KMS Encrypt. Il transmet la clé de la boîte aux lettres et l'identifiant de la clé principale du client (CMK) pour l'organisation. AWS KMSrenvoie le texte chiffré de la clé de boîte aux lettres cryptée sous le CMK.
- Amazon WorkMail stocke la clé cryptée de la boîte aux lettres avec les métadonnées de la boîte aux lettres.

Chiffrement d'un message de boîte de réception

Pour chiffrer un message, Amazon WorkMail utilise le processus suivant.

1. Amazon WorkMail génère une clé symétrique AES 256 bits unique pour le message. Il utilise la clé du message en texte brut et l'algorithme Advanced Encryption Standard (AES) pour chiffrer le message en dehors de. AWS KMS
2. Pour protéger la clé de message située sous la clé de boîte aux lettres, Amazon WorkMail doit déchiffrer la clé de boîte aux lettres, qui est toujours stockée sous sa forme cryptée.

   Amazon WorkMail lance l'opération AWS KMS Decrypt et transmet la clé cryptée de la boîte aux lettres. AWS KMSutilise le CMK pour que l'organisation déchiffre la clé de boîte aux lettres et renvoie la clé de boîte aux lettres en texte clair à Amazon. WorkMail
3. Amazon WorkMail utilise la clé de boîte aux lettres en texte brut et l'algorithme Advanced Encryption Standard (AES) pour chiffrer la clé du message en dehors de. AWS KMS
4. Amazon WorkMail stocke la clé du message chiffré dans les métadonnées du message chiffré afin qu'elle soit disponible pour le déchiffrer.

Déchiffrement d'un message de la boîte de réception

Pour déchiffrer un message, Amazon WorkMail utilise le processus suivant.

1. Amazon WorkMail lance l'opération AWS KMS Decrypt et transmet la clé cryptée de la boîte aux lettres. AWS KMSutilise le CMK pour que l'organisation déchiffre la clé de boîte aux lettres et renvoie la clé de boîte aux lettres en texte clair à Amazon. WorkMail
2. Amazon WorkMail utilise la clé de boîte aux lettres en texte brut et l'algorithme Advanced Encryption Standard (AES) pour déchiffrer la clé de message chiffrée en dehors de. AWS KMS
3. Amazon WorkMail utilise la clé du message en texte brut pour déchiffrer le message chiffré.

Mise en cache des clés de boîte de réception

Afin d'améliorer les performances et de minimiser les appelsAWS KMS, Amazon met en WorkMail cache chaque clé de boîte aux lettres en texte brut pour chaque client localement pendant une minute maximum. À la fin de la période de mise en cache, la clé de la boîte de réception est supprimée. Si la clé de boîte aux lettres de ce client est requise pendant la période de mise en cache, Amazon WorkMail peut l'obtenir depuis le cache au lieu d'appelerAWS KMS. La clé de la boîte de réception est protégée dans le cache et n'est jamais écrit sur le disque en texte brut.

Autorisation d'utilisation de la clé CMK

Lorsqu'Amazon WorkMail utilise une clé principale du client (CMK) dans le cadre d'opérations cryptographiques, elle agit pour le compte de l'administrateur de la boîte aux lettres.

Pour utiliser la clé principale du AWS KMS client (CMK) comme secret en votre nom, l'administrateur doit disposer des autorisations suivantes. Vous pouvez spécifier ces autorisations requises dans une politique IAM ou dans une politique de clé.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

Pour autoriser l'utilisation de la clé CMK uniquement pour les demandes provenant d'Amazon WorkMail, vous pouvez utiliser la clé de ViaService condition kms : avec la `workmail.<region>.amazonaws.com` valeur.

Vous pouvez également utiliser les clés ou les valeurs du contexte de chiffrement comme condition d'utilisation de la clé CMK pour les opérations de chiffrement. Par exemple, vous pouvez utiliser un opérateur de condition de chaîne dans un document de politique IAM ou de clé, ou utiliser une contrainte d'octroi dans un octroi.

Stratégie de clé pour la clé CMK gérée par AWS

La politique clé de la clé CMK AWS gérée pour Amazon WorkMail autorise les utilisateurs à utiliser la clé CMK pour des opérations spécifiques uniquement lorsqu'Amazon WorkMail fait la demande au nom de l'utilisateur. La stratégie de clé n'autorise pas tous les utilisateurs à utiliser la clé CMK directement.

Cette stratégie de clé, comme les stratégies de toutes les clés gérées par AWS, est établie par le service. Vous ne pouvez pas modifier la politique clé, mais vous pouvez la consulter à tout moment. Pour plus de détails, consultez la section Affichage d'une politique clé dans le guide du AWS Key Management Service développeur.

Les instructions de politique de la politique de clé ont l'effet suivant :

- Autorisez les utilisateurs du compte et de la région à utiliser le CMK pour des opérations cryptographiques et pour créer des autorisations, mais uniquement lorsque la demande provient d'Amazon en leur WorkMail nom. La clé de condition `kms:ViaService` applique cette restriction.
- Permet au AWS compte de créer des politiques IAM qui permettent aux utilisateurs de consulter les propriétés CMK et de révoquer les autorisations.

Voici une politique clé pour un exemple de clé CMK AWS gérée pour Amazon WorkMail.

JSON

```
{
  "Version":"2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that
 are authorized to use WorkMail",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
```

```
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*",
 "kms:DescribeKey", "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

Utiliser des subventions pour autoriser Amazon WorkMail

Outre les politiques clés, Amazon WorkMail utilise des subventions pour ajouter des autorisations au CMK pour chaque organisation. Pour consulter les subventions du CMK sur votre compte, utilisez l'ListGrantsopération.

Amazon WorkMail utilise des subventions pour ajouter les autorisations suivantes au CMK de l'organisation.

- Ajoutez l'`kms:Encrypt`autorisation permettant à Amazon de chiffrer WorkMail la clé de la boîte aux lettres.
- Ajoutez l'`kms:Decrypt`autorisation permettant à Amazon d'utiliser la clé CMK WorkMail pour déchiffrer la clé de la boîte aux lettres. Amazon WorkMail exige cette autorisation dans le cadre d'une autorisation, car la demande de lecture des messages de boîte aux lettres utilise le contexte de sécurité de l'utilisateur qui lit le message. La demande n'utilise pas les informations d'identification du AWS compte. Amazon WorkMail crée cette subvention lorsque vous sélectionnez une clé CMK pour l'organisation.

Pour créer les subventions, Amazon WorkMail appelle au CreateGrantnom de l'utilisateur qui a créé l'organisation. L'autorisation de créer l'octroi provient de la politique de clé. Cette politique permet aux

utilisateurs du compte d'appeler `CreateGrant` le CMK de l'organisation lorsqu'Amazon WorkMail fait la demande au nom d'un utilisateur autorisé.

La politique des clés permet également à l'utilisateur root du compte de révoquer l'attribution de la clé AWS gérée. Toutefois, si vous révoquez l'autorisation, Amazon ne WorkMail pourra pas déchiffrer les données chiffrées de vos boîtes aux lettres.

Contexte WorkMail de chiffrement Amazon

Un contexte de chiffrement est un ensemble de paires clé-valeur contenant les données non secrètes arbitraires. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, lie AWS KMS cryptographiquement le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez transmettre le même contexte de chiffrement. Consultez Contexte de chiffrement dans le AWS Key Management Serviceguide du développeur pour en savoir plus.

Amazon WorkMail utilise le même format de contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques. Vous pouvez utiliser le contexte de chiffrement pour identifier une opération de chiffrement dans les enregistrements d'audit et les journaux, tels qu' AWS CloudTrail, et en tant que condition pour l'autorisation dans les politiques et les octrois.

Dans ses demandes Encrypt and Decrypt à, AWS KMS Amazon WorkMail utilise un contexte de chiffrement dans lequel la clé `aws:workmail:arn` et la valeur sont le nom de ressource Amazon (ARN) de l'organisation.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

Par exemple, le contexte de chiffrement suivant inclut un exemple d'ARN d'organisation dans la région Europe (Irlande) `eu-west-1` ().

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
```

Surveillance de WorkMail l'interaction d'Amazon avec AWS KMS

Vous pouvez utiliser AWS CloudTrail Amazon CloudWatch Logs pour suivre les demandes qu'Amazon WorkMail envoie AWS KMS en votre nom.

Encrypt

Lorsque vous créez une boîte aux lettres, Amazon WorkMail génère une clé de boîte aux lettres et appelle AWS KMS pour chiffrer la clé de boîte aux lettres. Amazon WorkMail envoie une demande

de chiffrement à l'AWS KMSaide de la clé de boîte aux lettres en texte clair et d'un identifiant pour le CMK de l'organisation Amazon. WorkMail

L'événement qui enregistre l'opération `Encrypt` est similaire à l'exemple d'événement suivant. L'utilisateur est le WorkMail service Amazon. Les paramètres incluent l'ID CMK (`keyId`) et le contexte de chiffrement pour l' WorkMail organisation Amazon. Amazon transmet WorkMail également la clé de la boîte aux lettres, mais celle-ci n'est pas enregistrée dans le CloudTrail journal.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
```

```
}
```

Decrypt

Lorsque vous ajoutez, consultez ou supprimez un message de boîte aux lettres, Amazon WorkMail demande AWS KMS à déchiffrer la clé de la boîte aux lettres. Amazon WorkMail envoie une demande de déchiffrement à l'AWS KMSaide de la clé cryptée de la boîte aux lettres et d'un identifiant pour le CMK de l'organisation Amazon WorkMail.

L'événement qui enregistre l'opération `Decrypt` est similaire à l'exemple d'événement suivant. L'utilisateur est le WorkMail service Amazon. Les paramètres incluent la clé de boîte aux lettres cryptée (sous forme de blob de texte chiffré), qui n'est pas enregistrée dans le journal, et le contexte de chiffrement pour l'organisation Amazon. WorkMail AWS KMSdérive l'ID du CMK à partir du texte chiffré.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

Gestion des identités et des accès pour Amazon WorkMail

Gestion des identités et des accès AWS(IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon WorkMail . IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes liés à WorkMail l'identité et à l'accès à Amazon)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Amazon WorkMail travaille avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques WorkMail basées sur l'identité d'Amazon)

Authentification avec des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS.

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWSutilisateur root

Lorsque vous créez unCompte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle

IAM (console) ou en appelant une opération d'AWSAPI AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès entre comptes, les accès entre services et pour les applications exécutées sur Amazon. EC2 Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWSévalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWSprend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dansAWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations.
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s’appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon WorkMail travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon WorkMail, vous devez comprendre quelles fonctionnalités IAM peuvent être utilisées avec Amazon. WorkMail Pour obtenir une vue d'ensemble de la manière dont Amazon WorkMail et les autres AWS services fonctionnent avec IAM, consultez la section AWSServices compatibles avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur WorkMail l'identité d'Amazon
- Politiques basées sur WorkMail les ressources d'Amazon
- Autorisation basée sur les WorkMail tags Amazon
- Rôles Amazon WorkMail IAM

Politiques basées sur WorkMail l'identité d'Amazon

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Amazon WorkMail prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L’élément `Action` d’une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l’accès à une politique. Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Les actions politiques sur Amazon WorkMail utilisent le préfixe suivant avant l'action :`workmail:`. Par exemple, pour autoriser quelqu'un à récupérer une liste d'utilisateurs avec l'opération d' WorkMail `ListUsers`API Amazon, vous devez inclure l'`workmail:ListUsers`action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon WorkMail définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": "workmail:List*"
```

Pour consulter la liste des WorkMail actions Amazon, consultez la section Actions définies par Amazon WorkMail dans le guide de l'utilisateur IAM.

Ressources

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Amazon WorkMail prend en charge les autorisations au niveau des ressources pour les organisations Amazon WorkMail .

La ressource d' WorkMail organisation Amazon possède l'ARN suivant :

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

Pour plus d'informations sur le format de ARNs, consultez Amazon Resource Names (ARNs) et espaces de noms AWS de services.

Par exemple, pour spécifier l'organisation `m-n1pq2345678r901st2u3vx45x6789yza` dans votre instruction, utilisez l'ARN suivant.

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
```

Pour spécifier toutes les organisations qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/*"
```

Certaines WorkMail actions Amazon, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour consulter la liste des types de WorkMail ressources Amazon et leurs caractéristiques ARNs, consultez la section Ressources définies par Amazon WorkMail dans le guide de l'utilisateur IAM. Pour savoir quelles actions vous pouvez spécifier pour l'ARN de chaque ressource, consultez Actions, ressources et clés de condition pour Amazon WorkMail.

Clés de condition

Amazon WorkMail prend en charge les clés de condition globales suivantes.

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:MultiFactorAuthAge`
- `aws:MultiFactorAuthPresent`

- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

L'exemple de politique suivant accorde l'accès à la WorkMail console Amazon uniquement aux principaux IAM authentifiés MFA dans la région AWS. eu-west-1

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*",
                "lambda:ListFunctions",
                "iam:ListRoles",
                "logs:DescribeLogGroups",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
```

```
    ]
}
```

Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

`workmail:ImpersonationRoleId`est la seule clé de condition spécifique au service prise en charge par Amazon. WorkMail

L'exemple de politique suivant limite l'`AssumeImpersonationRole`action à une WorkMail organisation et à un rôle d'usurpation d'identité spécifiques.

Exemples

Pour consulter des exemples de politiques WorkMail basées sur l'identité d'Amazon, consultez. Exemples de politiques WorkMail basées sur l'identité d'Amazon

Politiques basées sur WorkMail les ressources d'Amazon

Amazon WorkMail ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les WorkMail tags Amazon

Vous pouvez associer des balises aux WorkMail ressources Amazon ou transmettre des balises dans une demande adressée à Amazon WorkMail. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur le balisage des WorkMail ressources Amazon, consultezBalisage d'une organisation.

Rôles Amazon WorkMail IAM

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Amazon WorkMail

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d'AWS STSAPI telles que AssumeRoleou GetFederationToken.

Amazon WorkMail prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Amazon WorkMail prend en charge les rôles liés aux services. Pour en savoir plus sur la création ou la gestion des rôles WorkMail liés aux services Amazon, consultez. Utilisation de rôles liés à un service pour Amazon WorkMail

Rôles du service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Amazon WorkMail prend en charge les rôles de service.

Exemples de politiques WorkMail basées sur l'identité d'Amazon

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou à modifier des WorkMail ressources Amazon. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'AWSAPI AWS Management ConsoleAWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, veuillez consulter Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la WorkMail console Amazon
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

- Autoriser les utilisateurs à accéder en lecture seule aux ressources Amazon WorkMail

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer WorkMail des ressources Amazon dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votreCompte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifiqueService AWS, tel queCloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la WorkMail console Amazon

Pour accéder à la WorkMail console Amazon, vous devez disposer d'un minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux WorkMail ressources Amazon de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

Pour garantir que ces entités peuvent toujours utiliser la WorkMail console Amazon, associez également la politique AWS gérée suivante aux entités. AmazonWorkMailFullAccess Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

La AmazonWorkMailFullAccesspolitique accorde à un utilisateur IAM un accès complet aux WorkMail ressources Amazon. Cette politique donne à l'utilisateur l'accès à toutes les opérations d'Amazon WorkMailAWS Key Management Service, d'Amazon Simple Email Service et à toutes les AWS Directory Service opérations. Cela inclut également plusieurs EC2 opérations Amazon qu'Amazon WorkMail doit effectuer en votre nom. Les `cloudwatch` autorisations `logs` et sont requises pour la journalisation des événements par e-mail et l'affichage des métriques dans la WorkMail console Amazon. La journalisation des audits utilise CloudWatch Logs, Amazon S3 et Amazon Data FireHose pour le stockage`logs`. Pour de plus amples informations, veuillez consulter Journalisation et surveillance sur Amazon WorkMail.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
```

```
        "Action": [
          "ds:AuthorizeApplication",
          "ds:CheckAlias",
          "ds:CreateAlias",
          "ds:CreateDirectory",
          "ds:CreateIdentityPoolDirectory",
          "ds:DeleteDirectory",
          "ds:DescribeDirectories",
          "ds:GetDirectoryLimits",
          "ds:ListAuthorizedApplications",
          "ds:UnauthorizeApplication",
          "ec2:AuthorizeSecurityGroupEgress",
          "ec2:AuthorizeSecurityGroupIngress",
          "ec2:CreateNetworkInterface",
          "ec2:CreateSecurityGroup",
          "ec2:CreateSubnet",
          "ec2:CreateTags",
          "ec2:CreateVpc",
          "ec2:DeleteSecurityGroup",
          "ec2:DeleteSubnet",
          "ec2:DeleteVpc",
          "ec2:DescribeAvailabilityZones",
          "ec2:DescribeRouteTables",
          "ec2:DescribeSubnets",
          "ec2:DescribeVpcs",
          "ec2:RevokeSecurityGroupEgress",
          "ec2:RevokeSecurityGroupIngress",
          "kms:DescribeKey",
          "kms:ListAliases",
          "lambda:ListFunctions",
          "route53:ChangeResourceRecordSets",
          "route53:ListHostedZones",
          "route53:ListResourceRecordSets",
          "route53:GetHostedZone",
          "route53domains:CheckDomainAvailability",
          "route53domains:ListDomains",
          "ses:*",
          "workmail:*",
          "iam:ListRoles",
          "logs:DescribeLogGroups",
          "logs:CreateLogGroup",
          "logs:PutRetentionPolicy",
          "logs:DeleteDeliveryDestination",
          "logs:DeleteDeliveryDestinationPolicy",
```

```
            "logs:DescribeDeliveryDestinations",
            "logs:GetDeliveryDestination",
            "logs:GetDeliveryDestinationPolicy",
            "logs:PutDeliveryDestination",
            "logs:PutDeliveryDestinationPolicy",
            "logs:CreateDelivery",
            "logs:DeleteDelivery",
            "logs:DescribeDeliveries",
            "logs:GetDelivery",
            "logs:DeleteDeliverySource",
            "logs:DescribeDeliverySources",
            "logs:GetDeliverySource",
            "logs:PutDeliverySource",
            "logs:DescribeResourcePolicies",
            "cloudwatch:GetMetricData",
            "firehose:DescribeDeliveryStream",
            "firehose:ListDeliveryStreams",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
```

```
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l'AWSAPI. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI orAWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Autoriser les utilisateurs à accéder en lecture seule aux ressources Amazon WorkMail

La déclaration de politique suivante accorde à un utilisateur IAM un accès en lecture seule aux ressources Amazon. WorkMail Cette politique donne le même niveau d'accès que la politique gérée par AWS AmazonWorkMailReadOnlyAccess. L'une ou l'autre politique donne à l'utilisateur l'accès à toutes les WorkMail `Describe` opérations Amazon. L'accès à l'AWS Directory Service`DescribeDirectories`opération est nécessaire pour obtenir des informations sur vos Directory Service annuaires. L'accès au service Amazon SES est nécessaire pour obtenir des informations sur les domaines configurés. L'accès à AWS Key Management Service est nécessaire pour obtenir des informations sur les clés de chiffrement utilisées. Les `cloudwatch` autorisations `logs` et sont requises pour la journalisation des événements par e-mail et l'affichage des métriques dans la WorkMail console Amazon. La journalisation des audits utilise CloudWatch Logs, Amazon S3 et Amazon Data FireHose pour le stockage`logs`. Pour de plus amples informations, veuillez consulter Journalisation et surveillance sur Amazon WorkMail.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailReadOnly",
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
```

```
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Résolution des problèmes liés à WorkMail l'identité et à l'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon WorkMail et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action sur Amazon WorkMail
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes WorkMail ressources Amazon

Je ne suis pas autorisé à effectuer une action sur Amazon WorkMail

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser la console pour afficher les détails d'un groupe mais ne dispose pas des `workmail:DescribeGroup` autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workmail:DescribeGroup on resource: group
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `group` à l'aide de l'action `workmail:DescribeGroup`.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon WorkMail.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action sur Amazon WorkMail. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes WorkMail ressources Amazon

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon WorkMail prend en charge ces fonctionnalités, consultezComment Amazon WorkMail travaille avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiersComptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

AWSpolitiques gérées pour Amazon WorkMail

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWSles services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccessAWSgérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AmazonWorkMailFullAccess

Vous pouvez associer la politique `AmazonWorkMailFullAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent un accès complet à Amazon WorkMail.

Pour consulter les autorisations relatives à cette politique, consultez AmazonWorkMailFullAccess dans AWS Management Console.

AWSpolitique gérée : AmazonWorkMailReadOnlyAccess

Vous pouvez associer la politique `AmazonWorkMailReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations permettant un accès en lecture seule à Amazon. WorkMail

Pour consulter les autorisations relatives à cette politique, consultez AmazonWorkMailReadOnlyAccess dans AWS Management Console.

AWSpolitique gérée : AmazonWorkMailEventsServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé AmazonWorkMailEventspour autoriser l'accès aux AWS services et aux ressources utilisés ou gérés par Amazon WorkMail Events. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon WorkMail.

Amazon WorkMail met à jour AWS ses politiques gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon WorkMail depuis que ce service a commencé à suivre ces modifications.

Modifier	Description	Date
Mises à jour des politiques gérées par AWS - Mise à jour d'une politique existante	Les `AmazonWorkMailFullAccess` autorisations `AmazonWorkMailReadOnlyAccess` et ont été mises à jour pour Amazon WorkMail afin de prendre en charge la journalisation des audits. Pour plus d'informa	14 février 2024

Modifier	Description	Date
	tions sur les autorisations mises à jour, voir Exemples de politiques WorkMail basées sur l'identité d'Amazon et pour plus d'informations sur la journalisation des audits, voirActivation de la journalisation des audits.	
Amazon WorkMail a commencé à suivre les modifications	Amazon WorkMail a commencé à suivre les modifications apportées AWS à ses politiques gérées.	1er mars 2021

Utilisation de rôles liés à un service pour Amazon WorkMail

Amazon WorkMail utilise des rôles Gestion des identités et des accès AWS liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon. WorkMail Les rôles liés au service sont prédéfinis par Amazon WorkMail et incluent toutes les autorisations requises par le service pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon WorkMail , car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon WorkMail définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon WorkMail peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable des ressources connexes. Cela protège vos WorkMail ressources Amazon, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour de plus amples informations sur les autres services qui prennent en charge les rôles liés à un service, veuillez consulter Services AWS qui fonctionnent avec IAM et recherchez les services qui comportent Oui dans la colonne Rôle lié à un service. Sélectionnez un Yes (Oui) avec un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour Amazon WorkMail

Amazon WorkMail utilise le rôle lié au service nommé — AmazonWorkMailEventsAmazon WorkMail utilise ce rôle lié au service pour permettre l'accès aux AWS services et aux ressources utilisés ou gérés par les WorkMail événements Amazon, tels que la surveillance des événements de courrier électronique enregistrés par Amazon. CloudWatch Pour plus d'informations sur l'activation de la journalisation des événements par e-mail pour Amazon WorkMail, consultezActivation de l'enregistrement des événements par e-mail.

Le rôle AmazonWorkMailEvents lié à un service fait confiance aux services suivants pour assumer le rôle :

- `events.workmail.amazonaws.com`

La politique d'autorisation des rôles permet WorkMail à Amazon d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `logs:CreateLogGroup` sur `allAWSresources`
- Action : `logs:CreateLogStream` sur `allAWSresources`
- Action : `logs:PutLogEvents` sur `allAWSresources`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon WorkMail

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez la journalisation des WorkMail événements Amazon et que vous utilisez les paramètres par défaut de la WorkMail console Amazon, Amazon WorkMail crée pour vous le rôle lié au service.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez la journalisation des WorkMail événements Amazon et que vous utilisez les paramètres par défaut, Amazon WorkMail crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Amazon WorkMail

Amazon WorkMail ne vous autorise pas à modifier le rôle AmazonWorkMailEvents lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Amazon WorkMail

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le WorkMail service Amazon utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les WorkMail ressources Amazon utilisées par AmazonWorkMailEvents

1. Désactivez la journalisation des WorkMail événements Amazon.

   a. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

      Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

   b. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.

   c. Dans le volet de navigation, choisissez Paramètres de l'organisation, puis Surveillance.

   d. Pour Log settings (Paramètres des journaux), choisissez Edit (Modifier).

   e. Déplacez le curseur Activer les événements de messagerie sur la position Off.

   f. Choisissez Enregistrer.

2. Supprimez le groupe de CloudWatch journaux Amazon.

    a. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.

    b. Choisissez Logs (Journaux).

    c. Pour Log Groups (Groupes de journaux), sélectionnez le groupe de journaux à supprimer.

    d. Pour Actions, choisissez Delete log group (Supprimer le groupe de journaux).

    e. Sélectionnez Yes, Delete (Oui, supprimer).

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, leAWS CLI, ou l'AWSAPI pour supprimer le rôle lié au AmazonWorkMailEvents service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles WorkMail liés aux services Amazon

Amazon WorkMail prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Amazon WorkMail Regions and Endpoints.

Journalisation et surveillance sur Amazon WorkMail

La surveillance et l'audit de vos e-mails et de vos journaux sont essentiels pour préserver la santé de votre WorkMail organisation Amazon. Amazon WorkMail prend en charge deux types de surveillance :

- Enregistrement des événements : la surveillance de l'activité d'envoi d'e-mails de votre organisation permet de protéger la réputation de votre domaine. La surveillance peut également vous permettre de suivre les e-mails qui sont envoyés et reçus. Pour plus d'informations sur l'activation de la journalisation des événements de messagerie, consultez Activation de l'enregistrement des événements par e-mail.
- Journalisation des audits : vous pouvez utiliser les journaux d'audit pour recueillir des informations détaillées sur WorkMail l'utilisation de votre organisation Amazon, notamment pour surveiller l'accès des utilisateurs aux boîtes aux lettres, vérifier les activités suspectes et déboguer les configurations des fournisseurs de contrôle d'accès et de disponibilité. Pour de plus amples informations, veuillez consulter Activation de la journalisation des audits.

AWSfournit les outils de surveillance suivants pour surveiller Amazon WorkMail, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Par exemple, lorsque vous activez la journalisation des événements par e-mail pour Amazon WorkMail, vous CloudWatch pouvez suivre les e-mails envoyés et reçus pour votre organisation. Pour plus d'informations sur la surveillance d'Amazon WorkMail avec CloudWatch, consultezSurveillance d'Amazon à WorkMail l'aide de CloudWatch métriques. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos événements d'e-mail et à vos journaux d'audit pour Amazon WorkMail lorsque la journalisation des e-mails et des audits est activée dans la WorkMail console Amazon. CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux, et vous pouvez archiver les données de vos journaux dans un stockage hautement durable. Pour plus d'informations sur le suivi des WorkMail messages Amazon à l'aide CloudWatch des journaux, consultez Activation de l'enregistrement des événements par e-mail etActivation de la journalisation des audits. Pour plus d'informations sur CloudWatch les journaux, consultez le guide de l'utilisateur Amazon CloudWatch Logs.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par vous ou en votre nomCompte AWS, et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelésAWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter Journalisation des appels WorkMail d'API Amazon avec AWS CloudTrail.
- Amazon S3 vous permet de stocker et d'accéder à vos WorkMail événements Amazon de manière rentable. Amazon S3 fournit des mécanismes pour gérer le cycle de vie des données d'événements, vous permettant de configurer la suppression automatique des anciens événements ou de configurer l'archivage automatique dans Amazon S3 Glacier. Notez que la livraison Amazon S3 n'est disponible que pour les événements de journalisation des audits. Pour plus d'informations sur Amazon S3, consultez le guide de l'utilisateur Amazon S3.
- Amazon Data Firehose vous permet de diffuser les données de vos événements vers d'autres services AWS tels qu'Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, OpenSearch Amazon Serverless, Splunk et tout point de terminaison HTTP personnalisé ou appartenant à des fournisseurs de services tiers pris en charge, notamment Datadog, LogicMonitor Dynatrace, MongoDB, New Relic, Corc alogix et Elastic. OpenSearch La livraison

à Firehose n'est disponible que pour les événements de journalisation des audits. Pour plus d'informations sur Firehose, consultez le guide du développeur Amazon Data Firehose.

Rubriques

Surveillance d'Amazon à WorkMail l'aide de CloudWatch métriques

Vous pouvez surveiller Amazon WorkMail en utilisant CloudWatch, qui collecte les données brutes et les traite en métriques lisibles en temps quasi réel. Les statistiques gratuites sont stockées pendant 15 mois afin que vous puissiez accéder aux informations historiques pour voir les performances de votre application ou service Web. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

CloudWatch statistiques pour Amazon WorkMail

Amazon WorkMail envoie les statistiques et informations de dimension suivantes à CloudWatch.

L'espace de noms `AWS/WorkMail` inclut les métriques suivantes.

Métrique	Description
`OrganizationEmailReceived`	Le nombre d'e-mails reçus par votre WorkMail organisation Amazon. Si un e-mail est adressé à 10 destinataires au sein de votre organisat ion, le `OrganizationEmailReceived` nombre est de un. Unités : nombre

Métrique	Description
`MailboxEmailDelivered`	Le nombre d'e-mails envoyés aux différentes boîtes aux lettres de votre WorkMail organisation Amazon. Si un e-mail est envoyé avec succès à 10 destinataires au sein de votre organisation, le `MailboxEmailDelivered` nombre est de 10. Unités : nombre
`IncomingEmailBounced`	Le nombre d'e-mails entrants qui ont été renvoyés en raison de boîtes aux lettres pleines. Cette métrique est décomptée pour chaque destinataire prévu. Par exemple, si un e-mail est envoyé à 10 destinataires au sein de votre organisation et que deux d'entre eux ont des boîtes aux lettres pleines, ce qui entraîne une réponse de rebond, le `IncomingEmailBounced` nombre est de deux. Unités : nombre
`OutgoingEmailBounced`	Le nombre d'e-mails sortants qui n'ont pas pu être livrés. Cette métrique est décomptée pour chaque destinataire prévu. Par exemple, si un e-mail est envoyé à 10 destinataires et que deux e-mails n'ont pas pu être livrés, le `OutgoingEmailBounced` nombre est de 2. Unités : nombre

Métrique	Description
`OutgoingEmailSent`	Le nombre d'e-mails envoyés avec succès par votre WorkMail organisation Amazon. Cette métrique est décomptée pour chaque destinataire d'un e-mail envoyé avec succès. Par exemple, si 1 e-mail a été envoyé à 10 destinataires et cet e-mail a été correctem ent remis à 8 de ces destinataires, la valeur de `OutgoingEmailSent` est 8. Unités : nombre
`AuthenticationFailure`	Cette métrique compte le nombre de tentative s d'authentification. Lorsque l'authentification est réussie, le nombre est de 0 et lorsque l'authentification échoue, le nombre est de 1. Utilisez les `Sum` statistiques pour surveiller le nombre de tentatives d'authentification infructue uses. Utilisez les `Sample count` statistiq ues pour surveiller le nombre total d'événeme nts d'authentification. Utilisez les `Average` statistiques pour surveiller le ratio d'événeme nts d'authentification ayant échoué et réussi. Unités : nombre

Métrique	Description
`AccessDenied`	Cette métrique compte le nombre d'évaluations du contrôle d'accès. Lorsque l'action est refusée par le contrôle d'accès, le nombre est de 1 et lorsque l'action est accordée, le nombre est de 0. Utilisez les `Sum` statistiques pour surveiller le volume d'actions refusées, les `Sample count` statistiques pour surveiller le nombre total de tentatives d'actions et les `Average` statistiques pour surveiller le ratio d'actions autorisées et refusées. Unités : nombre
`ActionDenied`	Cette métrique est prise en compte lorsqu'une action est effectuée sur les données de la boîte aux lettres. Lorsque l'action est refusée, le nombre est de 1 et si l'action est accordée, le nombre est de 0. Utilisez les `Sum` statistiques pour surveiller le volume d'actions de boîte aux lettres refusées, les `Sample count` statistiques pour surveiller le nombre total de tentatives d'actions de boîte aux lettres et les `Average` statistiques pour surveiller le ratio d'actions autorisées et refusées. Unités : nombre
`AvailabilityProviderFailure`	Cette métrique est prise en compte pour chaque demande de fournisseur de disponibilité WorkMail exécutée par Amazon pour récupérer la disponibilité du calendrier auprès d'une source externe. Pour plus d'informations sur les fournisseurs de disponibilité, consultez le manuel Amazon WorkMail Administrator Guide.

Surveillance des journaux d'événements WorkMail liés aux e-mails d'Amazon

Lorsque vous activez la journalisation des événements par e-mail pour votre WorkMail organisation Amazon, Amazon WorkMail enregistre les événements par e-mail avec CloudWatch. Pour plus d'informations sur l'activation de la journalisation des événements de messagerie, consultez Activation de l'enregistrement des événements par e-mail.

Les tableaux suivants décrivent les événements auxquels Amazon WorkMail se connecte CloudWatch, le moment où ils sont transmis et le contenu des champs d'événements.

`ORGANIZATION_EMAIL_RECEIVED`

Cet événement est enregistré lorsque votre WorkMail organisation Amazon reçoit un e-mail.

Champ	Description
recipients	Destinataires prévus du message.
sender	Adresse e-mail de l'utilisateur qui a envoyé l'e-mail au nom d'un autre utilisateur. Ce champ est défini uniquement lorsqu'un e-mail est envoyé au nom d'un autre utilisateur.
from	Adresse d'expédition (De), qui est généralem ent l'adresse e-mail de l'utilisateur qui a envoyé le message. Si l'utilisateur a envoyé le message en tant qu'un autre utilisateur ou au nom d'un autre utilisateur, ce champ renvoie l'adresse e-mail de l'utilisateur au nom duquel le message a été envoyé, et non l'adresse e-mail de l'expéditeur réel.
subject	Objet de l'e-mail.
messageId	ID de message SMTP
spamVerdict	Indique si le message est marqué comme spam par Amazon SES. Pour plus d'informa

Champ	Description
	tions, consultez le contenu des notifications relatives à la réception d'e-mails par Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.
dkimVerdict	Indique si le contrôle du courrier DomainKeys identifié (DKIM) a réussi. Pour plus d'informa tions, consultez le contenu des notifications relatives à la réception d'e-mails par Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.
dmarcVerdict	Indique si le contrôle DMARC (Domain-b ased Message Authentication, Reporting and Conformance) a réussi. Pour plus d'informa tions, consultez le contenu des notifications relatives à la réception d'e-mails par Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.
dmarcPolicy	Apparaît uniquement lorsque le champ dmarcVerdict contient « FAIL ». Indique l'action à exécuter sur l'e-mail lorsque le contrôle DMARC échoue (NONE, QUARANTINE ou REJECT). Celle-ci est définie par le propriétaire du domaine de messagerie d'envoi.
spfVerdict	Indique si les vérifications du Sender Policy Framework (SPF) sont réussies. Pour plus d'informations, consultez le contenu des notifications relatives à la réception d'e-mails par Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.
messageTimestamp	Indique quand le message est reçu.

MAILBOX_EMAIL_DELIVERED

Cet événement est consigné lorsqu'un message est remis à une boîte aux lettres de votre organisation. Étant donné qu'il est consigné une fois pour chaque boîte aux lettres à laquelle un message est remis, un seul événement `ORGANIZATION_EMAIL_RECEIVED` peut entraîner plusieurs événements `MAILBOX_EMAIL_DELIVERED`.

Champ	Description
destinataire	Boîte aux lettres à laquelle le message est remis.
folder	Dossier de la boîte aux lettres dans lequel le message est placé.

RULE_APPLIED

Cet événement est enregistré lorsqu'un message entrant ou sortant lance une règle de flux de courrier électronique.

Champ	Description
ruleName	Le nom de la règle .
ruleType	Type de règle appliqué (INBOUND_RULE, OUTBOUND_RULE ou MAILBOX_RULE). Les règles d'entrée et de sortie s'appliquent à votre organisation Amazon WorkMail. Les règles de boîte aux lettres s'appliquent uniquement aux boîtes aux lettres spécifiées. Pour de plus amples informations, veuillez consulter Gestion des flux de messagerie.
ruleActions	Actions effectuées en fonction de la règle. Les différents destinataires du message peuvent avoir différentes actions, par exemple, un e-mail renvoyé à l'expéditeur ou un e-mail remis avec succès.

Champ	Description
targetFolder	Dossier de destination prévu pour une règle MAILBOX_RULE `Move` ou `Copy`.
targetRecipient	Destinataire prévu pour une règle MAILBOX_RULE `Forward` ou `Redirect`.

JOURNALING_INITIATED

Cet événement est enregistré lorsqu'Amazon WorkMail envoie un e-mail à l'adresse de journalisation spécifiée par l'administrateur de votre organisation. Il n'est transmis que si la journalisation est configurée pour votre organisation. Pour de plus amples informations, veuillez consulter Utilisation de la journalisation des e-mails avec Amazon WorkMail.

Champ	Description
journalingAddress	Adresse e-mail à laquelle le message de journalisation est envoyé.

INCOMING_EMAIL_BOUNCED

Cet événement est enregistré lorsqu'un message entrant ne peut pas être remis à un destinataire cible. Les e-mails peuvent être renvoyés pour un certain nombre de raisons, comme une boîte aux lettres cible complète. Le système enregistre cet événement une fois pour chaque destinataire, ce qui entraîne le renvoi d'un e-mail. Par exemple, si un message entrant est adressé à trois destinataires et les boîtes aux lettres de deux d'entre eux sont pleines, deux événements INCOMING_EMAIL_BOUNCED sont consignés.

Champ	Description
bouncedRecipient	Le destinataire auquel Amazon WorkMail a renvoyé le message.

OUTGOING_EMAIL_SUBMITTED

Cet événement est consigné lorsqu'un utilisateur de votre organisation soumet un e-mail pour envoi. Ceci est enregistré avant que le message ne quitte Amazon WorkMail. Cet événement n'indique donc pas si l'e-mail a été livré avec succès.

Champ	Description
recipients	Destinataires du message tels que spécifiés par l'expéditeur. Inclut tous les destinataires indiqués sur les lignes À, Cc et Cci.
sender	Adresse e-mail de l'utilisateur qui a envoyé l'e-mail au nom d'un autre utilisateur. Ce champ est défini uniquement lorsqu'un e-mail est envoyé au nom d'un autre utilisateur.
from	Adresse d'expédition (De), qui est généralement l'adresse e-mail de l'utilisateur qui a envoyé le message. Si l'utilisateur a envoyé le message en tant qu'un autre utilisateur ou au nom d'un autre utilisateur, ce champ renvoie l'adresse e-mail de l'utilisateur au nom duquel le message a été envoyé, et non l'adresse e-mail de l'expéditeur réel.
subject	Objet de l'e-mail.

`OUTGOING_EMAIL_SENT`

Cet événement est consigné lorsqu'un e-mail sortant est correctement remis à un destinataire cible. Il est consigné une fois pour chaque destinataire. Par conséquent, un seul événement `OUTGOING_EMAIL_SUBMITTED` peut entraîner plusieurs entrées `OUTGOING_EMAIL_SENT`.

Champ	Description
destinataire	Destinataire de l'e-mail remis avec succès.
sender	Adresse e-mail de l'utilisateur qui a envoyé l'e-mail au nom d'un autre utilisateur. Ce champ

Champ	Description
	est défini uniquement lorsqu'un e-mail est envoyé au nom d'un autre utilisateur.
from	Adresse d'expédition (De), qui est généralement l'adresse e-mail de l'utilisateur qui a envoyé le message. Si l'utilisateur a envoyé le message en tant qu'un autre utilisateur ou au nom d'un autre utilisateur, ce champ renvoie l'adresse e-mail de l'utilisateur au nom duquel le message a été envoyé, et non l'adresse e-mail de l'expéditeur réel.
messageId	ID de message SMTP

`OUTGOING_EMAIL_BOUNCED`

Cet événement est enregistré lorsqu'un message sortant ne peut pas être remis à un destinataire cible. Les e-mails peuvent être renvoyés pour un certain nombre de raisons, comme une boîte aux lettres cible complète. Le système enregistre un rebond pour chaque destinataire, ce qui entraîne un e-mail renvoyé. Par exemple, si un message sortant est adressé à trois destinataires et les boîtes aux lettres de deux d'entre eux sont pleines, deux événements `OUTGOING_EMAIL_BOUNCED` sont consignés.

Champ	Description
bouncedRecipient	Destinataire prévu pour lequel le serveur de messagerie de destination a renvoyé le message à l'expéditeur.

`DMARC_POLICY_APPLIED`

Cet événement est consigné lorsqu'une stratégie DMARC est appliquée à un e-mail envoyé à votre organisation.

Champ	Description
from	Adresse d'expédition (De), qui est généralement l'adresse e-mail de l'utilisateur qui a envoyé le message. Si l'utilisateur a envoyé le message en tant qu'un autre utilisateur ou au nom d'un autre utilisateur, ce champ renvoie l'adresse e-mail de l'utilisateur au nom duquel le message a été envoyé, et non l'adresse e-mail de l'expéditeur réel.
recipients	Destinataires prévus du message.
policy	Stratégie DMARC appliquée, indiquant l'action à effectuer sur l'e-mail lorsque le contrôle DMARC échoue (NONE, QUARANTINE ou REJECT). Il s'agit de la même valeur que pour le champ dmarcPolicy de l'événement ORGANIZATION_EMAIL_RECEIVED.

Surveillance des journaux WorkMail d'audit Amazon

Vous pouvez utiliser les journaux d'audit pour contrôler l'accès aux boîtes aux lettres de votre WorkMail organisation Amazon. Amazon WorkMail enregistre cinq types d'événements d'audit qui peuvent être publiés sur CloudWatch Logs, Amazon S3 ou Amazon Firehouse. Vous pouvez utiliser les journaux d'audit pour surveiller l'interaction des utilisateurs avec les boîtes aux lettres de votre organisation, les tentatives d'authentification, l'évaluation des règles de contrôle d'accès, effectuer des appels aux fournisseurs de disponibilité vers des systèmes externes et surveiller les événements à l'aide de jetons d'accès personnels. Pour plus d'informations sur la configuration de la journalisation des audits, consultezActivation de la journalisation des audits.

Les sections suivantes décrivent les événements d'audit enregistrés par Amazon WorkMail, le moment où les événements sont transmis et les informations relatives aux champs des événements.

journaux d'accès aux boîtes aux lettres

Les événements d'accès aux boîtes aux lettres fournissent des informations sur l'action entreprise (ou tentée) sur tel ou tel objet de boîte aux lettres. Un événement d'accès à la boîte aux lettres est généré pour chaque opération que vous tentez d'exécuter sur un élément ou un dossier d'une boîte aux lettres. Ces événements sont utiles pour auditer l'accès aux données des boîtes aux lettres.

Champ	Description
event_timestamp	Quand l'événement s'est produit, en millisecondes depuis l'époque d'Unix.
request_id	L'ID qui identifie de manière unique la demande.
organization_arn	L'ARN de l' WorkMail organisation & Amazon à laquelle appartient l'utilisateur authentifié.
user_id	L'ID de l'utilisateur authentifié.
imitateur_id	L'identifiant de l'imitateur. Présent uniquement si la fonction d'usurpation d'identité a été utilisée pour la demande.
protocole ;	Le protocole utilisé. Le protocole peut être :`AutoDiscover` , `EWSIMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
adresse IP de la source	Adresse IP source de la demande.
user_agent	L'agent utilisateur à l'origine de la demande.
action	Action effectuée sur l'objet, qui peut être : `readread_hierarchy` ,`read_summary` ,`read_attachment` ,`read_permissions` , `createupdate`,`update_permissions` ,`update_re`

Champ	Description
	ad_state ,delete,submit_email_for_sending ,abort_sending_email , movemove_to,copy, oucopy_to.
owner_id	L'ID de l'utilisateur propriétaire de l'objet sur lequel on agit.
object_type	Type d'objet, qui peut être : dossier, message ou pièce jointe.
item_id	L'ID qui identifie de manière unique le message faisant l'objet de l'événement ou contenant la pièce jointe faisant l'objet de l'événement.
chemin_dossier	Le chemin du dossier sur lequel on agit ou le chemin du dossier contenant l'élément sur lequel on agit.
identifiant_dossier	ID identifiant de manière unique le dossier faisant l'objet de l'événement ou contenant l'objet objet de l'événement.
chemin_pièce jointe	Le chemin des noms d'affichage vers la pièce jointe concernée.
action_autorisée	Si l'action a été autorisée. Cela peut être vrai ou faux.

Journaux de contrôle d'accès

Des événements de contrôle d'accès sont générés chaque fois qu'une règle de contrôle d'accès est évaluée. Ces journaux sont utiles pour auditer les accès interdits ou pour déboguer les configurations de contrôle d'accès.

Champ	Description
event_timestamp	Quand l'événement s'est produit, en millisecondes depuis l'époque d'Unix.
request_id	L'ID qui identifie de manière unique la demande.
organization_arn	L'ARN de l' WorkMail organisation à laquelle appartient l'utilisateur authentifié.
user_id	L'ID de l'utilisateur authentifié.
imitateur_id	L'identifiant de l'imitateur. Présent uniquement si la fonction d'usurpation d'identité a été utilisée pour la demande.
protocole ;	Le protocole utilisé, qui peut être : `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` , `ActiveSync SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
adresse IP de la source	Adresse IP source de la demande.
scope	Le champ d'application de la règle, qui peut être : `AccessControl DeviceAccessControl` , ou`ImpersonationAccessControl` .
rule_id	ID de la règle de contrôle d'accès correspondante. Lorsqu'aucune règle ne correspond, rule_id n'est pas disponible.
accès_accordé	Si l'accès a été autorisé. Cela peut être vrai ou faux.

Journaux d'authentification

Les événements d'authentification contiennent des informations sur les tentatives d'authentification.

> **Note**
>
> Les événements d'authentification ne sont pas générés pour les événements d'authentification via l' WorkMail WebMail application Amazon.

Champ	Description
event_timestamp	Quand l'événement s'est produit, en millisecondes depuis l'époque d'Unix.
request_id	L'ID qui identifie de manière unique la demande.
organization_arn	L'ARN de l' WorkMail organisation à laquelle appartient l'utilisateur authentifié.
user_id	L'ID de l'utilisateur authentifié.
user	Le nom d'utilisateur avec lequel l'authentification a été tentée.
protocole ;	Le protocole utilisé, qui peut être : `AutoDiscover EWS`,`IMAP`,`WindowsOutlook` , `ActiveSync SMTP`,`WebMail`,`IncomingEmail` , ou`OutgoingEmail` .
adresse IP de la source	Adresse IP source de la demande.
user_agent	L'agent utilisateur à l'origine de la demande.
méthode	La méthode d'authentification. Actuellement, seule la version de base est prise en charge.

Champ	Description
auth_successful	Si la tentative d'authentification a réussi. Cela peut être vrai ou faux.
auth_failed_reason	La raison de l'échec de l'authentification . Présent uniquement en cas d'échec de l'authentification.
identifiant_jeton d'accès personnel	L'ID du jeton d'accès personnel utilisé pour l'authentification.

Journaux de jetons d'accès personnels

Un événement de jeton d'accès personnel (PAT) est généré pour chaque tentative de création ou de suppression d'un jeton d'accès personnel. Les événements relatifs aux jetons d'accès personnels fournissent des informations indiquant si les utilisateurs ont réussi à créer des jetons d'accès personnels. Les journaux des jetons d'accès personnels sont utiles pour auditer les utilisateurs finaux qui créent et suppriment les leurs PATs. La connexion de l'utilisateur avec des jetons d'accès personnels générera des événements dans les journaux d'authentification existants. Pour plus d'informations, consultez la section Journaux d'authentification.

Champ	Description
event_timestamp	Quand l'événement s'est produit, en millisecondes depuis l'époque d'Unix.
request_id	L'ID qui identifie de manière unique la demande.
organization_arn	L'ARN de l' WorkMail organisation à laquelle appartient l'utilisateur authentifié.
user_id	L'ID de l'utilisateur authentifié.
user	Le nom d'utilisateur de l'utilisateur qui a effectué cette action.

Champ	Description
protocole ;	Le protocole utilisé dans le cadre de l'action a eu lieu, qui peut être : webapp
adresse IP de la source	Adresse IP source de la demande.
user_agent	L'agent utilisateur à l'origine de la demande.
action	L'action du jeton d'accès personnel, qui peut être : créer ou supprimer.
name	Le nom du jeton d'accès personnel.
expiration_heure	Date d'expiration du jeton d'accès personnel.
portées	Étendue des autorisations relatives aux jetons d'accès personnels sur la boîte aux lettres.

Logs des fournisseurs de disponibilité

Les événements relatifs aux fournisseurs de disponibilité sont générés pour chaque demande de disponibilité WorkMail qu'Amazon effectue en votre nom auprès du fournisseur de disponibilité configuré. Ces événements sont utiles pour débugger la configuration de votre fournisseur de disponibilité.

Champ	Description
event_timestamp	Quand l'événement s'est produit, en millisecondes depuis l'époque d'Unix.
request_id	L'ID qui identifie de manière unique la demande.
organization_arn	L'ARN de l' WorkMail organisation à laquelle appartient l'utilisateur authentifié.
user_id	L'ID de l'utilisateur authentifié.

Champ	Description
type	Le type de fournisseur de disponibilité invoqué, qui peut être : `EWS` ou`LAMBDA`.
domaine	Domaine pour lequel la disponibilité est obtenue.
fonction_arn	L'ARN du Lambda invoqué, si le type est LAMBDA. Dans le cas contraire, ce champ n'est pas présent.
ews_endpoint	Le point de terminaison EWS est de type EWS. Dans le cas contraire, ce champ n'est pas présent.
error_message	Le message décrivant la cause de l'échec. Si la demande a abouti, ce champ n'est pas présent.
événement_disponibilité réussi	Si la demande de disponibilité a été traitée avec succès.

Utilisation d' CloudWatch Insights avec Amazon WorkMail

Si vous avez activé la journalisation des événements par e-mail dans la WorkMail console Amazon ou activé la livraison des journaux d'audit à CloudWatch Logs, vous pouvez utiliser Amazon CloudWatch Logs Insights pour interroger vos journaux d'événements. Pour plus d'informations sur l'activation de la journalisation des événements de messagerie, consultez Activation de l'enregistrement des événements par e-mail. Pour plus d'informations sur CloudWatch Logs Insights, consultez Analyser les données des CloudWatch journaux avec Logs Insights dans le guide de l'utilisateur Amazon CloudWatch Logs.

Les exemples suivants montrent comment interroger les CloudWatch journaux pour les événements de courrier électronique courants. Vous exécutez ces requêtes dans la CloudWatch console. Pour savoir comment exécuter ces requêtes, consultez Tutoriel : Exécuter et modifier un exemple de requête dans le guide de l'utilisateur Amazon CloudWatch Logs.

Example Découvrez pourquoi l'utilisateur B n'a pas reçu d'e-mail envoyé par l'utilisateur A.

L'exemple de code suivant montre comment rechercher un e-mail sortant envoyé par l'utilisateur A à l'utilisateur B, trié par horodatage.

```
fields @timestamp, traceId

| sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/
and event.eventName = "OUTGOING_EMAIL_SUBMITTED"
and event.recipients.0 like /(?i)userB@example.com/)
```

Cela renvoie le message envoyé et l'ID de suivi. Utilisez l'ID de suivi dans l'exemple de code suivant pour interroger les journaux d'événements afin de rechercher le message envoyé.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

Cela renvoie l'ID de message et les événements de messagerie. `OUTGOING_EMAIL_SENT` indique que l'e-mail a été envoyé. `OUTGOING_EMAIL_BOUNCED` indique que l'e-mail a été renvoyé à l'expéditeur. Pour voir si l'e-mail a été reçu, effectuez une requête en utilisant l'ID de message dans l'exemple de code suivant.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter event.messageId like "$MESSAGEID"
```

Cela doit également renvoyer le message reçu, car il a le même ID de message Utilisez l'ID de suivi dans l'exemple de code suivant pour effectuer une requête concernant la transmission.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

Cela renvoie l'action de transmission et les actions de règle applicables.

Example Afficher tous les e-mails reçus d'un utilisateur ou d'un domaine

L'exemple de code suivant montre comment rechercher tous les e-mails reçus à partir d'un utilisateur spécifié.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like /(?i)user@example.com/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

L'exemple de code suivant montre comment rechercher tous les e-mails reçus à partir d'un domaine spécifié.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Example Découvrez qui a envoyé des e-mails renvoyés

L'exemple de code suivant montre comment rechercher les e-mails sortants qui ont été renvoyés à l'expéditeur, et renvoie également les raisons des retours à l'expéditeur.

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

L'exemple de code suivant montre comment rechercher les e-mails entrants qui ont été renvoyés. Il renvoie également les adresses e-mail des destinataires renvoyés et les raisons du rebond.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example Découvrez quels domaines envoient du spam

L'exemple de code suivant montre comment rechercher les destinataires de votre organisation qui reçoivent du courrier indésirable.

```
stats count(*) as c by event.recipients.0
```

```
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict =
 "FAIL")
| sort c desc
```

L'exemple de code suivant montre comment rechercher l'expéditeur des courriers indésirables.

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
| filter (event.spamVerdict = "FAIL")
```

Example Découvrez pourquoi un e-mail a été envoyé dans le dossier de courrier indésirable d'un destinataire

L'exemple de code suivant montre comment rechercher les e-mails identifiés comme courrier indésirable, filtrés par objet.

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
 event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?i)$SUBJECT/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED"
```

Vous pouvez également effectuer une requête par ID de suivi d'e-mail pour voir tous les événements associés à l'e-mail.

Example Afficher les e-mails conformes aux règles de flux d'e-mails

L'exemple de code suivant montre comment rechercher les e-mails qui correspondaient aux règles de flux de messagerie sortant.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

L'exemple de code suivant montre comment rechercher les e-mails qui correspondaient aux règles de flux de messagerie entrant.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
 event.ruleActions.0.recipients.0
```

```
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example Découvrez le nombre d'e-mails reçus ou envoyés par votre organisation

L'exemple de code suivant montre comment rechercher le nombre d'e-mails reçus par chaque destinataire de votre organisation.

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

L'exemple de code suivant montre comment rechercher le nombre d'e-mails envoyés par chaque expéditeur de votre organisation.

```
stats count(*) as c by event.from
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
| sort c desc
```

Journalisation des appels WorkMail d'API Amazon avec AWS CloudTrail

Amazon WorkMail est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS utilisateur sur Amazon WorkMail. CloudTrail capture tous les appels d'API pour Amazon WorkMail sous forme d'événements, y compris les appels depuis la WorkMail console Amazon et les appels de code vers Amazon WorkMail APIs. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon WorkMail. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon WorkMail, 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.

WorkMail Informations Amazon dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité a lieu sur Amazon WorkMail, elle est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et

télécharger les événements récents dans votreCompte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon WorkMail, vous devez créer un suivi. 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 d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. 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 en savoir plus, consultez :

- Présentation 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

Toutes les WorkMail actions Amazon sont enregistrées CloudTrail et documentées dans le Amazon WorkMail API Reference. À titre d'exemple, les appels des opérations d'API `CreateUser`, `CreateAlias` et `GetRawMessageContent` génèrent des entrées dans les fichiers journaux CloudTrail.

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 effectuée avec des informations d'identification d'utilisateur root ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou 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 des fichiers WorkMail journaux Amazon

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 individuelle à partir d'une source quelconque et comprend des informations sur l'action demandée, sur tous les paramètres, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne sont pas des séries ordonnées retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateUser`action de l' WorkMail API Amazon.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateAlias`action de l' WorkMail API Amazon.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
    "entityId": "a3a9176d-EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`GetRawMessageContent`action de l'API Amazon WorkMail Message Flow.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
```

```
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```


Activation de l'enregistrement des événements par e-mail

Vous activez la journalisation des événements par e-mail dans la WorkMail console Amazon afin de suivre les e-mails de votre organisation. La journalisation des événements par e-mail utilise un rôle Gestion des identités et des accès AWS lié à un service (SLR) pour autoriser la publication des journaux des événements par e-mail sur Amazon. CloudWatch Pour plus d'informations sur les rôles liés aux services IAM, consultez. Utilisation de rôles liés à un service pour Amazon WorkMail

Dans les journaux CloudWatch d'événements, vous pouvez utiliser des outils CloudWatch de recherche et des indicateurs pour suivre les messages et résoudre les problèmes liés aux e-mails. Pour plus d'informations sur les journaux d'événements auxquels Amazon WorkMail envoie CloudWatch, consultezSurveillance des journaux d'événements WorkMail liés aux e-mails d'Amazon. Pour plus d'informations sur CloudWatch les journaux, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

Rubriques

- Activation de la journalisation des événements de messagerie
- Création d'un groupe de journaux personnalisé et d'un rôle IAM pour la journalisation des événements par e-mail
- Désactivation de la journalisation des événements de messagerie
- Prévention du cas de figure de l'adjoint désorienté entre services

Activation de la journalisation des événements de messagerie

Voici ce qui se produit lorsque vous activez la journalisation des événements par e-mail à l'aide des paramètres par défaut, Amazon WorkMail :

- Crée un rôle Gestion des identités et des accès AWS lié à un service —. `AmazonWorkMailEvents`
- Crée un groupe de CloudWatch journaux —`/aws/workmail/emailevents/`*`organization-alias`*.
- Définit la durée de conservation des CloudWatch journaux à 30 jours.

Pour activer la journalisation des événements de messagerie

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Paramètres de journalisation.
4. Choisissez l'onglet Paramètres du journal du flux de courrier électronique.
5. Dans la section Paramètres du journal du flux d'e-mails, choisissez Modifier.
6. Déplacez le curseur Activer les événements de messagerie sur la position Activée.
7. Effectuez l'une des actions suivantes :

   - (Recommandé) Choisissez Utiliser les paramètres par défaut.
   - (Facultatif) Effacez les paramètres Utiliser par défaut et sélectionnez un groupe de journaux de destination et un rôle IAM dans les listes qui apparaissent.

   > **Note**
   >
   > Choisissez cette option uniquement si vous avez déjà créé un groupe de journaux et un rôle IAM personnalisé à l'aide duAWS CLI. Pour de plus amples informations, veuillez consulter Création d'un groupe de journaux personnalisé et d'un rôle IAM pour la journalisation des événements par e-mail.

8. Sélectionnez J'autorise Amazon WorkMail à publier les journaux sur mon compte en utilisant cette configuration.
9. Choisissez Enregistrer.

Création d'un groupe de journaux personnalisé et d'un rôle IAM pour la journalisation des événements par e-mail

Nous vous recommandons d'utiliser les paramètres par défaut lorsque vous activez la journalisation des événements par e-mail pour Amazon WorkMail. Si vous avez besoin d'une configuration de surveillance personnalisée, vous pouvez utiliser le AWS CLI pour créer un groupe de journaux dédié et un rôle IAM personnalisé pour la journalisation des événements de courrier électronique.

Pour créer un groupe de journaux et un rôle IAM personnalisés pour la journalisation des événements par e-mail

1. Utilisez la AWS CLI commande suivante pour créer un groupe de journaux dans la même AWS région que votre WorkMail organisation Amazon. Pour plus d'informations, consultez create-log-group dans la Référence des commandes de l'AWS CLI.

   ```
   aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
   ```

2. Créez un fichier contenant la stratégie suivante :

   JSON

   ```
   {
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Service": "events.workmail.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }
   ```

3. Utilisez la AWS CLI commande suivante pour créer un rôle IAM et joignez ce fichier en tant que document de politique de rôle. Pour plus d'informations, consultez create-role dans la Référence des commandes de l'AWS CLI.

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-
document file://trustpolicyforworkmail.json
```

> **Note**
>
> Si vous êtes un utilisateur de politiques `WorkMailFullAccess` gérées, vous devez inclure le terme `workmail` dans le nom du rôle. Cette stratégie gérée vous permet uniquement de configurer la journalisation des événements de messagerie à l'aide de rôles dont le nom contient `workmail`. Pour plus d'informations, consultez la section Octroi à un utilisateur des autorisations lui permettant de transmettre un rôle à un AWS service dans le Guide de l'utilisateur IAM.

4. Créez un fichier contenant la politique pour le rôle IAM que vous avez créée à l'étape précédente. Au minimum, la stratégie doit accorder à ce rôle les autorisations pour créer des flux de journaux et insérer des événements de journal dans le groupe de journaux que vous avez créé à l'étape 1.
5. Utilisez la AWS CLI commande suivante pour associer le fichier de politique au rôle IAM. Pour plus d'informations, consultez put-role-policy dans la Référence des commandes de l'AWS CLI.

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-
name workmail-permissions --policy-document file://rolepolicy.json
```

Désactivation de la journalisation des événements de messagerie

Désactivez la journalisation des événements par e-mail depuis la WorkMail console Amazon. Si vous n'avez plus besoin d'utiliser la journalisation des événements par e-mail, nous vous recommandons de supprimer également le groupe de CloudWatch journaux et le rôle lié au service associés. Pour de plus amples informations, veuillez consulter Supprimer un rôle lié à un service pour Amazon WorkMail.

Pour désactiver la journalisation des événements de messagerie

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Surveillance.
4. Dans la section Paramètres du journal, choisissez Modifier.
5. Déplacez le curseur Activer les événements de messagerie sur la position Off.
6. Choisissez Enregistrer.

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. EnAWS, 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 d'appel peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client auquel il n'aurait pas été autorisé à accéder autrement.

Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services auprès des principaux fournisseurs de services qui ont obtenu l'accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés de contexte dans les politiques de ressources afin de limiter les autorisations accordées par CloudWatch Logs et Amazon S3 aux services qui génèrent des journaux. Si vous utilisez les deux clés contextuelles de condition globale, les valeurs doivent utiliser le même identifiant de compte lorsqu'elles sont utilisées dans la même déclaration de politique.

Les valeurs de `aws:SourceArn` doivent être celles ARNs des sources de diffusion qui génèrent des 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.

Activation de la journalisation des audits

Vous pouvez utiliser les journaux d'audit pour recueillir des informations détaillées sur WorkMail l'utilisation de votre organisation Amazon. Les journaux d'audit peuvent être utilisés pour surveiller l'accès des utilisateurs aux boîtes aux lettres, vérifier les activités suspectes et déboguer les configurations des fournisseurs de contrôle d'accès et de disponibilité.

> **Note**
>
> La politique AmazonWorkMailFullAccessgérée n'inclut pas toutes les autorisations requises pour gérer les livraisons de journaux. Si vous utilisez cette politique pour gérer WorkMail, assurez-vous que le principal (par exemple, le rôle assumé) utilisé pour configurer les livraisons de journaux dispose également de toutes les autorisations requises.

Amazon WorkMail prend en charge trois destinations de livraison pour les journaux d'audit : CloudWatch Logs, Amazon S3 et Amazon Data Firehose. Pour plus d'informations, consultez la section Journalisation nécessitant des autorisations supplémentaires [V2] dans le guide de l'utilisateur Amazon CloudWatch Logs.

Outre les autorisations répertoriées sous Logging qui nécessitent des autorisations supplémentaires [V2], Amazon a WorkMail besoin d'une autorisation supplémentaire pour configurer la livraison des journaux :`workmail:AllowVendedLogDeliveryForResource`.

La livraison d'un journal de travail comprend trois éléments :

- DeliverySource, un objet logique qui représente la ou les ressources qui envoient les journaux. Pour Amazon WorkMail, il s'agit de l' WorkMailorganisation Amazon.
- A DeliveryDestination, qui est un objet logique qui représente la destination de livraison réelle.
- Une livraison, qui connecte une source de livraison à une destination de livraison.

Pour configurer la livraison des journaux entre Amazon WorkMail et une destination, vous pouvez effectuer les opérations suivantes :

- Créez une source de diffusion avec PutDeliverySource.

- Créez une destination de livraison avec PutDeliveryDestination.
- Si vous distribuez des journaux entre comptes, vous devez les utiliser PutDeliveryDestinationPolicydans le compte de destination pour attribuer une politique IAM à la destination. Cette politique autorise la création d'une livraison depuis la source de livraison dans le compte A vers la destination de livraison dans le compte B.
- Créez une livraison en associant exactement une source de livraison et une destination de livraison en utilisant CreateDelivery.

Les sections suivantes fournissent les détails des autorisations dont vous devez disposer lorsque vous êtes connecté pour configurer la livraison des journaux vers chaque type de destination. Ces autorisations peuvent être accordées à un rôle IAM avec lequel vous êtes connecté.

> **Important**
>
> Il est de votre responsabilité de supprimer les ressources de livraison de journaux après avoir supprimé la ressource génératrice de journaux.

Pour supprimer les ressources de livraison de journaux après avoir supprimé la ressource génératrice de journaux, procédez comme suit.

1. Supprimez la livraison à l'aide de l'DeleteDeliveryopération.
2. DeliverySourceSupprimez-le à l'aide de l'DeleteDeliverySourceopération.
3. Si le DeliveryDestinationfichier associé à DeliverySourcecelui que vous venez de supprimer n'est utilisé que pour ce DeliverySourceparamètre spécifique, vous pouvez le supprimer en utilisant l'DeleteDeliveryDestinationsopération.

Configuration de la journalisation des audits à l'aide de la WorkMail console Amazon

Vous pouvez configurer la journalisation des audits dans la WorkMail console Amazon :

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et sélectionnez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.

3. Choisissez Paramètres de journalisation.
4. Choisissez l'onglet Paramètres du journal d'audit.
5. Configurez les livraisons pour le type de journal requis à l'aide du widget approprié.
6. Choisissez Enregistrer.

Logs envoyés à CloudWatch Logs

Autorisations des utilisateurs

Pour activer l'envoi de CloudWatch journaux à Logs, vous devez être connecté avec les autorisations suivantes.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
```

```
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyCWL",
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

Politique de ressources du groupe de journaux

Le groupe de journaux dans lequel les journaux sont envoyés doit avoir une politique de ressources qui inclut certaines autorisations. Si le groupe de journaux n'a actuellement aucune politique de ressources et que l'utilisateur qui configure la journalisation dispose des `logs:DescribeLogGroups` autorisations

`logs:PutResourcePolicylogs:DescribeResourcePolicies`, et pour le groupe de journaux, crée AWS automatiquement la politique suivante pour celui-ci lorsque vous commencez à envoyer les CloudWatch journaux à Logs.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:my-log-group:log-
stream:*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "111122223333"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:*"
                    ]
                }
            }
        }
    ]
}
```

Considérations sur la limite de taille de la politique de ressources des groupes de journaux

Ces services doivent répertorier chaque groupe de journaux auquel ils envoient des journaux dans la politique de ressources. CloudWatch Les politiques relatives aux ressources des journaux sont limitées à 5 120 caractères. Un service qui envoie des journaux à un grand nombre de groupes de journaux peut respecter cette limite.

Pour atténuer ce problème, CloudWatch Logs surveille la taille des politiques de ressources utilisées par le service qui envoie les journaux. Lorsqu'il détecte qu'une politique approche la limite de taille de 5 120 caractères, CloudWatch Logs l'active automatiquement `/aws/vendedlogs/*` dans la politique de ressources pour ce service. Vous pouvez alors commencer à utiliser des groupes de journaux dont les noms commencent par `/aws/vendedlogs/` comme destinations des journaux provenant de ces services.

Journaux envoyés à Amazon S3

Autorisations des utilisateurs

Pour activer l'envoi de journaux à Amazon S3, vous devez être connecté avec les autorisations suivantes.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
```

```
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

Le compartiment S3 où les journaux sont envoyés doit avoir une politique de ressources qui inclut certaines autorisations. Si le compartiment n'a actuellement aucune politique de ressources et que l'utilisateur qui configure la journalisation dispose des `S3:PutBucketPolicy` autorisations `S3:GetBucketPolicy` et des autorisations pour le compartiment, il crée AWS automatiquement la politique suivante pour celui-ci lorsque vous commencez à envoyer les journaux à Amazon S3.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "account-id"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/111122223333/*",
            "Condition": {
```

```
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "account-id"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

Dans la politique précédente, pour`aws:SourceAccount`, spécifiez la liste des comptes IDs pour lesquels les journaux sont envoyés à ce compartiment. Pour`aws:SourceArn`, spécifiez la liste ARNs des ressources qui génèrent les journaux, dans le formulaire`arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Si le bucket dispose d'une politique de ressources, mais que cette politique ne contient pas l'instruction indiquée dans la stratégie précédente, et que l'utilisateur qui configure la journalisation dispose des `S3:PutBucketPolicy` autorisations `S3:GetBucketPolicy` et pour le bucket, cette instruction est ajoutée à la politique de ressources du bucket.

> **Note**
>
> Dans certains cas, des `AccessDenied` erreurs peuvent s'afficher AWS CloudTrail si l'`s3:ListBucket`autorisation n'a pas été accordée`delivery.logs.amazonaws.com`. Pour éviter ces erreurs dans vos CloudTrail journaux, vous devez accorder l'`s3:ListBucket`autorisation à`delivery.logs.amazonaws.com`. Vous devez également inclure les `Condition` paramètres indiqués dans l'`s3:GetBucketAcl`autorisation définie dans la politique de compartiment précédente. Pour rationaliser cela, au lieu d'en créer un nouveau`Statement`, vous pouvez directement mettre à jour le `AWSLogDeliveryAclCheck` futur`"Action": ["s3:GetBucketAcl", "s3:ListBucket"]`.

Chiffrement côté serveur des compartiments Amazon S3

Vous pouvez protéger les données de votre compartiment Amazon S3 en activant le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou le chiffrement côté serveur avec une clé stockée dans (SSE-KMS). AWS KMS AWS Key Management Service Pour plus d'informations, consultez Protection des données à l'aide du chiffrement côté serveur.

Si vous choisissez l'option SSE-S3, aucune configuration supplémentaire n'est requise. Amazon S3 gère la clé de chiffrement.

> **Warning**
>
> Si vous choisissez SSE-KMS, vous devez utiliser une clé gérée par le client, car l'utilisation d'une Clé gérée par AWS n'est pas prise en charge dans ce scénario. Si vous configurez le chiffrement à l'aide d'une clé AWS gérée, les journaux seront fournis dans un format illisible.

Lorsque vous utilisez une AWS KMS clé gérée par le client, vous pouvez spécifier le nom de ressource Amazon (ARN) de la clé gérée par le client lorsque vous activez le chiffrement des compartiments. Ajoutez ce qui suit à la politique de clé pour votre clé gérée par le client (et non à la politique de compartiment de votre compartiment S3), afin que le compte de livraison du journal puisse écrire dans votre compartiment S3.

Si vous choisissez SSE-KMS, vous devez utiliser une clé gérée par le client, car l'utilisation d'une clé AWS gérée n'est pas prise en charge dans ce scénario. Lorsque vous utilisez une AWS KMS clé gérée par le client, vous pouvez spécifier le nom de ressource Amazon (ARN) de la clé gérée par le client lorsque vous activez le chiffrement des compartiments. Ajoutez ce qui suit à la politique de clé pour votre clé gérée par le client (et non à la politique de compartiment de votre compartiment S3), afin que le compte de livraison du journal puisse écrire dans votre compartiment S3.

```
{
    "Sid":"Allow Logs Delivery to use the key",
    "Effect":"Allow",
    "Principal":{
        "Service":[
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action":[
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource":"*",
    "Condition":{
        "StringEquals":{
            "aws:SourceAccount":[
                "account-id"
            ]
        },
        "ArnLike":{
            "aws:SourceArn":[
                "arn:aws:logs:region:account-id:delivery-source:*"
            ]
        }
    }
}
```

Pour`aws:SourceAccount`, spécifiez la liste des comptes IDs pour lesquels les journaux sont envoyés à ce compartiment. Pour`aws:SourceArn`, spécifiez la liste ARNs des ressources qui génèrent les journaux, dans le formulaire`arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Logs envoyés à Firehose

Autorisations des utilisateurs

Pour activer l'envoi de logs à Firehose, vous devez être connecté avec les autorisations suivantes.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
```

```
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:us-east-1:111122223333:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
```

```
            "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

Rôles IAM utilisés pour les autorisations de ressources

Comme Firehose n'utilise pas de politiques de ressources, il AWS utilise les rôles IAM lors de la configuration de ces journaux à envoyer à Firehose. AWScrée un rôle lié à un service nommé. AWSServiceRoleForLogDelivery Ce rôle lié à un service comprend les autorisations suivantes.

Ce rôle lié à un service accorde l'autorisation à tous les flux de diffusion Firehose dont la `LogDeliveryEnabled` balise est définie sur. `true` AWSattribue cette balise au flux de diffusion de destination lorsque vous configurez la journalisation.

Ce rôle lié à un service possède également une politique d'approbation qui permet au principal du service `delivery.logs.amazonaws.com` d'assumer le rôle lié au service nécessaire. Cette politique d'approbation est la suivante :

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorisations spécifiques à la console

Outre les autorisations répertoriées dans les sections précédentes, si vous configurez la livraison des journaux à l'aide de la console au lieu de la APIs, vous devez également disposer des autorisations suivantes :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:*",
                "arn:aws:firehose:us-east-1:111122223333:deliverystream/*",
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "ListAccessForDeliveryDestinations",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Validation de conformité pour Amazon WorkMail

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon dans WorkMail le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des normes SOC, ISO et C5.

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, consultez la section Services AWS concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformité AWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide deAWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement des rapports dans AWS Artifact.

Lorsque vous utilisez Amazon WorkMail , votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWSfournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- AWSRessources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience chez Amazon WorkMail

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWSLes 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 mondiale.

Outre l'infrastructure AWS mondiale, Amazon WorkMail propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Sécurité de l'infrastructure sur Amazon WorkMail

> **Note**
>
> Amazon WorkMail a interrompu le support pour Transport Layer Security (TLS) 1.0 et 1.1. Si vous utilisez TLS 1.0 ou 1.1, vous devez mettre à niveau la version TLS vers la version 1.2. Pour plus d'informations, consultez TLS 1.2 pour devenir le niveau de protocole TLS minimal pour tous les points de terminaison d'API AWS.

En tant que service géré, Amazon WorkMail 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 AWSbien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon WorkMail 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.

Commencer à utiliser Amazon WorkMail

Après avoir terminé leConditions préalables, vous êtes prêt à commencer à utiliser Amazon WorkMail. Pour de plus amples informations, veuillez consulter Commencer à utiliser Amazon WorkMail.

Pour en savoir plus sur la migration des boîtes aux lettres existantes vers Amazon WorkMail, l'interopérabilité avec Microsoft Exchange et les WorkMail quotas Amazon, consultez les sections suivantes.

Rubriques

Commencer à utiliser Amazon WorkMail

Que vous soyez un nouvel WorkMail utilisateur d'Amazon ou un utilisateur existant d'Amazon WorkSpaces, commencez à utiliser Amazon WorkMail en suivant les étapes suivantes.

> **Note**
>
> Complétez la section Conditions préalables avant de commencer.

Rubriques

Étape 1 : connectez-vous à la WorkMail console Amazon

Vous devez vous connecter à la WorkMail console Amazon pour pouvoir ajouter des utilisateurs et gérer leurs comptes et boîtes aux lettres.

Pour vous connecter à la WorkMail console Amazon

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.
2. Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

Étape 2 : configurer votre WorkMail site Amazon

1. Une fois connecté à la WorkMail console Amazon, vous configurez votre organisation et ajoutez un domaine. Nous vous recommandons d'utiliser un domaine dédié pour votre WorkMail organisation Amazon. Pour plus d'informations, consultez Création d'une organisation et Ajout d'un domaine.
2. (Facultatif) Vous pouvez choisir d'utiliser un domaine de test gratuit fourni par Amazon WorkMail. Si vous choisissez de le faire, passez à l'étape 4.

> **Note**
>
> Les domaines de test utilisent le format suivant : *alias* .awsapps.com. Au fur et à mesure, n'oubliez pas que vous ne devez utiliser des domaines de test qu'à des fins de test. N'utilisez pas de domaine de test pour un environnement de production. Vous devez également avoir au moins un utilisateur activé dans votre WorkMail organisation Amazon. Si aucun utilisateur n'est activé, le domaine peut être enregistré et utilisé par d'autres clients.

3. Si vous utilisez un domaine externe, vérifiez ce domaine en ajoutant les enregistrements de texte (TXT) et d'échange de courrier (MX) appropriés à votre service DNS (Domain Name System). Les enregistrements TXT vous permettent de saisir des notes dans le DNS. Les enregistrements MX spécifient les serveurs de courrier entrant. Assurez-vous de définir votre domaine comme domaine par défaut pour votre organisation. Pour plus d'informations, consultez Vérification des domaines et Choix du domaine par défaut.
4. Créez de nouveaux utilisateurs ou activez les utilisateurs de votre annuaire existants pour Amazon WorkMail. Pour de plus amples informations, veuillez consulter Ajout d'un utilisateur.
5. (Facultatif) Si vous possédez déjà des boîtes aux lettres Microsoft Exchange, migrez-les vers Amazon WorkMail. Pour de plus amples informations, veuillez consulter Migration vers Amazon WorkMail.

Une fois que vous avez terminé de configurer votre WorkMail site Amazon, vous pouvez accéder à Amazon à WorkMail l'aide de l'URL de l'application Web.

Pour localiser l'URL de votre application WorkMail Web Amazon

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Pour ce faire, ouvrez la liste Sélectionnez une région située à droite du champ de recherche, puis choisissez la région souhaitée. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.

   La page des paramètres de l'organisation apparaît et affiche l'URL sous Connexion utilisateur. Ils URLs prennent le formulaire suivant : https ://*alias*.awsapps.com/mail.

Étape 3 : configurer WorkMail l'accès utilisateur Amazon

Choisissez l'une des options suivantes pour configurer WorkMail l'accès des utilisateurs Amazon :

- Configurez l'accès utilisateur à partir de votre client pour ordinateur de bureau existant à l'aide du client Microsoft Outlook. Pour plus d'informations, consultez Connect Microsoft Outlook à votre WorkMail compte Amazon.

- Configurez l'accès utilisateur depuis un appareil mobile, tel qu'un Kindle, un Android, un iPad ou un iPhone. Pour de plus amples informations, veuillez consulter Mise en route avec un appareil mobile.
- Pour configurer l'accès utilisateur, utilisez un logiciel client compatible avec le protocole IMAP (Internet Mail Access Protocol). Pour plus d'informations, consultez Connect IMAP clients à votre WorkMail compte Amazon.

Ressources supplémentaires

- Migration vers Amazon WorkMail
- Interopérabilité entre Amazon WorkMail et Microsoft Exchange
- WorkMail Quotas Amazon

Migration vers Amazon WorkMail

Vous pouvez migrer vers Amazon WorkMail depuis Microsoft Exchange, Microsoft Office 365, G Suite Basic (anciennement Google Apps for Work) et d'autres plateformes en collaborant avec l'un de nos partenaires. Pour plus d'informations sur nos partenaires, consultez Amazon WorkMail Features.

Rubriques

- Étape 1 : créer ou activer des utilisateurs sur Amazon WorkMail
- Étape 2 : migrer vers Amazon WorkMail
- Étape 3 : terminer la migration vers Amazon WorkMail

Étape 1 : créer ou activer des utilisateurs sur Amazon WorkMail

Avant de migrer vos utilisateurs, vous devez les ajouter dans Amazon WorkMail pour approvisionner leur boîte aux lettres. Pour de plus amples informations, veuillez consulter Ajout d'un utilisateur.

Étape 2 : migrer vers Amazon WorkMail

Vous pouvez travailler avec n'importe quel partenaire de AWS migration pour migrer vers Amazon WorkMail. Pour plus d'informations sur ces fournisseurs, consultez les WorkMailfonctionnalités d'Amazon.

Pour migrer vos boîtes aux lettres, créez un WorkMail utilisateur Amazon dédié qui agira en tant qu'administrateur de migration. La procédure suivante autorise cet utilisateur à accéder à toutes les boîtes aux lettres de votre organisation.

Pour créer un administrateur de migration

1. Effectuez l'une des actions suivantes :
   - Dans la WorkMail console Amazon, créez un nouvel utilisateur qui agira en tant qu'administrateur de migration. Pour de plus amples informations, veuillez consulter Ajout d'un utilisateur.
   - Dans votre Active Directory, créez un nouvel utilisateur qui agira en tant qu'administrateur de migration, puis activez l'utilisateur pour Amazon WorkMail. Pour de plus amples informations, veuillez consulter Activation des utilisateurs.
2. Dans le volet de navigation de la WorkMail console Amazon, choisissez Organizations, puis choisissez le nom de votre organisation.
3. Choisissez Paramètres de l'organisation, Migration, puis Modifier.
4. Déplacez le curseur activé pour la migration vers la position activée.
5. Ouvrez l'administrateur de migration et sélectionnez un utilisateur.
6. Choisissez Enregistrer.

Étape 3 : terminer la migration vers Amazon WorkMail

Après avoir migré vos comptes de messagerie vers Amazon WorkMail, vous pouvez vérifier vos enregistrements DNS et configurer vos clients de bureau et mobiles.

Pour terminer la migration vers Amazon WorkMail

1. Vérifiez que tous les enregistrements DNS sont mis à jour et qu'ils pointent vers Amazon WorkMail. Pour plus d'informations sur les enregistrements DNS requis, consultez la section Ajout d'un domaine.

   > **Note**
   >
   > Le processus de mise à jour des enregistrements DNS peut prendre plusieurs heures. Si de nouveaux éléments apparaissent dans une boîte aux lettres source pendant que les

enregistrements MX sont modifiés, vous pouvez exécuter à nouveau l'outil de migration pour migrer de nouveaux éléments après la mise à jour des enregistrements DNS.

2. Pour plus d'informations sur la configuration de vos clients de bureau ou mobiles pour utiliser Amazon WorkMail, consultez Connect Microsoft Outlook à votre WorkMail compte Amazon dans le guide de WorkMail l'utilisateur Amazon.

Interopérabilité entre Amazon WorkMail et Microsoft Exchange

L'interopérabilité entre Amazon WorkMail et Microsoft Exchange Server vous permet de minimiser les perturbations pour vos utilisateurs lorsque vous migrez des boîtes aux lettres vers Amazon WorkMail ou que vous utilisez Amazon WorkMail pour un sous-ensemble de vos boîtes aux lettres d'entreprise.

Cette l'interopérabilité vous permet d'utiliser le même domaine d'entreprise pour les boîtes aux lettres des deux environnements. Ainsi, vos utilisateurs peuvent planifier des réunions grâce au partage bidirectionnel des informations d' free/busy état du calendrier.

Prérequis

Avant d'activer l'interopérabilité avec Microsoft Exchange, procédez comme suit :

- Assurez-vous qu'au moins un utilisateur est activé pour Amazon. WorkMail Cela est nécessaire pour configurer les paramètres de disponibilité pour Microsoft Exchange. Pour activer un utilisateur, suivez les étapes décrites dans Activation du routage des e-mails pour un utilisateur.
- Configurez un connecteur Active Directory (AD Connector). La configuration d'un AD Connector avec votre annuaire local permet aux utilisateurs de continuer à utiliser leurs informations d'identification d'entreprise existantes. Pour plus d'informations, consultez Create an AD Connector et intégrez Amazon WorkMail à votre annuaire local.
- Configurez votre WorkMail organisation Amazon. Créez une WorkMail organisation Amazon qui utilise l'AD Connector que vous avez configuré.
- Ajoutez vos domaines d'entreprise à votre WorkMail organisation Amazon, puis vérifiez-les dans la WorkMail console Amazon. Sinon, les e-mails envoyés à cet alias seront renvoyés à l'expéditeur. Pour de plus amples informations, veuillez consulter Utilisation des domaines.
- Migrez les boîtes aux lettres vers Amazon WorkMail. Permettez aux utilisateurs de provisionner et de migrer des boîtes aux lettres de votre environnement sur site vers Amazon. WorkMail Pour plus d'informations, consultez Activer les utilisateurs existants et voir Migration vers Amazon WorkMail.

> **Note**
>
> Ne mettez pas à jour les enregistrements DNS pour qu'ils pointent vers Amazon WorkMail. Ainsi, Microsoft Exchange reste le serveur principal pour les e-mails entrants tant que vous souhaitez une interopérabilité entre les deux environnements.

- Assurez-vous que les noms principaux d'utilisateur (UPNs) dans Active Directory correspondent aux adresses SMTP principales des utilisateurs.

Amazon WorkMail envoie des requêtes HTTPS à l'URL d'Exchange Web Services (EWS) sur Microsoft Exchange pour obtenir des free/busy informations de calendrier.

Pour les fournisseurs de disponibilité basés sur EWS, WorkMail Amazon envoie des requêtes HTTPS à l'URL des services Web Exchange (EWS) sur Microsoft Exchange afin d'obtenir des free/busy informations de calendrier. Par conséquent, les conditions préalables suivantes ne s'appliquent qu'aux fournisseurs de disponibilité basés sur EWS.

- Assurez-vous que les paramètres de pare-feu appropriés sont configurés pour autoriser l'accès depuis Internet. Le port par défaut pour les requêtes HTTPS est le port 443.
- Amazon ne WorkMail peut envoyer des requêtes HTTPS réussies à l'URL EWS sur Microsoft Exchange que lorsqu'un certificat signé par une autorité de certification (CA) valide est disponible dans votre environnement Microsoft Exchange. Pour plus d'informations, voir Créer une demande de certificat Exchange Server pour une autorité de certification sur le site Web de documentation Microsoft Exchange.
- Vous devez activer l'authentification de base pour EWS dans Microsoft Exchange. Pour de plus amples informations, veuillez consulter Virtual Directories: Exchange 2013 sur le site Microsoft MVP Award Program Blog.

Ajout de domaines et activation de boîtes aux lettres

Ajoutez les domaines de votre entreprise à Amazon WorkMail afin qu'ils puissent être utilisés dans les adresses e-mail. Assurez-vous que les domaines ajoutés à Amazon WorkMail sont vérifiés, puis autorisez les utilisateurs et les groupes à approvisionner des boîtes aux lettres sur Amazon WorkMail. Les ressources ne peuvent pas être activées dans Amazon WorkMail en mode interopérabilité et doivent être recréées dans Amazon WorkMail après avoir désactivé le mode interopérabilité. En revanche, vous pouvez tout de même les utiliser pour planifier des réunions lorsque le mode

interopérabilité est actif. Les ressources de Microsoft Exchange sont toujours affichées dans l'onglet Utilisateurs d'Amazon WorkMail.

- Pour de plus amples informations, veuillez consulter Ajout de domaines, Activation d'utilisateurs existants et Activation d'un groupe existant.

> **Note**
>
> Pour garantir l'interopérabilité avec Microsoft Exchange, ne mettez pas à jour les enregistrements DNS pour qu'ils pointent vers WorkMail des enregistrements Amazon. Microsoft Exchange reste le serveur principal pour les e-mails entrants tant que vous souhaitez une interopérabilité entre les deux environnements.

Activation de l'interopérabilité

Si vous n'avez pas créé d' WorkMail organisation Amazon, vous pouvez utiliser l'API publique pour créer une nouvelle WorkMail organisation avec le mode interopérabilité activé.

Si vous possédez déjà une WorkMail organisation Amazon dotée d'un AD Connector lié à Active Directory et que vous disposez également de Microsoft Exchange, contactez le support AWS pour obtenir de l'aide afin d'activer l'interopérabilité avec Microsoft Exchange pour une WorkMail organisation Amazon existante.

Création de comptes de service dans Microsoft Exchange et Amazon WorkMail

> **Note**
>
> La création d'un compte de service dans Exchange n'est pas requise lorsque Exchange n'est pas utilisé comme serveur principal pour un fournisseur de disponibilité personnalisé.

Pour accéder aux free/busy informations du calendrier, créez un compte de service sur Microsoft Exchange et Amazon WorkMail. Le compte de service Microsoft Exchange désigne tout utilisateur de Microsoft Exchange ayant accès aux free/busy informations de calendrier d'autres utilisateurs d'Exchange. L'accès est accordé par défaut ; aucune autorisation spéciale n'est donc requise.

De même, le compte WorkMail de service Amazon désigne tout utilisateur d'Amazon WorkMail ayant accès aux free/busy informations du calendrier d'autres WorkMail utilisateurs d'Amazon. Cet accès est également accordé par défaut. Vous devez créer l' WorkMail utilisateur Amazon dans votre annuaire local, puis activer cet utilisateur pour qu'Amazon WorkMail intègre Amazon WorkMail à AD Connector dans votre annuaire.

Limitations applicables au mode interopérabilité

Lorsque votre organisation est en mode interopérabilité, vous devez utiliser le centre d'administration Exchange pour gérer tous les utilisateurs, groupes et ressources. Pour activer WorkMail les utilisateurs et les groupes Amazon, utilisez le AWS Management Console. Pour de plus amples informations, veuillez consulter Activation d'utilisateurs existants et Activation d'un groupe existant.

Lorsque vous activez un utilisateur ou un groupe pour Amazon WorkMail, vous ne pouvez pas modifier les adresses e-mail ou les alias de ces utilisateurs et groupes. Ils doivent également être configurés via le centre d'administration Exchange. Amazon WorkMail synchronise les modifications apportées à votre annuaire toutes les quatre heures.

Les ressources ne peuvent pas être créées ou activées dans Amazon WorkMail en mode interopérabilité. Cependant, toutes vos ressources Exchange sont disponibles dans le carnet d' WorkMail adresses Amazon et peuvent être utilisées pour planifier des réunions comme d'habitude.

Configurer les paramètres de disponibilité sur Amazon WorkMail

Configurez les paramètres de disponibilité sur Amazon WorkMail pour permettre d'interroger des systèmes externes, de proposer des fonctionnalités de calendrier et d'obtenir des informations de calendrier free/busy . Amazon WorkMail prend en charge deux modes d'obtention d' free/busy informations à partir d'un système distant :

- Exchange Web Services (EWS) : dans cette configuration, Amazon WorkMail interroge un serveur Exchange ou une autre WorkMail organisation pour obtenir des informations de disponibilité à l'aide du protocole EWS. Il s'agit de la configuration la plus simple, mais elle nécessite que le point de terminaison EWS du serveur Exchange soit accessible via Internet public.
- Fournisseur de disponibilité personnalisé (CAP) : dans cette configuration, un administrateur peut configurer une fonction AWS Lambda afin d'obtenir des informations sur la disponibilité des utilisateurs pour un domaine de messagerie donné. En fonction de la plate-forme de votre serveur de messagerie, l'utilisation de CAP avec Amazon WorkMail offre les avantages suivants :

- Bénéficiez de la disponibilité des utilisateurs grâce à l'EWS interne sans avoir à ouvrir leur pare-feu WorkMail.
- Bénéficiez de la disponibilité des utilisateurs à partir de systèmes autres qu'Exchange ou EWS, tels que Google Workspace (anciennement connu sous le nom de G Suite).

Rubriques

Configuration d'un fournisseur de disponibilité basé sur EWS

Pour configurer des paramètres de disponibilité basés sur EWS sur la console, procédez comme suit :

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Pour ce faire, ouvrez la liste Sélectionnez une région située à droite du champ de recherche, puis choisissez la région souhaitée. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom d'une organisation.
3. Dans le volet de navigation, choisissez Paramètres de l'organisation, puis sélectionnez l'onglet Interopérabilité.
4. Choisissez Ajouter une configuration de disponibilité, puis entrez les informations suivantes :

   - Type — Sélectionnez EWS.
   - Domaine : domaine pour lequel WorkMail vous tenterez de demander des informations de disponibilité à l'aide de cette configuration.
   - URL EWS — Amazon WorkMail demandera cette URL au point de terminaison EWS. Consultez la section Obtenir l'URL EWS de ce guide.
   - Adresse e-mail de l'utilisateur : adresse e-mail de l'utilisateur qui WorkMail sera utilisée pour s'authentifier auprès du point de terminaison EWS.
   - Mot de passe : mot de passe qui WorkMail sera utilisé pour s'authentifier auprès du point de terminaison EWS.

5. Choisissez Enregistrer.

Obtenir l'URL EWS

Pour obtenir l'URL EWS pour Exchange à l'aide de Microsoft Outlook, procédez comme suit :

1. Connectez-vous à Microsoft Outlook sous Windows pour un utilisateur de votre environnement Exchange.
2. Maintenez la touche Ctrl enfoncée et ouvrez le menu contextuel (clic droit) sur l'icône de Microsoft Outlook dans la barre des tâches.
3. Choisissez Test E-mail AutoConfiguration.
4. Entrez l'adresse e-mail de l'utilisateur de Microsoft Exchange et le mot de passe, puis sélectionnez Test.
5. Dans la fenêtre de résultats, copiez la valeur de l'URL du service de disponibilité.

Pour obtenir l'URL EWS pour Exchange en utilisant PowerShell, à l' PowerShell invite, exécutez la commande suivante :

```
Get-WebServicesVirtualDirectory |Select name, *url* | fl
```

Pour obtenir l'URL EWS d'Amazon WorkMail, recherchez d'abord le domaine EWS sous Amazon WorkMail endpoints and quotas. Entrez l'URL EWS `https://"EWS domain"/EWS/Exchange.asmx` et remplacez « domaine EWS » par votre domaine EWS.

Configuration d'un fournisseur de disponibilité personnalisé

Pour configurer un fournisseur de disponibilité personnalisé (CAP), procédez comme suit :

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Pour ce faire, ouvrez la liste Sélectionnez une région située à droite du champ de recherche, puis choisissez la région souhaitée.
2. Dans le volet de navigation, choisissez Organizations, puis le nom d'une organisation.
3. Dans le panneau de navigation, choisissez Paramètres de l'organisation, puis Interopérabilité.
4. Choisissez Ajouter une configuration de disponibilité, puis entrez les informations suivantes :

   - Type — Sélectionnez CAP Lambda.

- Domaine : domaine pour lequel WorkMail vous tenterez de demander des informations de disponibilité à l'aide de cette configuration.
- ARN — L'ARN de la fonction Lambda qui fournira les informations de disponibilité.

Pour créer une fonction CAP Lambda, consultez. Création d'une fonction Lambda de fournisseur de disponibilité personnalisé

Création d'une fonction Lambda de fournisseur de disponibilité personnalisé

Les fournisseurs de disponibilité personnalisés (CAPs) sont configurés avec un protocole de demande et de réponse basé sur JSON écrit dans un schéma JSON bien défini. Une fonction Lambda analysera la demande et fournira une réponse valide.

Rubriques

- Éléments de demande et de réponse
- Octroi d'accès
- Exemple d' WorkMail utilisation par Amazon d'une fonction CAP Lambda

Éléments de demande et de réponse

Éléments d'une demande

Voici un exemple de demande utilisé pour configurer un CAP pour un WorkMail utilisateur Amazon :

```
{
    "requester": {
        "email": "user1@internal.example.com",
        "userName": "user1",
        "organization": "m-0123456789abcdef0123456789abcdef",
        "userId": "S-1-5-18",
        "origin": "127.0.0.1"
    },
    "mailboxes": [
        "user2@external.example.com",
        "unknown@internal.example.com"
    ],
    "window": {
        "startDate": "2021-05-04T00:00:00.000Z",
        "endDate": "2021-05-06T00:00:00.000Z"
```

```
    }
}
```

Une demande est composée de trois sections : demandeur, boîtes aux lettres et fenêtre. Ils sont décrits dans ce qui suit Demandeur et dans Fenêtre les sections de ce guide. Boîtes aux lettres

Demandeur

La section du demandeur fournit des informations sur l'utilisateur qui a fait la demande initiale à Amazon WorkMail. CAPs utilisez ces informations pour modifier le comportement du fournisseur. Par exemple, ces données peuvent être utilisées pour se faire passer pour le même utilisateur auprès du fournisseur de disponibilité du backend ou certains détails peuvent être omis de la réponse.

Champ	Description	Obligatoire
`Email`	Adresse e-mail principale du demandeur.	Oui
`Username`	Le nom d'utilisateur du demandeur.	Oui
`Organization`	ID d'organisation du demandeur.	Oui
`UserID`	L'ID du demandeur.	Oui
`Origin`	Adresse distante de la demande.	Non
`Bearer`	Réservé pour un usage futur.	Non

Boîtes aux lettres

La section des boîtes aux lettres contient une liste séparée par des virgules des adresses e-mail des utilisateurs pour lesquels des informations de disponibilité sont demandées.

Fenêtre

La section fenêtre contient la fenêtre horaire pour laquelle les informations de disponibilité sont demandées. Les deux `startDate` `endDate` sont spécifiés en UTC et sont formatés conformément

à la RFC 3339. Les événements ne devraient pas être tronqués. En d'autres termes, si un événement commence avant la date définie`StartDate`, le début d'origine sera utilisé.

Éléments de réponse

Amazon WorkMail attendra 25 secondes pour obtenir une réponse de la fonction CAP Lambda. Au bout de 25 secondes, Amazon WorkMail considérera que la fonction a échoué et générera des défaillances pour les boîtes aux lettres associées dans la GetUserAvailability réponse EWS. Cela n'entraînera pas l'échec de l' GetUserAvailability opération.

Voici un exemple de réponse issu de la configuration définie au début de cette section :

```
{
    "mailboxes": [{
        "mailbox": "user2@external.example.com",
        "events": [{
            "startTime": "2021-05-03T23:00:00.000Z",
            "endTime": "2021-05-04T03:00:00.000Z",
            "busyType": "BUSY"|"FREE"|"TENTATIVE",
            "details": {  // optional
                "subject": "Late meeting",
                "location": "Chime",
                "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
                "isMeeting": true,
                "isReminderSet": true,
                "isPrivate": false
            }
        }],
        "workingHours": {
            "timezone": {
                "name": "W. Europe Standard Time"
                "bias": 60,
                "standardTime": {  // optional (not needed for fixed offsets)
                    "offset": 60,
                    "time": "02:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
                "daylightTime": {  // optional (not needed for fixed offsets)
                    "offset": 0,
                    "time": "03:00:00",
```

```
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
            },
            "workingPeriods":[{
                "startMinutes": 480,
                "endMinutes": 1040,
                "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
            }]
        }
    },{
        "mailbox": "unknown@internal.example.com",
        "error": "MailboxNotFound"
    }]
}
```

Une réponse est composée d'une seule section de boîtes aux lettres qui consiste en une liste de boîtes aux lettres. Chaque boîte aux lettres dont la disponibilité est obtenue avec succès est composée de trois sections : boîte aux lettres, événements et heures de travail. Si le fournisseur de disponibilité n'a pas réussi à obtenir les informations de disponibilité d'une boîte aux lettres, la section est composée de deux sections : boîte aux lettres et erreur. Ils sont décrits dans les Erreur sections suivantes Boîte aux lettres de ce guide. Événements Heures de travail Fuseau horaire Périodes de travail

Boîte aux lettres

La section boîte aux lettres est l'adresse e-mail de l'utilisateur trouvée dans la section boîtes aux lettres de la demande.

Événements

La section des événements est une liste des événements qui se produisent dans la fenêtre demandée. Chaque événement est défini avec les paramètres suivants :

Champ	Description	Obligatoire
`startTime`	Heure de début de l'événement en UTC et formatée conformément à la RFC 3339.	Oui

Champ	Description	Obligatoire
`endTime`	Heure de fin de l'événement en UTC et formatée conformément à la RFC 3339.	Oui
`busyType`	Type d'événement très fréquenté. Peut être `Busy`, `Free` ou `Tentative` .	Oui
`details`	Les détails de l'événement.	Non
`details.subject`	Le sujet de l'événement.	Oui
`details.location`	Le lieu de l'événement.	Oui
`details.instanceType`	Type d'instance de l'événement. Peut être `Single_Instance` , `Recurring_Instance` ou `Exception` .	Oui
`details.isMeeting`	Un booléen pour indiquer si l'événement a des participants.	Oui
`details.isReminderSet`	Un booléen pour indiquer si un rappel est défini pour l'événement.	Oui
`details.isPrivate`	Un booléen pour indiquer si l'événement est défini comme privé.	Oui

Heures de travail

La section Heures de travail contient des informations sur les heures de travail du propriétaire de la boîte aux lettres. Il contient deux sections : timezone et WorkingPeriods.

Fuseau horaire

La sous-section fuseau horaire décrit le fuseau horaire du propriétaire de la boîte aux lettres. Il est important d'afficher correctement les heures de travail de l'utilisateur lorsque le demandeur travaille dans un autre fuseau horaire. Le fournisseur de disponibilité est tenu de décrire explicitement le fuseau horaire, plutôt que d'utiliser un nom. L'utilisation de la description normalisée du fuseau horaire permet d'éviter les incohérences entre les fuseaux horaires.

Champ	Description	Obligatoire
`name`	Le nom du fuseau horaire.	Oui
`bias`	Décalage par défaut par rapport à l'heure GMT en minutes.	Oui
`standardTime`	Début de l'heure normale pour le fuseau horaire spécifié.	Non
`daylightTime`	Début de l'heure d'été pour le fuseau horaire spécifié.	Non

Vous devez soit définir `standardTime` les deux`daylightTime`, soit omettre les deux. Les champs de l'`daylightTime`objet `standardTime` et sont les suivants :

Champ	Description	Valeurs autorisées
`offset`	Le décalage par rapport au décalage par défaut en minutes.	NA
`time`	Heure à laquelle la transitio n entre l'heure normale et l'heure d'été a lieu, spécifiée sous la forme`hh:mm:ss`.	NA

Champ	Description	Valeurs autorisées
`month`	Le mois au cours duquel la transition entre l'heure normale et l'heure d'été a lieu.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	Semaine du mois spécifié pendant laquelle la transitio n entre l'heure normale et l'heure d'été a lieu.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`
`dayOfWeek`	Le jour de la semaine spécifiée où la transition entre l'heure normale et l'heure d'été a lieu.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Périodes de travail

La section WorkingPeriods contient un ou plusieurs objets de période de travail. Chaque période définit un début et une fin de journée de travail pour un ou plusieurs jours.

Champ	Description	Valeurs autorisées
`startMinutes`	Début de la journée de travail en quelques minutes à partir de minuit.	NA
`endMinutes`	Fin de la journée de travail en quelques minutes à partir de minuit.	NA
`days`	Les jours auxquels cette période s'applique.	`SUN`, `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`

Erreur

Le champ d'erreur peut contenir des messages d'erreur arbitraires. Le tableau suivant répertorie un mappage des codes connus avec les codes d'erreur EWS. Tous les autres messages seront mappés vers. `ERROR_FREE_BUSY_GENERATION_FAILED`

Valeur	Code d'erreur EWS	
`MailboxNotFound`	`ERROR_MAIL_RECIPIENT_NOT_FOUND`	
`ErrorAvailabilityConfigNotFound`	`ERROR_AVAILABILITY_CONFIG_NOT_FOUND`	
`ErrorServerBusy`	`ERROR_SERVER_BUSY`	
`ErrorTimeoutExpired`	`ERROR_TIMEOUT_EXPIRED`	
`ErrorFreeBusyGenerationFailed`	`ERROR_FREE_BUSY_GENERATION_FAILED`	
`ErrorResponseSchemaValidation`	`ERROR_RESPONSE_SCHEMA_VALIDATION`	

Octroi d'accès

Exécutez la commande Lambda suivante à partir du AWS Command Line Interface ()AWS CLI. Cette commande ajoute une politique de ressources à la fonction Lambda qui analyse le CAP. Cette fonction permet au service de WorkMail disponibilité Amazon d'appeler votre fonction Lambda.

```
aws lambda add-permission \
    --region LAMBDA_REGION \
    --function-name CAP_FUNCTION_NAME \
    --statement-id AllowWorkMail \
    --action "lambda:InvokeFunction" \
    --principal availability.workmail.WM_REGION.amazonaws.com \
    --source-account WM_ACCOUNT_ID \
    --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

Dans la commande, ajoutez les paramètres suivants là où cela est indiqué :

- *LAMBDA_REGION*— Nom de la région dans laquelle le CAP Lambda est déployé. Par exemple, `us-east-1`.
- *CAP_FUNCTION_NAME*— Nom de la fonction CAP Lambda.

> **Note**
>
> Il peut s'agir du nom, de l'alias ou de l'ARN partiel ou complet de la fonction CAP Lambda.

- *WM_REGION*— Nom de la région dans laquelle l' WorkMail organisation Amazon invoque la fonction Lambda.

> **Note**
>
> Seules les régions suivantes peuvent être utilisées avec CAP :
>
> - USA Est (Virginie du Nord)
> - USA Ouest (Oregon)
> - Europe (Irlande)

- *WM_ACCOUNT_ID*— L'identifiant du compte de l'organisation.
- *ORGANIZATION_ID*— L'ID de l'organisation qui invoque le CAP Lambda. Par exemple, ID d'organisation : m-934ebb9eb57145d0a6cab566ca81a21f.

> **Note**
>
> *LAMBDA_REGION*et ne *WM_REGION* sera différent que si des appels interrégionaux sont nécessaires. Si les appels interrégionaux ne sont pas nécessaires, ils seront identiques.

Exemple d' WorkMail utilisation par Amazon d'une fonction CAP Lambda

Pour un exemple d'Amazon WorkMail utilisant une fonction CAP Lambda pour interroger un point de terminaison EWS, consultez cet AWS exemple d'application sur le référentiel Serverless applications for Amazon. WorkMail GitHub

Configuration des paramètres de disponibilité de Microsoft Exchange

Pour rediriger toutes les demandes free/busy d'informations de calendrier pour les utilisateurs autorisés vers Amazon WorkMail, configurez un espace d'adressage de disponibilité dans Microsoft Exchange.

Utilisez la PowerShell commande suivante pour créer l'espace d'adressage :

```
$credentials = Get-Credential
```

À l'invite, entrez les informations d'identification du compte de WorkMail service Amazon. Le nom d'utilisateur doit être saisi sous la forme **domain\username** (c'est-à-dire,***orgname*.awsapps.com\workmail_service_account_*username***. Ici, ***orgname*** représente le nom de l' WorkMail organisation Amazon. Pour de plus amples informations, veuillez consulter Création de comptes de service dans Microsoft Exchange et Amazon WorkMail.

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -
Credentials $credentials
```

Pour plus d'informations, voir Add- AvailabilityAddressSpace on Microsoft Docs.

Activer le routage des e-mails entre les WorkMail utilisateurs de Microsoft Exchange et d'Amazon

Grâce au routage des e-mails entre Microsoft Exchange Server et Amazon WorkMail, les utilisateurs peuvent conserver leurs adresses e-mail existantes après leur migration vers Amazon WorkMail. Le routage des e-mails vous permet de conserver Microsoft Exchange Server comme serveur SMTP (Simple Mail Transfer Protocol) principal pour le courrier entrant de votre organisation.

Avant d'utiliser le routage des e-mails, vous devez remplir les conditions préalables suivantes :

- Activez le mode d'interopérabilité pour votre organisation. Pour de plus amples informations, veuillez consulter Activation de l'interopérabilité.
- Assurez-vous que votre domaine apparaît dans la WorkMail console Amazon.
- Vérifiez que notre serveur Microsoft Exchange peut envoyer des e-mails sur Internet. Vous devrez peut-être configurer un connecteur d'envoi. Pour plus d'informations sur les connecteurs d'envoi,

consultez la section Créer un connecteur d'envoi dans Exchange Server pour envoyer du courrier électronique sur Internet dans la documentation Microsoft.

Activation du routage des e-mails pour un utilisateur

Nous vous recommandons d'effectuer d'abord les étapes suivantes pour les utilisateurs de test avant d'appliquer des modifications à votre organisation.

1. Activez le compte utilisateur que vous souhaitez migrer vers Amazon WorkMail. Pour de plus amples informations, veuillez consulter Activation d'utilisateurs existants.
2. Dans la WorkMail console Amazon, assurez-vous qu'au moins deux adresses e-mail sont associées à l'utilisateur activé.
   - <*workmailuser*@ *orgname* .awsapps.com> (ceci est ajouté automatiquement et peut être utilisé pour des tests sans votre Microsoft Exchange.)
   - <*workmailuser*@ *yourdomain* .com> (cette adresse est ajoutée automatiquement et constitue l'adresse Microsoft Exchange principale.)

     Pour de plus amples informations, veuillez consulter Modification d'adresses e-mail d'utilisateurs.
3. Assurez-vous de migrer toutes les données de la boîte aux lettres de Microsoft Exchange vers celle d'Amazon WorkMail. Pour plus d'informations, consultez la section Migration vers Amazon WorkMail.
4. Une fois toutes les données migrées, désactivez la boîte aux lettres de l'utilisateur sur Microsoft Exchange. Créez ensuite un utilisateur de messagerie (ou utilisateur à extension messagerie) dont l'adresse SMTP externe pointe vers Amazon. WorkMail Pour ce faire, utilisez les commandes suivantes dans l'environnement de ligne de commande Exchange Management Shell :

> **Important**
>
> Les étapes suivantes effacent le contenu de la boîte aux lettres. Assurez-vous que vos données ont été migrées vers Amazon WorkMail avant de tenter d'activer le routage des e-mails. Certains clients de messagerie ne passent pas facilement à Amazon WorkMail lorsque vous exécutez cette commande. Pour de plus amples informations, veuillez consulter Configuration de client de messagerie.

```
$old_mailbox = Get-Mailbox exchangeuser
```

```
Disable-Mailbox $old_mailbox
```

```
$new_mailuser = Enable-MailUser $old_mailbox.Identity -
ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress
 $old_mailbox.PrimarySmtpAddress
```

```
Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -
HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
```

Dans les commandes ci-dessus, *orgname* représente le nom de votre WorkMail organisation Amazon. Pour plus d'informations, consultez Désactivation de la boîte aux lettres et Activation des utilisateurs de messagerie sur Microsoft TechNet.

5. Envoyez un e-mail de test à l'utilisateur (dans l'exemple ci-dessus,**workmailuser@yourdomain.com**). Si le routage des e-mails a été correctement activé, l'utilisateur doit pouvoir se connecter à sa WorkMail boîte aux lettres Amazon et recevoir l'e-mail.

> **Note**
>
> Microsoft Exchange reste le serveur principal pour les e-mails entrants tant que vous souhaitez disposer d'une interopérabilité entre les deux environnements. Pour garantir l'interopérabilité avec Microsoft Exchange, les enregistrements DNS ne doivent être mis à jour pour pointer vers Amazon WorkMail que plus tard.

Tâches post-configuration

Les étapes ci-dessus déplacent une boîte aux lettres d'un utilisateur de Microsoft Exchange Server vers Amazon WorkMail, tout en conservant l'utilisateur dans Microsoft Exchange en tant que contact. L'utilisateur migré étant désormais un utilisateur de messagerie externe, Microsoft Exchange Server impose des contraintes supplémentaires. Des exigences de configuration supplémentaires peuvent également être requises pour terminer la migration.

- Il se peut que l'utilisateur ne puisse pas envoyer d'e-mails à des groupes par défaut. Pour activer cette fonctionnalité, vous devez ajouter l'utilisateur à une liste d'expéditeurs fiables pour tous les groupes. Pour plus d'informations, consultez la section Gestion des livraisons sur Microsoft TechNet.
- L'utilisateur ne sera peut-être pas en mesure de réserver des ressources. Pour activer cette fonctionnalité, vous devez définir toutes les ressources auxquelles l'utilisateur doit accéder. `ProcessExternalMeetingMessages` Pour plus d'informations, consultez Set-CalendarProcessing sur Microsoft TechNet.

Configuration de client de messagerie

Certains clients de messagerie ne passent pas facilement à Amazon WorkMail. Ces clients demandent à l'utilisateur d'effectuer des étapes de configuration supplémentaires. Différents clients de messagerie requièrent différentes actions.

- Microsoft Outlook sous Windows : nécessite le redémarrage d'Outlook. Lors du démarrage, vous devez indiquer si vous souhaitez continuer à utiliser l'ancienne boîte aux lettres ou utiliser une boîte aux lettres temporaire. Choisissez l'option de boîte aux lettres temporaire. Reconfigurez ensuite la boîte aux lettres Microsoft Exchange.
- Microsoft Outlook sur macOS : au redémarrage d'Outlook, le message suivant s'affiche : Outlook a été redirigé vers le serveur ***orgname*** .awsapps.com. Voulez-vous que ce serveur configure vos paramètres ? Acceptez la suggestion.
- Mail sur iOS : l'application de messagerie cesse de recevoir des e-mails et génère un message d'erreur « Impossible de recevoir le courrier ». Recréez et reconfigurez la boîte aux lettres Microsoft Exchange.

Désactivation du mode interopérabilité et mise hors service de votre serveur de messagerie

Après avoir configuré vos boîtes aux lettres Microsoft Exchange pour Amazon WorkMail, vous pouvez désactiver le mode d'interopérabilité. Si vous n'avez migré aucun utilisateur ou enregistrement, la désactivation du mode interopérabilité n'affecte aucune de vos configurations.

> **Warning**
>
> Avant de désactiver le mode d'interopérabilité, assurez-vous de suivre toutes les étapes requises. Le non-respect de cette consigne peut entraîner le renvoi d'e-mails ou un comportement involontaire. Si vous n'avez pas terminé la migration, la désactivation de l'interopérabilité peut provoquer des interruptions dans votre organisation. Vous ne pouvez pas annuler cette opération.

Pour désactiver la prise en charge du mode interopérabilité

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation pour laquelle vous souhaitez désactiver le mode d'interopérabilité.
3. Sous Paramètres de l'organisation, choisissez Désactiver le mode d'interopérabilité.
4. Dans la boîte de dialogue Désactiver le mode d'interopérabilité, entrez le nom de l'organisation et choisissez Désactiver le mode d'interopérabilité.

Après avoir désactivé le support d'interopérabilité, les utilisateurs et les groupes qui ne sont pas activés pour Amazon WorkMail sont supprimés du carnet d'adresses. Vous pouvez toujours activer les utilisateurs ou groupes manquants à l'aide de la WorkMail console Amazon, et ils sont ajoutés au carnet d'adresses. Les ressources provenant de Microsoft Exchange ne peuvent pas être activées et n'apparaissent pas dans le carnet d'adresses tant que vous n'avez pas effectué l'étape ci-dessous.

- Création de ressources sur Amazon WorkMail — Vous pouvez créer des ressources sur Amazon, WorkMail puis configurer les délégués et les options de réservation pour ces ressources. Pour de plus amples informations, veuillez consulter Utilisation des ressources.
- Création d'un enregistrement AutoDiscover DNS : configurez un enregistrement AutoDiscover DNS pour tous les domaines de messagerie de l'organisation. Cela permet aux utilisateurs de se connecter à leurs WorkMail boîtes aux lettres Amazon à partir de leurs clients Microsoft Outlook et mobiles. Pour plus d'informations, consultez la section Utiliser AutoDiscover pour configurer les points de terminaison.

- Transférez votre enregistrement DNS MX vers Amazon WorkMail — Pour envoyer tous les e-mails entrants à Amazon WorkMail, vous devez transférer votre enregistrement DNS MX vers Amazon WorkMail. Les modifications apportées aux enregistrements DNS peuvent prendre jusqu'à 72 heures pour se propager à tous les serveurs DNS.
- Désactiver votre serveur de messagerie : après avoir vérifié que tous les e-mails sont acheminés directement vers Amazon WorkMail, vous pouvez désactiver votre serveur de messagerie si vous n'avez pas l'intention de l'utiliser à l'avenir.

Résolution des problèmes

Les solutions aux erreurs d' WorkMail interopérabilité et de migration les plus fréquemment rencontrées sur Amazon sont répertoriées ci-dessous.

L'URL des services Web Exchange (EWS) n'est pas valide ou est inaccessible. Vérifiez que vous disposez de l'URL EWS correcte. Pour de plus amples informations, veuillez consulter Configurer les paramètres de disponibilité sur Amazon WorkMail.

Échec de connexion lors de la validation EWS — Il s'agit d'une erreur générale qui peut être causée par :

- Aucune connexion Internet dans Microsoft Exchange.
- Votre pare-feu n'est pas configuré pour autoriser l'accès depuis Internet. Assurez-vous que le port 443 (port par défaut pour les requêtes HTTPS) est ouvert.

Si vous avez confirmé les paramètres de connexion Internet et de pare-feu, mais que l'erreur persiste, contactez AWS Support.

Nom d'utilisateur et mot de passe non valides lors de la configuration de l'interopérabilité avec Microsoft Exchange. Il s'agit d'une erreur générale qui peut être causée par :

- Le nom d'utilisateur qui n'est pas spécifié dans le format attendu. Utilisez le modèle suivant :

```
DOMAIN\username
```

- Votre serveur Microsoft Exchange qui n'est pas configuré pour l'authentification de base pour EWS. Pour de plus amples informations, veuillez consulter Virtual Directories: Exchange 2013 sur le site Microsoft MVP Award Program Blog.

L'utilisateur reçoit des e-mails avec une pièce jointe winmail.dat — Cela peut se produire lorsqu' S/MIME un e-mail crypté est envoyé d'Exchange à Amazon WorkMail et reçu dans Outlook 2016 pour Mac ou un client IMAP. La solution consiste à exécuter la commande suivante dans l'environnement de ligne de commande Exchange Management Shell.

Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

Si vous avez vérifié les éléments ci-dessus, mais que l'erreur persiste, contactez AWS Support.

WorkMail Quotas Amazon

Amazon WorkMail peut être utilisé à la fois par les entreprises clientes et les propriétaires de petites entreprises. Bien que nous prenions en charge la plupart des cas d'utilisation sans que vous ayez à configurer de changements de quotas, nous protégeons également nos utilisateurs et Internet d'éventuels abus du produit. Par conséquent, certains clients peuvent atteindre les quotas que nous avons fixés. Cette section présente ces quotas et la façon de les modifier.

Certaines valeurs de quota peuvent être modifiées, tandis que d'autres sont des quotas stricts qui ne peuvent pas être modifiés. Pour de plus amples informations sur la demande d'augmentation de quota, veuillez consulter les informations relatives aux quotas de service AWS dans la Référence générale d'Amazon Web Services.

Quotas d' WorkMail organisation et d'utilisateurs Amazon

Vous pouvez ajouter jusqu'à 25 utilisateurs à votre WorkMail organisation Amazon pour bénéficier d'un essai gratuit de 30 jours. Une fois cette période terminée, vous êtes débité pour tous les utilisateurs actifs, sauf si vous les supprimez ou fermez votre WorkMail compte Amazon.

Tous les messages envoyés à un autre utilisateur sont pris en compte lors de l'évaluation de ces quotas. Il s'agit des e-mails, demandes de réunion, réponses aux demandes de réunion, demandes de tâches et messages qui sont envoyés ou redirigés automatiquement grâce à une règle.

> **Note**
>
> Lorsque vous demandez une augmentation de quota pour une organisation spécifique, vous devez inclure le nom de l'organisation dans votre demande.

Ressource	Quota par défaut	Limite supérieure des demandes de modification
WorkMail Organisations Amazon par AWS compte	100	Peut être augmenté en fonction du type de répertoire d'une organisation. Vous pouvez consulter Directory Service les quotas et demander des augmentations depuis la AWS Directory Service console. Pour plus d'informations, consultez la rubrique Quotas dans le Références générales AWS.
Utilisateurs par WorkMail organisation Amazon	1 000	Peut être augmenté en fonction du type de répertoire de l'organisation, comme suit : • WorkMail Annuaire Amazon : jusqu'à 10 millions d'utilisateurs • Simple AD ou AD Connector, grand : jusqu'à 5 000 utilisateurs* • Simple AD ou AD Connector, petit : jusqu'à 5 000 utilisateurs* • Microsoft AD, hébergé par Directory Service : jusqu'à 10 millions d'utilisateurs en fonction de votre installation et de votre configuration, *Si vous utilisez Simple AD ou AD Connector, consultez AWS

Ressource	Quota par défaut	Limite supérieure des demandes de modification
		Directory Service pour plus d'informations.
Utilisateurs de l'évaluation gratuite	Jusqu'à 25 utilisateurs les 30 premiers jours	La période d'évaluation gratuite est valable uniquement pour les 25 premiers utilisateurs d'une organisation. Les utilisateurs supplémentaires ne sont pas compris dans l'offre d'évaluation gratuite.
Destinataires adressés par AWS compte et par jour	100 000 destinataires externes à l'organisation, sans quota strict du nombre de destinataires internes à l'organisation	Il n'y a pas de limite supérieure. Cependant, Amazon WorkMail est un service de messagerie professionnel qui n'est pas destiné à être utilisé pour des services de courrier électronique en masse. Pour ces services, consultez Amazon SES ou Amazon Pinpoint.
Destinataires adressés par AWS compte et par jour en utilisant l'un des domaines de test	200 destinataires, quelle que soit la destination	Le domaine de messagerie de test n'est pas destiné à une utilisation à long terme. Nous vous recommandons d'ajouter votre propre domaine et de l'utiliser comme domaine par défaut.

Les quotas pour les groupes sont définis par le répertoire sous-jacent.

WorkMail organisation établissant des quotas

Ressource	Quota par défaut
Nombre de domaines par WorkMail organisation Amazon	1 000 Il s'agit d'un quota strict qui ne peut pas être modifié.
Nombre de modèles d'expéditeurs dans les règles de flux de messagerie par règle	250 Il s'agit d'un quota strict qui ne peut pas être modifié.
Nombre de modèles d'expéditeurs dans les règles de flux de messagerie par organisation	1 000 Il s'agit d'un quota strict qui ne peut pas être modifié.

Quotas par utilisateur

Tous les messages envoyés à un autre utilisateur sont pris en compte lors de l'évaluation de ces quotas. Il s'agit des e-mails, demandes de réunion, réponses aux demandes de réunion, demandes de tâches et messages qui sont envoyés ou redirigés automatiquement grâce à une règle.

Ressource	Quota par défaut	Quota supérieur pour les demandes de modification
Taille maximale de la boîte de réception	50 Go Il s'agit d'un quota strict qui ne peut pas être modifié.	Ne s’applique pas
Nombre maximal d'alias par utilisateur	100 Il s'agit d'un quota strict qui ne peut pas être modifié.	Ne s’applique pas

Ressource	Quota par défaut	Quota supérieur pour les demandes de modification
Destinataires traités par utilisateur par jour en utilisant le domaine dont vous êtes propriétaire	10 000 destinataires externes à l'organisation, sans quota strict du nombre de destinataires internes à l'organisation.	Il n'y a pas de limite supérieure. Cependant, Amazon WorkMail est un service de messagerie professionnel qui n'est pas destiné à être utilisé pour des services de courrier électronique en masse. Pour ces services, consultez Amazon SES ou Amazon Pinpoint.

Quotas de messages

Tous les messages envoyés à un autre utilisateur sont pris en compte lors de l'évaluation de ces quotas. Il s'agit des e-mails, demandes de réunion, réponses aux demandes de réunion, demandes de tâches et messages qui sont envoyés ou redirigés automatiquement grâce à une règle.

Ressource	Quota par défaut
Taille maximale des messages entrants	29 Mo de données non codées. Les messages sont reçus au format MIME. La taille maximale du message MIME entrant est de 40 Mo. Il s'agit d'un quota strict qui ne peut pas être modifié.
Taille maximale des messages sortants	29 Mo de données non codées. Les messages sont envoyés au format MIME. La taille maximale du message MIME sortant est de 40 Mo.

Ressource	Quota par défaut
	Il s'agit d'un quota strict qui ne peut pas être modifié.
Nombre maximal de destinataires par message	500 Il s'agit d'un quota strict qui ne peut pas être modifié.
Nombre maximum de pièces jointes par message	500 Il s'agit d'un quota strict qui ne peut pas être modifié.

Utilisation des organisations

Sur Amazon WorkMail, votre organisation représente les utilisateurs de votre entreprise. Dans la WorkMail console Amazon, vous pouvez consulter la liste des organisations disponibles. Si vous n'en avez pas, vous devez créer une organisation pour pouvoir utiliser Amazon WorkMail.

Rubriques

Création d'une organisation

Pour utiliser Amazon WorkMail, vous devez d'abord créer une organisation. Un AWS compte peut avoir plusieurs WorkMail organisations Amazon. Lorsque vous créez une organisation, vous sélectionnez également un domaine pour l'organisation et vous configurez l'annuaire des utilisateurs et les paramètres de chiffrement.

Vous pouvez créer un nouvel WorkMail annuaire Amazon à utiliser par votre WorkMail organisation ou intégrer Amazon WorkMail à un annuaire existant. Vous pouvez utiliser Amazon WorkMail avec des annuaires existants des types suivants :

- Microsoft Active Directory sur site
- AWSManaged Active Directory (qui est un Microsoft AD géré par AWS Directory Service)
- Simple AD

En intégrant votre annuaire local, vous pouvez utiliser vos utilisateurs et groupes existants sur Amazon WorkMail et les utilisateurs peuvent se connecter avec leurs informations d'identification existantes. Si vous utilisez un annuaire local, vous devez d'abord configurer un AD Connector

dansAWS Directory Service. L'AD Connector synchronise vos utilisateurs et vos groupes avec le carnet d' WorkMail adresses Amazon et exécute les demandes d'authentification des utilisateurs. Pour plus d'informations, consultez la section Active Directory Connector dans le Guide d'Directory Serviceadministration.

Vous avez également la possibilité d'en sélectionner un AWS KMS key qu'Amazon WorkMail utilise pour chiffrer le contenu de la boîte aux lettres. Vous pouvez soit sélectionner la clé principale AWS gérée par défaut pour Amazon WorkMail, soit utiliser une clé KMS existante dans AWS Key Management Service (AWS KMS). Pour plus d'informations sur la création d'une nouvelle clé KMS, consultez la section Création de clés dans le guide du AWS Key Management Service développeur. Si vous êtes connecté en tant qu'utilisateur Gestion des identités et des accès AWS (IAM), devenez un administrateur clé sur la clé KMS. Pour plus d'informations, consultez la section Activation et désactivation des clés dans le guide du AWS Key Management Service développeur.

Considérations

N'oubliez pas les points suivants lorsque vous créez une WorkMail organisation Amazon :

- Amazon WorkMail ne prend actuellement pas en charge les services Microsoft Active Directory gérés que vous partagez avec plusieurs comptes.
- Si vous disposez d'un Active Directory local avec Microsoft Exchange et un AD Connector, nous vous recommandons de configurer les paramètres d'interopérabilité pour votre organisation. Cela vous permet de minimiser les perturbations pour vos utilisateurs lorsque vous migrez des boîtes aux lettres vers Amazon WorkMail ou que vous utilisez Amazon WorkMail pour un sous-ensemble de vos boîtes aux lettres d'entreprise. Pour de plus amples informations, veuillez consulter Interopérabilité entre Amazon WorkMail et Microsoft Exchange.
- Si vous sélectionnez l'option Domaine de test gratuit, vous pouvez commencer à utiliser votre WorkMail organisation Amazon avec le domaine de test fourni. Le domaine de test utilise le format suivant : *example* .awsapps.com. Vous pouvez utiliser le domaine de messagerie de test avec Amazon WorkMail et d'autres AWS services pris en charge tant que vous conservez les utilisateurs autorisés au sein de votre WorkMail organisation Amazon. Toutefois, vous ne pouvez pas utiliser le domaine de test à d'autres fins. Le domaine de test peut être disponible à l'enregistrement et à l'utilisation par d'autres clients si votre WorkMail organisation Amazon ne possède pas au moins un utilisateur activé.
- Amazon WorkMail ne prend pas en charge les annuaires multirégionaux.
- Amazon WorkMail synchronise les données d'annuaire avec AWS Managed Active Directory, Simple AD et AD Connector toutes les quatre heures.

Changements importants relatifs à l'utilisation de AWS Managed Active Directory

Amazon WorkMail met à jour son modèle d'autorisation pour les organisations qui utilisent AWS Managed Active Directory (Managed AD). Cette modification affecte la manière dont Amazon WorkMail interagit avec les données de l'annuaire et vous oblige à prendre des mesures spécifiques pour garantir le fonctionnement continu.

Auparavant, lorsqu'une WorkMail organisation Amazon était créée avec AWS Managed Active Directory, Amazon WorkMail utilisait des autorisations de niveau de service pour interagir avec Managed AD. Pour offrir aux clients une flexibilité supplémentaire leur permettant de séparer les rôles de gestion des annuaires et d'administration des boîtes aux lettres, WorkMail la console utilisera désormais AWS Directory Service Data (DS-Data) APIs pour créer ou mettre à jour des utilisateurs et des groupes dans AWS Managed Active Directories. APIs Un responsable IAM exécute ces opérations par le biais de la WorkMail console ou APIs devra également être autorisé à utiliser les actions DS-Data équivalentes contre le Managed AD associé à son WorkMail organisation, offrant ainsi un contrôle plus précis et une meilleure intégration aux politiques IAM.

Que vous créiez une nouvelle organisation avec Managed AD ou que vous ayez une organisation existante qui utilise Managed AD, si vous souhaitez continuer à créer, mettre à jour ou supprimer des utilisateurs et des groupes via la WorkMail console APIs, vous devrez également effectuer des étapes de configuration supplémentaires pour garantir le bon fonctionnement du modèle d'autorisation mis à jour. Ceci est expliqué dansthe section called “Intégration AD gérée”.

Rubriques

Création d'une organisation

Créez une nouvelle organisation dans la WorkMail console Amazon.

Pour créer une organisation

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans la barre de navigation, sélectionnez Organisation.

   La page Organizations apparaît et affiche vos organisations, le cas échéant.
3. Choisissez Créer une organisation.
4. Sous Domaine de messagerie, sélectionnez le domaine à utiliser pour les adresses e-mail de votre organisation :

   - Domaine Route 53 existant : sélectionnez un domaine existant que vous gérez avec une zone hébergée Amazon Route 53 (Route 53).
   - Nouveau domaine Route 53 — Enregistrez un nouveau nom de domaine Route 53 à utiliser avec Amazon WorkMail.
   - Domaine externe : entrez un domaine existant que vous gérez avec un fournisseur de système de noms de domaine (DNS) externe.
   - Domaine de test gratuit — Utilisez un domaine de test gratuit fourni par Amazon WorkMail. Vous pouvez explorer Amazon WorkMail à l'aide d'un domaine de test, puis ajouter un domaine à votre organisation ultérieurement.
5. (Facultatif) Si votre domaine est géré via Amazon Route 53, pour la zone hébergée Route 53, sélectionnez votre domaine Route 53.
6. Pour Alias, entrez un alias unique pour votre organisation.
7. Choisissez Paramètres avancés, puis dans Répertoire des utilisateurs, sélectionnez l'une des options suivantes :

   - Créer un nouvel WorkMail annuaire Amazon — Crée un nouveau répertoire pour ajouter et gérer vos utilisateurs.
   - Utiliser un annuaire existant : utilise un annuaire existant pour gérer vos utilisateurs, tel qu'un répertoire Microsoft Active Directory, AWS Managed Active Directory ou Simple AD sur site.
8. Pour le chiffrement, sélectionnez l'une des options suivantes :

- Utiliser une clé WorkMail gérée par Amazon : crée une nouvelle clé de chiffrement dans votre compte.
- Utiliser une clé KMS existante — Utilise une clé KMS existante que vous avez déjà créée dansAWS KMS.

9. Choisissez Créer une organisation.

Si vous utilisez un domaine externe, vérifiez-le en ajoutant le texte (TXT) et les enregistrements d'échange de courrier (MX) appropriés à votre service DNS. Les enregistrements TXT vous permettent de saisir des notes sur le service DNS. Les enregistrements MX spécifient le serveur de courrier entrant.

Assurez-vous de définir votre domaine comme domaine par défaut pour votre organisation. Pour plus d'informations, consultez Vérification des domaines et Choix du domaine par défaut.

Lorsque votre organisation est active, vous pouvez y ajouter des utilisateurs et configurer leurs clients de messagerie. Pour plus d'informations, consultez Ajout d'un utilisateur la section Configuration des clients de messagerie pour Amazon WorkMail.

Configuration de l'intégration d'AWS Managed Active Directory

Lorsque vous utilisez AWS Managed Active Directory avec votre WorkMail organisation Amazon, des étapes de configuration supplémentaires garantissent le bon fonctionnement du modèle d'autorisation mis à jour.

Pour configurer l'intégration de Managed AD pour les nouvelles organisations

1. Dans la Directory Service console, accédez à votre compte Managed AD (Microsoft AD) ou, depuis la WorkMail console Amazon, sélectionnez Utilisateurs ou groupes dans le panneau de navigation de gauche, puis cliquez sur le lien du répertoire dans la zone de note en haut de la page.
2. Choisissez Activer pour la gestion des utilisateurs et des groupes. Ce paramètre est désactivé par défaut et doit être activé pour effectuer des opérations d'écriture sur des utilisateurs et des groupes.
3. Assurez-vous que votre principal IAM dispose des autorisations requises en joignant une politique aux actions suivantes :

```
ds:AccessDSData
```

```
ds:ResetUserPassword
ds-data:CreateGroup
ds-data:DeleteGroup
ds-data:AddGroupMember
ds-data:RemoveGroupMember
ds-data:CreateUser
ds-data:DeleteUser
ds-data:UpdateUser
```

Pour migrer les organisations Managed AD existantes

1. Surveillez la page Utilisateurs ou groupes de la WorkMail console Amazon pour les notifications de migration.
2. Lorsque la notification apparaît, activez l'option Activer les opérations d'annuaire mises à jour pour migrer vers le nouveau Service APIs d'annuaire.
3. Enfin, assurez-vous d'avoir activé la gestion des utilisateurs et des groupes dans la Directory Service console et d'avoir mis à jour vos politiques IAM avec les autorisations DS-Data requises, comme décrit dans la section précédente.

L'utilisation de AWS Directory Service Data (DS-Data) APIs pour créer, mettre à jour et supprimer des utilisateurs sera activée pour toutes les WorkMail organisations Amazon restantes utilisant Managed AD lorsque cela n'a pas été activé auparavant.

Afficher les détails d'une organisation

Chacune de vos WorkMail organisations Amazon peut afficher une page détaillée de l'organisation. La page vous présente des informations sur leur organisation, y compris celles IDs que vous pouvez utiliser avec leAWS Command Line Interface. Les messages sur la page peuvent également vous indiquer toutes les étapes nécessaires pour terminer la configuration et l'organisation, telles qu'un domaine non vérifié ou un manque d'utilisateurs. Les messages fournissent également la première étape à suivre pour configurer un client de messagerie donné.

Pour consulter les détails de l'organisation

1. Dans la barre de navigation, sélectionnez Organisation.

   La page Organizations apparaît et affiche vos organisations.
2. Choisissez l'organisation que vous souhaitez consulter.

Intégration d'un WorkSpaces annuaire

Pour utiliser Amazon WorkMail avec WorkSpaces, créez un répertoire compatible en suivant les étapes ci-dessous.

Pour ajouter un WorkSpaces répertoire compatible

1. Créez un répertoire compatible à l'aide de WorkSpaces. Pour obtenir WorkSpaces des instructions, consultez Get started with Amazon WorkSpaces Quick Setup dans le guide d' WorkSpaces administration Amazon.
2. Dans la WorkMail console Amazon, créez votre WorkMail organisation Amazon et choisissez d'utiliser votre répertoire existant à cette fin. Pour de plus amples informations, veuillez consulter Création d'une organisation.

États des organisations et descriptions

Une fois une organisation créée, son état peut être l'un des suivants.

État	Description
Actif	Votre organisation est saine et prête à être utilisée.
Création	Un flux de travail est en cours d'exécution pour créer votre organisation.
Échec	Votre organisation n'a pas pu être créée.
Dégradé	Votre organisation fonctionne mal ou un problème a été détecté.
Inactif	Votre organisation est inactive.
Demandé	Votre demande de création d'organisation est dans la file d'attente et en attente d'être créée.
Validation en cours	L'état de tous les paramètres de l'organisation est en train d'être vérifié.

Suppression d'une organisation

Si vous ne souhaitez plus utiliser Amazon WorkMail pour les e-mails de votre organisation, vous pouvez supprimer votre organisation d'Amazon WorkMail.

> **Note**
>
> Cette opération ne peut pas être annulée. Vous ne pourrez pas récupérer les données de votre boîte aux lettres après la suppression d'une organisation.

Pour supprimer une organisation

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Sur l'écran Organisations, dans la liste des organisations, sélectionnez l'organisation à supprimer et choisissez Supprimer.
3. Pour Supprimer l'organisation, choisissez de supprimer ou de conserver l'annuaire des utilisateurs existant, puis entrez le nom de l'organisation.
4. Choisissez Supprimer l'organisation.

> **Note**
>
> Si vous n'avez pas fourni votre propre répertoire pour Amazon WorkMail, nous en créerons un pour vous. Si vous conservez ce répertoire existant lorsque vous supprimez l'organisation, il vous sera facturé, sauf s'il est utilisé par Amazon WorkMail WorkDocs, ou WorkSpaces. Pour de plus amples informations sur la tarification, veuillez consulter la tarification des autres types d'annuaires.
> Pour supprimer le répertoire, aucune autre AWS application ne doit être activée. Pour plus d'informations, consultez la section Suppression d'un annuaire Simple AD ou Suppression d'un répertoire AD Connector dans le Guide d'AWS Directory Serviceadministration.

Vous pouvez recevoir un message d'erreur non valide relatif à l'ensemble de règles Amazon Simple Email Service (Amazon SES) lorsque vous tentez de supprimer une organisation. Si vous recevez cette erreur, modifiez la règle Amazon SES dans la console Amazon SES et supprimez l'ensemble de règles non valide. Le nom de la règle que vous modifiez doit contenir votre identifiant d' WorkMailorganisation Amazon. Pour plus d'informations sur la modification des règles Amazon SES, consultez la section Création de règles de réception dans le manuel Amazon Simple Email Service Developer Guide.

Si vous devez déterminer quel ensemble de règles n'est pas valide, enregistrez d'abord la règle. Un message d'erreur s'affiche pour l'ensemble de règles.

Trouver une adresse e-mail

Vous pouvez savoir si une adresse e-mail est utilisée dans votre organisation par utilisateur, ressource ou groupe.

Pour trouver une adresse e-mail

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom d'une organisation.
3. Sur la page Organisation, choisissez Rechercher une adresse e-mail.
4. Choisissez Rechercher.

Utilisation des paramètres de l'organisation

Les sections suivantes expliquent comment utiliser les paramètres disponibles pour les WorkMail organisations Amazon. Les paramètres que vous choisissez s'appliqueront à l'ensemble de l'organisation.

Rubriques

- Activer la migration des boîtes aux lettres
- Activation de la journalisation

- Permettre l'interopérabilité
- Activation des passerelles SMTP
- Gestion des flux de messagerie
- Application de stratégies DMARC sur les e-mails entrants

Activer la migration des boîtes aux lettres

Vous activez la migration de boîtes aux lettres lorsque vous souhaitez transférer des boîtes aux lettres d'une source, telle que Microsoft Exchange ou G Suite Basic, vers Amazon WorkMail. Vous activez la migration dans le cadre d'un processus de migration plus vaste. Pour plus d'informations, y compris les étapes à suivre, consultez la section Mise Migration vers Amazon WorkMail en route de ce guide.

Activation de la journalisation

Vous activez la journalisation pour enregistrer vos communications par e-mail. Lorsque vous utilisez la journalisation, vous utilisez généralement des outils tiers intégrés d'archivage et d'eDiscovery. La journalisation permet de garantir que vous respectez les réglementations de conformité en matière de stockage des données, de protection de la confidentialité et de protection des informations.

Pour plus d'informations, y compris les étapes à suivre, consultez la section Mise Utilisation de la journalisation des e-mails avec Amazon WorkMail en route de ce guide.

Permettre l'interopérabilité

L'interopérabilité vous permet de migrer depuis Microsoft Exchange et d'utiliser Amazon WorkMail comme sous-ensemble de vos boîtes aux lettres d'entreprise. Pour plus d'informations, y compris les étapes à suivre, consultez la section Mise Configurer les paramètres de disponibilité sur Amazon WorkMail en route de ce guide.

Activation des passerelles SMTP

Vous activez les passerelles SMTP (Simple Mail Transfer Protocol) à utiliser avec les règles de flux de courrier sortant. Les règles de flux d'e-mails sortants vous permettent d'acheminer les e-mails envoyés par votre WorkMail organisation Amazon via une passerelle SMTP. Pour de plus amples informations, veuillez consulter Actions de règle pour les e-mails sortants.

> **Note**
>
> Les passerelles SMTP configurées pour les règles de flux de courrier sortant doivent prendre en charge le protocole TLS (Transport Layer Security) v1.2 à l'aide de certificats émis par les principales autorités de certification. Seule l'authentification de base est prise en charge.

Pour configurer une passerelle SMTP

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom d'une organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).

   La page des paramètres de l'organisation apparaît et contient un ensemble d'onglets.
4. Choisissez l'onglet Passerelles SMTP, puis sélectionnez Créer une passerelle.
5. Saisissez :

   - Nom de la passerelle — Entrez un nom unique.
   - Adresse de la passerelle : entrez le nom d'hôte ou l'adresse IP de la passerelle.
   - Numéro de port — Entrez le numéro de port de la passerelle.
   - Nom d'utilisateur — Entrez un nom d'utilisateur.
   - Mot de passe — Entrez un mot de passe sécurisé.
6. Choisissez Créer.

   La passerelle SMTP est disponible pour une utilisation avec les règles de flux de messagerie sortant.

Lorsque vous configurez une passerelle SMTP pour une utilisation avec une règle de flux de courrier sortant, les messages sortants tentent de faire correspondre la règle à une passerelle SMTP. Le message correspondant à la règle est acheminé vers la passerelle SMTP correspondante, qui gère ensuite le reste de la livraison du courrier électronique.

Si Amazon WorkMail ne parvient pas à atteindre la passerelle SMTP, le système renvoie le message électronique à l'expéditeur. Dans ce cas, suivez les étapes précédentes pour corriger les paramètres de la passerelle.

Gestion des flux de messagerie

Pour faciliter la gestion des e-mails, vous pouvez configurer des règles de flux d'e-mails. Les règles de flux de messagerie peuvent effectuer une ou plusieurs actions sur les messages électroniques en fonction de leurs adresses ou de leurs domaines. Vous pouvez utiliser des règles de flux d'e-mails sur les adresses e-mail ou les domaines des expéditeurs et des destinataires.

Lorsque vous créez une règle de flux de courrier électronique, vous spécifiez une action de règle qui s'applique à un e-mail lorsqu'un modèle de règle spécifié correspond.

Rubriques

Actions de règle pour les e-mails entrants

Les règles de flux de messagerie entrant empêchent les messages indésirables d'atteindre les boîtes aux lettres de vos utilisateurs. Les règles relatives au flux d'e-mails entrants, également appelées actions de règles, s'appliquent automatiquement à tous les e-mails envoyés à un membre de votre WorkMail organisation Amazon. Elles diffèrent des règles de messagerie pour les boîtes aux lettres individuelles.

> **Note**
>
> Vous pouvez éventuellement utiliser des règles dotées d'une AWS Lambda fonction pour traiter les e-mails entrants avant qu'ils ne soient envoyés aux boîtes aux lettres de vos

utilisateurs. Pour plus d'informations sur l'utilisation de Lambda avec Amazon WorkMail, consultez. Configuration AWS Lambda pour Amazon WorkMail Pour plus d'informations sur Lambda, consultez le guide du développeur AWS Lambda.

Les règles relatives au flux d'e-mails entrants, également appelées actions de règles, s'appliquent automatiquement à tous les e-mails envoyés à un membre de l' WorkMail organisation Amazon. Elles diffèrent des règles de messagerie pour les boîtes aux lettres individuelles.

Les actions de règle suivantes définissent la façon dont les messages entrants sont traités. Pour chaque règle, vous spécifiez des modèles d'expéditeur et de destinataire, accompagnés de l'une des actions suivantes.

Action	Description
Drop email (Ignorer l'e-mail)	Le message électronique est ignoré. Il n'est pas remis et l'expéditeur n'est pas averti de sa non-remise.
Send bounce response (Envoyer une réponse de retour à l'expéditeur)	Le message électronique n'est pas remis et l'expéditeur est informé de la non-livraison dans un message de rebond.
Deliver to junk folder (Placer dans le dossier Courrier indésirable)	Le message électronique est envoyé dans les dossiers de spam ou de courrier indésirable des utilisateurs, même s'il n'a pas été initialem ent identifié comme spam par le système de détection du WorkMail spam Amazon.
Par défaut	L'e-mail est livré après avoir été vérifié par le système de détection de WorkMail spam Amazon. Le message indésirable est placé dans le dossier Courrier indésirable. Tous les autres e-mails sont envoyés dans la boîte de réception. Les autres règles de flux de messagerie avec un modèle d'expéditeur moins spécifique sont

Action	Description
	ignorées. Pour ajouter des exceptions à des règles de flux de messagerie basées sur des domaines, configurez l'action par défaut avec un modèle d'expéditeur plus spécifique. Pour de plus amples informations, veuillez consulter Modèles d'expéditeur et de destinataire.
Never deliver to junk folder (Ne jamais placer dans le dossier Courrier indésirable)	Le message électronique est toujours envoyé dans les boîtes de réception des utilisate urs, même s'il est identifié comme spam par le système de détection de WorkMail spam Amazon. **Important** En n'utilisant pas le système de détection de courrier indésirable par défaut, vous pouvez exposer vos utilisateur à du contenu présentant des risques élevés provenant des adresses que vous spécifiez.
Courir AWS Lambda	Transmet le message électronique à une fonction Lambda pour traitement avant ou pendant son envoi dans les boîtes de réception des utilisateurs.

Note

Les e-mails entrants sont d'abord envoyés à Amazon SES, puis à Amazon WorkMail. Si Amazon SES bloque un e-mail entrant, les actions des règles ne s'appliqueront pas. Par exemple, Amazon SES bloque un e-mail lorsqu'un virus connu est détecté ou en raison de règles de filtrage IP explicites. La spécification d'une action de règle comme Default (Par

défaut), Deliver to junk folder (Placer dans le dossier Courrier indésirable) ou Never deliver to junk folder (Ne jamais placer dans le dossier Courrier indésirable) n'a aucun effet.

Actions de règle pour les e-mails sortants

Vous utilisez les règles de flux de courrier sortant pour diriger les e-mails via des passerelles SMTP ou pour empêcher les expéditeurs d'envoyer des e-mails à des destinataires spécifiques. Pour plus d'informations sur les passerelles SMTP, consultez. Activation des passerelles SMTP

Vous pouvez également utiliser les règles de flux de courrier sortant pour transmettre le message électronique à une AWS Lambda fonction qui le traitera après son envoi. Pour plus d'informations sur Lambda, consultez le guide du développeur AWS Lambda.

Les actions de règle suivantes définissent la façon dont les messages sortants sont traités. Pour chaque règle, vous spécifiez des modèles d'expéditeur et de destinataire, accompagnés de l'une des actions suivantes.

Action	Description
Par défaut	Le message électronique est envoyé via le flux normal.
Drop email (Ignorer l'e-mail)	Le message électronique est supprimé. Il n'est pas envoyé et l'expéditeur n'est pas averti.
Send bounce response (Envoyer une réponse de retour à l'expéditeur)	Le message électronique n'est pas envoyé et l'expéditeur est averti par un message indiquant que l'administrateur a bloqué le message électronique.
Route to SMTP gateway (Acheminer vers la passerelle SMTP)	Le message électronique est envoyé via une passerelle SMTP configurée.
Exécutez Lambda	Transmet le message électronique à une fonction Lambda pour traitement avant ou pendant l'envoi du message électronique.

Modèles d'expéditeur et de destinataire

Une règle de flux de messagerie peut s'appliquer à une adresse particulière ou à toutes les adresses d'un domaine ou d'un ensemble de domaines donné. Vous définissez un modèle afin de déterminer les adresses e-mail auxquelles une règle s'applique.

Les modèles d'expéditeur et de destinataire ont l'une des formes suivantes :

- Une adresse e-mail correspond à une adresse e-mail unique ; par exemple :

```
mailbox@example.com
```

- Un nom de domaine correspond à toutes les adresses e-mail de ce domaine ; par exemple :

```
example.com
```

- Un domaine générique correspond à toutes les adresses e-mail de ce domaine et de tous ses sous-domaines. Un caractère générique apparaît uniquement avant un domaine, par exemple :

```
*.example.com
```

- Une étoile correspond à n'importe quelle adresse e-mail de n'importe quel domaine.

```
*
```

> **Note**
>
> Le symbole + n'est pas valide dans les modèles d'expéditeur ou de destinataire.

Vous pouvez préciser plusieurs modèles pour une même règle. Pour plus d'informations, consultez Actions de règle pour les e-mails entrants et Actions de règle pour les e-mails sortants.

Les règles de flux de courrier entrant sont appliquées si l'`From`en-tête `Sender` ou l'en-tête d'un e-mail entrant correspond à un modèle quelconque. Si elle est présente, l'adresse `Sender` est mise en correspondance d'abord. L'adresse `From` est mise en correspondance si aucun en-tête `Sender` n'est présent ou si celui-ci ne `Sender` correspond à aucune règle. Si plusieurs destinataires du message électronique répondent à des règles différentes, chaque règle s'applique aux destinataires correspondants.

Les règles de flux de courrier sortant sont appliquées si le destinataire et l'`From`en-tête `Sender` ou l'en-tête d'un e-mail sortant correspondent à un modèle quelconque. Si plusieurs destinataires du message électronique répondent à des règles différentes, chaque règle s'applique aux destinataires correspondants.

Si plusieurs règles correspondent, l'action de la règle la plus spécifique est appliquée. Par exemple, une règle pour une adresse e-mail précise prévaut sur une règle concernant un domaine complet. Si plusieurs règles ont la même spécificité, l'action la plus restrictive est appliquée. Par exemple, une action Drop a priorité sur une action Bounce. L'ordre de priorité des actions est le même que l'ordre dans lequel elles sont répertoriées dans Actions de règle pour les e-mails entrants et Actions de règle pour les e-mails sortants.

> **Note**
>
> Soyez vigilant lorsque vous créez des règles comportant des modèles d'expéditeurs superposés avec des actions Drop ou Bounce. Un ordre de priorité inattendu peut empêcher la livraison de nombreux e-mails entrants.

Création de règles de flux d'e-mails

Les règles de flux de courrier électronique appliquent des actions de règles aux e-mails entrants et sortants. Les actions s'appliquent lorsque les messages correspondent à un modèle spécifié. Les nouvelles règles de flux d'e-mails entrent en vigueur immédiatement.

Pour créer des règles de flux d'e-mails

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom d'une organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).

   La page des paramètres de l'organisation apparaît et contient un ensemble d'onglets. À partir de cette page, vous pouvez créer des règles entrantes ou sortantes. Les étapes suivantes expliquent comment créer les deux types.

Pour créer des règles de trafic entrant

1. Cliquez sur l'onglet Règles de trafic entrant, puis sur Créer.
2. Dans le champ Nom de la règle, entrez un nom unique.
3. Sous Action, ouvrez la liste et sélectionnez une action. Chaque élément de la liste contient une description, et certains contiennent des liens pour en savoir plus.

> **Note**
>
> Si vous choisissez l'action Exécuter Lambda, des commandes supplémentaires apparaissent : pour plus d'informations sur l'utilisation de ces commandes, reportez-vous à la section suivante,. Configuration AWS Lambda pour Amazon WorkMail

4. Sous Domaines ou adresses de l'expéditeur, entrez les domaines ou adresses de l'expéditeur auxquels vous souhaitez que la règle s'applique.
5. Sous Domaines ou adresses de destination, entrez n'importe quelle combinaison de domaines de destination et d'adresses e-mail.
6. Choisissez Créer.

Pour créer des règles de sortie

1. Cliquez sur l'onglet Règles sortantes, puis sur Créer.
2. Dans le champ Nom de la règle, entrez un nom unique.
3. Sous Action, ouvrez la liste et sélectionnez une action. Chaque élément de la liste contient une description, et certains contiennent des liens pour en savoir plus.

> **Note**
>
> Si vous choisissez l'action Exécuter Lambda, des commandes supplémentaires apparaissent. Pour plus d'informations sur l'utilisation de ces commandes, reportez-vous à la section suivante,Configuration AWS Lambda pour Amazon WorkMail.

4. Sous Domaines ou adresses de l'expéditeur, entrez n'importe quelle combinaison de domaines d'expéditeur et d'adresses e-mail valides.
5. Sous Domaines ou adresses de destination, entrez n'importe quelle combinaison de domaines de destination et d'adresses e-mail valides.

6. Choisissez Créer.

   Vous pouvez tester la nouvelle règle de flux de messagerie que vous avez créée. Pour de plus amples informations, veuillez consulter Test d'une règle de flux de messagerie.

Modification des règles de flux d'e-mails

Vous modifiez les règles de flux d'e-mails chaque fois que vous devez modifier une ou plusieurs actions de règles pour les messages électroniques. Les étapes décrites dans cette section s'appliquent aux e-mails entrants et sortants.

Pour modifier les règles de flux d'e-mails

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom d'une organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation).

   La page des paramètres de l'organisation apparaît et contient un ensemble d'onglets.
4. Choisissez les onglets Règles entrantes ou Règles sortantes.
5. Cliquez sur le bouton radio situé à côté de la règle que vous souhaitez modifier, puis sélectionnez Modifier.
6. Modifiez l'action ou les actions de la règle selon vos besoins, puis choisissez Enregistrer.

Configuration AWS Lambda pour Amazon WorkMail

Utilisez l'action Exécuter Lambda dans les règles de flux de courrier entrant et sortant pour transmettre les messages électroniques conformes aux règles à une AWS Lambda fonction à des fins de traitement.

Choisissez parmi les configurations suivantes pour une action Run Lambda dans Amazon. WorkMail

Configuration Lambda d'exécution synchrone

Les messages électroniques qui correspondent à la règle de flux sont transmis à une fonction Lambda pour traitement avant d'être envoyés ou remis. Utilisez cette configuration pour modifier le contenu des e-mails. Vous pouvez également contrôler le flux de courrier entrant ou sortant pour différents cas d'utilisation. Par exemple, une règle transmise à une fonction Lambda peut bloquer la livraison de messages électroniques sensibles, supprimer des pièces jointes ou ajouter des clauses de non-responsabilité.

Configuration d'exécution asynchrone de Lambda

Les messages électroniques qui correspondent à la règle de flux sont transmis à une fonction Lambda pour être traités lors de leur envoi ou de leur remise. Cette configuration n'affecte pas la livraison des e-mails, et est utilisée lors de tâches telles que la collecte de métriques pour les messages électroniques entrants ou sortants.

Que vous choisissiez une configuration synchrone ou asynchrone, l'objet d'événement transmis à votre fonction Lambda contient les métadonnées de l'événement d'e-mail entrant ou sortant. Vous pouvez également accéder au contenu complet du message électronique grâce à l'ID de message dans les métadonnées. Pour de plus amples informations, veuillez consulter Récupération de contenu des messages avec AWS Lambda. Pour de plus amples informations sur les événements d'e-mails, veuillez consulter Données d'événements Lambda.

Pour plus d'informations sur les règles de flux de messagerie entrant et sortant, consultez Gestion des flux de messagerie. Pour plus d'informations sur Lambda, consultez le guide du développeur AWS Lambda.

> **Note**
>
> Actuellement, les règles de flux de messagerie Lambda font uniquement référence aux fonctions Lambda dans la même région AWS et dans la même organisation Amazon WorkMail en cours Compte AWS de configuration.

Commencer à utiliser AWS Lambda pour Amazon WorkMail

Pour commencer à utiliser AWS Lambda Amazon WorkMail, nous vous recommandons de déployer la fonction WorkMail Hello World Lambda depuis votre AWS Serverless Application Repository compte. La fonction dispose de toutes les ressources nécessaires et des autorisations configurées

pour vous. Pour plus d'exemples, consultez le amazon-workmail-lambda-templatesréférentiel sur GitHub.

Si vous choisissez de créer votre propre fonction Lambda, vous devez configurer les autorisations à l'aide de AWS Command Line Interface ()AWS CLI. Dans l'exemple de commande suivant, procédez comme suit :

- Remplacez `MY_FUNCTION_NAME` par le nom de votre fonction Lambda.
- `REGION`Remplacez-le par votre région Amazon WorkMail AWS. Les WorkMail régions Amazon disponibles incluent `us-east-1` (USA Est (Virginie du Nord)), `us-west-2` (USA Ouest (Oregon)) et `eu-west-1` (Europe (Irlande)).
- `AWS_ACCOUNT_ID`Remplacez-le par votre Compte AWS identifiant à 12 chiffres.
- `WORKMAIL_ORGANIZATION_ID`Remplacez-le par votre identifiant d' WorkMailorganisation Amazon. Vous le trouverez sur la carte de votre organisation sur la page Organizations.

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal workmail.REGION.amazonaws.com
--source-arn
 arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

Pour plus d'informations sur l'utilisation duAWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Configuration des règles Run Lambda synchrones

Pour configurer une règle d'exécution Lambda synchrone, créez une règle de flux de courrier électronique avec l'action Exécuter Lambda et cochez la case Exécuter de manière synchrone. Pour plus d'informations sur la création de règles de flux d'e-mails, veuillez consulter Création de règles de flux d'e-mails.

Pour terminer la création de la règle synchrone, ajoutez le nom de ressource Lambda Amazon (ARN) et configurez les options suivantes.

Action de secours

L'action Amazon WorkMail s'applique si la fonction Lambda ne s'exécute pas. Cette action s'applique également à tous les destinataires omis dans la réponse Lambda si l'indicateur AllRecipients n'est pas défini. L'action Fallback ne peut pas être une autre action Lambda.

Temps d'expiration de la règle (en minutes)

Période pendant laquelle la fonction Lambda est réessayée si Amazon WorkMail ne parvient pas à l'invoquer. L'action de secours est utilisée à la fin de cette période.

> **Note**
>
> Les règles Synchrous Run Lambda ne prennent en charge que * la condition de destination.

Données d'événements Lambda

La fonction Lambda est déclenchée à l'aide des données d'événement suivantes. La présentation des données varie en fonction du langage de programmation utilisé pour la fonction Lambda.

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

L'événement JSON comprend les données suivantes.

summaryVersion

Le numéro de version de`LambdaEventData`. Cela n'est mis à jour que lorsque vous apportez une modification rétrocompatible dans`LambdaEventData`.

envelope

L'enveloppe du message électronique, qui comprend les éléments suivants : champs.

mailFrom

L'adresse From (d'expédition), généralement l'adresse e-mail de l'utilisateur ayant envoyé le message. Si l'utilisateur a envoyé l'e-mail au nom d'une autre personne ou en tant qu'un autre utilisateur, le champ mailFrom renvoie l'adresse e-mail de l'utilisateur au nom de qui le message a été envoyé, et non celle de l'émetteur réel.

recipients

Liste de toutes les adresses e-mail des destinataires Amazon WorkMail ne fait pas de distinction entre To, CC ou BCC.

> **Note**
>
> En ce qui concerne les règles relatives au flux d'e-mails entrants, cette liste inclut les destinataires de tous les domaines de WorkMail l'organisation Amazon dans laquelle vous créez la règle. La fonction Lambda est invoquée séparément pour chaque conversation SMTP par l'expéditeur, et le champ des destinataires répertorie les destinataires de cette conversation SMTP. Les destinataires avec des domaines externes ne sont pas inclus.

sender

Adresse e-mail de l'utilisateur qui a envoyé l'e-mail au nom d'un autre utilisateur. Ce champ est défini uniquement lorsqu'un e-mail est envoyé au nom d'un autre utilisateur.

subject

Ligne d'objet de l'e-mail. Tronquée lorsqu'elle dépasse la limite de 256 caractères.

messageId

Un identifiant unique utilisé pour accéder au contenu complet du message électronique lors de l'utilisation du SDK Amazon WorkMail Message Flow.

invocationId

L'ID d'un appel Lambda unique. Cet identifiant reste le même lorsqu'une fonction Lambda est appelée plusieurs fois pour la même fonction. LambdaEventData Permet de détecter les nouvelles tentatives et éviter la duplication.

flowDirection

Indique la direction du flux de messagerie, soit INBOUND (ENTRANT) ou OUTBOUND (SORTANT).

truncated

S'applique à la charge utile, non à la longueur de la ligne d'objet. Lorsque la valeur est `true`, la taille de la charge utile dépasse la limite de 128 Ko. La liste des destinataires est donc tronquée pour respecter la limite.

Schéma de réponse Synchrous Run Lambda

Lorsqu'une règle de flux d'e-mails comportant une action Run Lambda synchrone correspond à un e-mail entrant ou sortant, Amazon WorkMail appelle la fonction Lambda configurée et attend la réponse avant d'agir sur le message électronique. La fonction Lambda renvoie une réponse selon un schéma prédéfini qui répertorie les actions, les types d'actions, les paramètres applicables et les destinataires auxquels l'action s'applique.

L'exemple suivant montre une réponse Run Lambda synchrone. Les réponses varient en fonction du langage de programmation utilisé pour la fonction Lambda.

```
{
    "actions": [
      {
        "action" : {
          "type": "string",
          "parameters": { various }
        },
        "recipients": [list of strings],
        "allRecipients": boolean
      }
```

```
    ]
}
```

La réponse JSON inclut les données suivantes :

action

L'action à entreprendre pour les destinataires.

type

Le type d'action. Les types d'action ne sont pas renvoyés pour les actions Run Lambda asynchrones.

Les types d'action de messages entrants incluent BOUNCE (RETOUR À L'EXPÉDITEUR), DROP (IGNORER), DEFAULT (PAR DÉFAUT), BYPASS_SPAM_CHECK (ÉVITER_VÉRIFICATION_ANTI-SPAM), et MOVE_TO_JUNK (DÉPLACER_VERS_COURRIER_INDÉSIRABLE). Pour de plus amples informations, veuillez consulter Actions de règle pour les e-mails entrants.

Les types d'action de messages sortants incluent BOUNCE (RETOUR À L'EXPÉDITEUR), DROP (IGNORER), et DEFAULT (PAR DÉFAUT). Pour de plus amples informations, veuillez consulter Actions de règle pour les e-mails sortants.

parameters

Paramètres d'action supplémentaires. Compatibles avec les types d'action BOUNCE (RETOUR À L'EXPÉDITEUR) en tant qu'objet JSON avec la clé bounceMessage et la chaînede valeur. L'option de message de retour à l'expéditeur est utilisée pour créer un e-mail revenant à l'expéditeur.

recipients

Liste des adresses e-mail concernées par l'action. Vous pouvez ajouter de nouveaux destinataires à la réponse, même s'ils n'étaient pas inclus dans la liste initiale. Ce champ n'est pas obligatoire si allRecipients est activé pour une action.

> **Note**
>
> Lorsqu'une action Lambda est appelée pour un e-mail entrant, vous ne pouvez ajouter que de nouveaux destinataires issus de votre organisation. Les nouveaux destinataires ajoutés à la réponse apparaissent dans le champ BCC (Cci).

allRecipients

Lorsque vrai, applique l'action à tous les destinataires qui ne sont pas soumis à une autre action spécifique dans la réponse Lambda.

Limites d'action Synchrous Run Lambda

Les limites suivantes s'appliquent lorsqu'Amazon WorkMail invoque des fonctions Lambda pour des actions Run Lambda synchrones :

- Les fonctions Lambda doivent répondre dans les 15 secondes, sous peine d'être considérées comme des appels ayant échoué.

> **Note**
>
> Le système tente à nouveau l'appel pendant l'intervalle de délai d'expiration des règles que vous spécifiez.

- Les réponses de la fonction Lambda jusqu'à 256 Ko sont autorisées.
- Jusqu'à 10 actions différentes sont autorisées pour la réponse. S'il y en a plus de 10, elles seront soumises à l'action de secourspréalablement configurée.
- Jusqu'à 500 destinataires sont autorisés pour les fonctions Lambda sortantes.
- La valeur maximale du temps d'expiration de la règle est de 240 minutes. Si la valeur minimale de 0 est configurée, il n'y a aucune nouvelle tentative avant qu'Amazon n' WorkMail applique l'action de secours.

Défaillances de l'action Synchrone Run Lambda

Si Amazon ne WorkMail parvient pas à appeler votre fonction Lambda en raison d'une erreur, d'une réponse non valide ou d'un délai Lambda expiré, Amazon WorkMail tente à nouveau l'appel avec un retard exponentiel qui réduit le taux de traitement jusqu'à la fin du délai d'expiration de la règle. Ensuite, l'action de secours est appliquée à tous les destinataires de l'e-mail. Pour de plus amples informations, veuillez consulter Configuration des règles Run Lambda synchrones.

Exemple de réponses Run Lambda synchrones

Les exemples suivants illustrent la structure des réponses Run Lambda synchrones courantes.

Example : supprime certains destinataires précis d'un e-mail

L'exemple suivant illustre la structure d'une réponse synchrone Run Lambda pour supprimer des destinataires d'un message électronique.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      },
      {
        "action": {
          "type": "DROP"
        },
        "recipients": [
          "drop-recipient@example.com"
        ]
      }
    ]
}
```

Example : Renvoyer un e-mail personnalisé à l'expéditeur

L'exemple suivant illustre la structure d'une réponse synchrone Run Lambda destinée à être renvoyée à un e-mail personnalisé.

```
{
    "actions" : [
      {
        "action" : {
          "type": 'BOUNCE',
          "parameters": {
            "bounceMessage" : "Email in breach of company policy."
          }
        },
        "allRecipients": true
      }
    ]
}
```

Example : Ajouter des destinataires à un e-mail

L'exemple suivant illustre la structure d'une réponse synchrone Run Lambda pour ajouter des destinataires au message électronique. Cela ne met pas à jour les champs To (À) ou CC de l'e-mail.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "recipients": [
          "new-recipient@example.com"
         ]
      },
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      }
    ]
}
```

Pour plus d'exemples de code à utiliser lors de la création de fonctions Lambda pour les actions Run Lambda, consultez les modèles Amazon Lambda. WorkMail

Plus d'informations sur l'utilisation de Lambda avec Amazon WorkMail

Vous pouvez également accéder au contenu complet du message électronique qui déclenche la fonction Lambda. Pour de plus amples informations, veuillez consulter Récupération de contenu des messages avec AWS Lambda.

Récupération de contenu des messages avec AWS Lambda

Après avoir configuré une AWS Lambda fonction pour gérer les flux d'e-mails pour Amazon WorkMail, vous pouvez accéder au contenu complet des e-mails traités à l'aide de Lambda. Pour plus d'informations sur la prise en main de Lambda pour Amazon WorkMail, consultez. Configuration AWS Lambda pour Amazon WorkMail

Pour accéder au contenu complet des e-mails, utilisez l'`GetRawMessageContent`action dans l'API Amazon WorkMail Message Flow. L'ID du message électronique transmis à votre fonction Lambda

lors de l'invocation envoie une demande à l'API. Ensuite, l'API répond avec le contenu MIME complet du message électronique. Pour plus d'informations, consultez Amazon WorkMail Message Flow dans le manuel Amazon WorkMail API Reference.

L'exemple suivant montre comment une fonction Lambda utilisant l'environnement d'exécution Python peut récupérer le contenu complet du message.

> **Tip**
>
> Si vous commencez par déployer la fonction Lambda Amazon WorkMail Hello World depuis votre compte, le AWS Serverless Application Repository système crée une fonction Lambda dans votre compte avec toutes les ressources et autorisations nécessaires. Vous pouvez ensuite ajouter votre logique métier à la fonction lambda en fonction de votre cas d'utilisation.

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)

    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
    print(parsed_msg)
```

Pour des exemples plus détaillés de méthodes d'analyse du contenu des messages en transit, consultez le amazon-workmail-lambda-templatesréférentiel sur GitHub.

> **Note**
>
> Vous utilisez uniquement l'API Amazon WorkMail Message Flow pour accéder aux e-mails en transit. Vous ne pouvez accéder aux messages que dans les 24 heures suivant leur envoi ou leur réception. Pour accéder par programmation aux messages dans la boîte aux lettres d'un utilisateur, utilisez l'un des autres protocoles pris en charge par Amazon WorkMail, tels que IMAP ou Exchange Web Services (EWS).

Mise à jour du contenu des messages avec AWS Lambda

Après avoir configuré une AWS Lambda fonction synchrone pour gérer les flux d'e-mails, vous pouvez utiliser l'`PutRawMessageContent`action de l'API Amazon WorkMail Message flow pour mettre à jour le contenu des e-mails en transit. Pour plus d'informations sur la prise en main des fonctions Lambda pour Amazon WorkMail, consultez. Configuration des règles Run Lambda synchrones Pour plus d'informations sur l'API, consultez PutRawMessageContent.

> **Note**
>
> L' PutRawMessageContent API nécessite boto3 1.17.8, ou vous pouvez ajouter une couche à votre fonction Lambda. Pour télécharger la bonne version de boto3, consultez la page de démarrage sur. GitHub Pour plus d'informations sur l'ajout de couches, voir Configurer une fonction pour utiliser des couches.
> Voici un exemple de couche :`"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. Dans cet exemple, remplacez-le `${AWS::Region}` par une région aws appropriée, telle que us-east-1.

> **Tip**
>
> Si vous commencez par déployer la fonction Lambda Amazon WorkMail Hello World depuis AWS Serverless Application Repository sur votre compte, le système crée une fonction Lambda dans votre compte avec les ressources et autorisations nécessaires. Vous pouvez ensuite ajouter une logique métier à la fonction lambda, en fonction de vos cas d'utilisation.

Au fur et à mesure, souvenez-vous de ce qui suit :

- Utilisez l' GetRawMessageContentAPI pour récupérer le contenu du message d'origine. Pour de plus amples informations, veuillez consulter Récupération de contenu des messages avec AWS Lambda.
- Une fois que vous avez le message d'origine, modifiez le contenu MIME. Lorsque vous avez terminé, téléchargez le message dans un compartiment Amazon Simple Storage Service (Amazon S3) de votre compte. Assurez-vous que le compartiment S3 utilise la même chose Compte AWS que vos WorkMail opérations Amazon et qu'il utilise la même région AWS que vos appels d'API.

- Pour WorkMail qu'Amazon puisse traiter les demandes, votre compartiment S3 doit disposer de la politique appropriée afin d'accéder à l'objet S3. Pour de plus amples informations, veuillez consulter Example S3 policy.
- Utilisez l' PutRawMessageContentAPI pour renvoyer le contenu du message mis à jour à Amazon WorkMail.

> **Note**
>
> L'`PutRawMessageContent`API garantit que le contenu MIME du message mis à jour répond aux normes RFC, ainsi qu'aux critères mentionnés dans le type de RawMessageContentdonnées. Les e-mails envoyés à votre WorkMail organisation Amazon ne répondent pas toujours à ces normes. L'`PutRawMessageContent`API peut donc les rejeter. Dans ce cas, vous pouvez consulter le message d'erreur renvoyé pour plus d'informations sur la manière de résoudre les problèmes.

Example Exemple de politique S3

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "Bool": {
                    "aws:SecureTransport": "true"
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

L'exemple suivant montre comment une fonction Lambda utilise le moteur d'exécution Python pour mettre à jour l'objet d'un e-mail en transit.

```
    import boto3
    import os
    import uuid
    import email

    def email_handler(event, context):
        workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
        s3 = boto3.client('s3', region_name=os.environ["AWS_REGION"])

        msg_id = event['messageId']
        raw_msg = workmail.get_raw_message_content(messageId=msg_id)
        parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

        # Updating subject. For more examples, see https://github.com/aws-samples/
amazon-workmail-lambda-templates.
        parsed_msg.replace_header('Subject', "New Subject Updated From Lambda")

        # Store updated email in S3
        key = str(uuid.uuid4());
        s3.put_object(Body=parsed_msg.as_bytes(), Bucket="amzn-s3-demo-bucket",
 Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "amzn-s3-demo-bucket",
            'key': key
        }
```

```
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

Pour d'autres exemples de méthodes d'analyse du contenu des messages en transit, consultez le amazon-workmail-lambda-templatesréférentiel sur GitHub.

Gestion de l'accès à l'API Amazon WorkMail Message Flow

Utilisez des politiques Gestion des identités et des accès AWS (IAM) pour gérer l'accès à l'API Amazon WorkMail Message Flow.

L'API Amazon WorkMail Message Flow fonctionne avec un seul type de ressource, un e-mail en transit. Chaque e-mail en transit est associé à un Amazon Resource Name (ARN) unique.

L'exemple suivant montre la syntaxe d'un ARN associé à un message électronique en transit.

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

Les champs modifiables de l'exemple précédent sont les suivants :

- Région : région AWS de votre WorkMail organisation Amazon.
- Compte : Compte AWS identifiant de votre WorkMail organisation Amazon.
- Organisation : l'identifiant de votre WorkMail organisation Amazon.
- Contexte — Indique si le message est `incoming` destiné à votre organisation ou `outgoing` provient de celle-ci.
- ID du message : identifiant unique du message électronique transmis en entrée à votre fonction Lambda.

L'exemple suivant inclut un IDs exemple d'ARN associé à un e-mail entrant en transit.

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

Vous pouvez les utiliser ARNs comme ressources dans la `Resource` section de vos politiques utilisateur IAM afin de gérer l'accès aux WorkMail messages Amazon en transit.

Exemples de politiques IAM pour l'accès au flux de WorkMail messages Amazon

L'exemple de politique suivant accorde à une entité IAM un accès en lecture complet à tous les messages entrants et sortants pour chaque WorkMail organisation Amazon de votre entreprise. Compte AWS

Si vous avez plusieurs organisations dans votre entrepriseCompte AWS, vous pouvez également limiter l'accès à une ou plusieurs organisations. Cela est utile si certaines fonctions Lambda ne doivent être utilisées que pour certaines organisations.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/organization/*",
            "Effect": "Allow"
        }
    ]
}
```

Vous pouvez également choisir d'accorder l'accès aux messages selon qu'ils `incoming` à votre organisation ou `outgoing` partir de celle-ci. Pour ce faire, utilisez le qualificateur `incoming` ou `outgoing` dans l'ARN.

L'exemple de stratégie suivant accorde l'accès uniquement aux messages entrants dans votre organisation.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

L'exemple de politique suivant accorde à une entité IAM un accès complet en lecture et en mise à jour à tous les messages entrants et sortants pour chaque WorkMail organisation Amazon de votre entreprise. Comptes AWS

Test d'une règle de flux de messagerie

Pour vérifier votre configuration de règle actuelle, vous pouvez tester le comportement de la configuration avec des adresses spécifiques.

Pour tester une règle de flux de messagerie

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation), Inbound/Outbound rules (Règles entrantes/sortantes).
4. En regard de Test configuration (Tester la configuration), entrez les adresses e-mail complètes de l'expéditeur et du destinataire à tester.
5. Sélectionnez Tester). L'action à réaliser pour l'adresse fournie s'affiche.

Suppression d'une règle de flux de messagerie

Lorsque vous supprimez une règle de flux de messagerie, les changements sont appliqués sur-le-champ.

Pour supprimer une règle de flux de messagerie

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation), Inbound/Outbound rules (Règles entrantes/sortantes).
4. Sélectionnez la règle et choisissez Remove (Supprimer).
5. À l'invite de confirmation, choisissez Remove (Supprimer).

Application de stratégies DMARC sur les e-mails entrants

Les domaines de messagerie utilisent des enregistrements DNS (Domain Name System) pour des raisons de sécurité. Ils protègent vos utilisateurs contre les attaques courantes telles que l'usurpation d'identité ou le hameçonnage. Les enregistrements DNS incluent souvent des enregistrements DMARC (Domain-based Message Authentication, Reporting, Conformance), définis par le propriétaire du domaine qui envoie l'e-mail. Les enregistrements DMARC incluent des politiques qui spécifient les mesures à prendre lorsqu'un e-mail échoue à une vérification DMARC. Vous pouvez choisir d'appliquer la stratégie DMARC sur les e-mails envoyés à votre organisation.

L'application du DMARC est activée par défaut pour les nouvelles WorkMail organisations Amazon.

Pour activer l'application de DMARC

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Organization settings (Paramètres de l'organisation). La page des paramètres de l'organisation apparaît et contient un ensemble d'onglets.
4. Choisissez l'onglet DMARC, puis sélectionnez Modifier.
5. Déplacez le curseur d'application du DMARC sur la position activée.

6. Cochez la case à côté de Je reconnais que l'activation de l'application du DMARC peut entraîner la suppression ou la mise en quarantaine des e-mails entrants en fonction de la configuration du domaine de l'expéditeur.
7. Choisissez Enregistrer.

Pour désactiver l'application de DMARC

- Suivez les étapes de la section précédente, mais déplacez le curseur d'application de la DMARC sur la position Off.

Utilisation de la journalisation d'événements d'e-mail pour effectuer le suivi de l'application de DMARC

L'activation de l'application de DMARC peut entraîner la suppression d'e-mails entrants ou leur marquage comme courrier indésirable, selon la façon dont l'expéditeur a configuré son domaine. Si un expéditeur ne configure pas son domaine de messagerie, vos utilisateurs peuvent cesser de recevoir des e-mails légitimes. Pour vérifier les e-mails qui ne sont pas envoyés à vos utilisateurs, vous pouvez activer la journalisation des événements par e-mail pour votre WorkMail organisation Amazon. Ensuite, vous pouvez interroger vos journaux d'événements d'e-mail pour rechercher les e-mails entrants qui sont filtrés en fonction des stratégies DMARC de l'expéditeur.

Avant d'utiliser la journalisation des événements par e-mail pour suivre l'application du DMARC, activez la journalisation des événements par e-mail dans la WorkMail console Amazon. Pour tirer le meilleur parti de vos données de journal, laissez passer un certain temps pendant que les événements d'e-mail sont enregistrés. Pour en savoir plus et des instructions, consultez the section called “Activation de la journalisation des événements de messagerie”.

Pour utiliser la journalisation d'événements d'e-mail pour effectuer le suivi de l'application de DMARC

1. Dans la console CloudWatch Insights, sous Logs, sélectionnez Insights.
2. Pour Sélectionner un ou plusieurs groupes de journaux, sélectionnez le groupe de journaux de votre WorkMail organisation Amazon. Par exemple,/aws/workmail/events/organization-alias.
3. Sélectionnez une période à interroger.
4. Exécutez la requête suivante : stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Choisissez Exécuter la requête.

Vous pouvez également configurer des métriques personnalisées pour ces événements. Pour de plus amples informations, veuillez consulter Création de filtres de métriques.

Balisage d'une organisation

Le balisage d'une ressource d' WorkMail organisation Amazon vous permet de :

- Faites la différence entre les organisations dans la AWS Billing and Cost Management console.
- Contrôlez l'accès aux ressources de WorkMail l'organisation Amazon en les ajoutant à l'`Resource`élément des déclarations de politique d'autorisation Gestion des identités et des accès AWS (IAM).

Pour plus d'informations sur les autorisations WorkMail au niveau des ressources Amazon, consultez. Ressources Pour plus d'informations sur le contrôle d'accès basé sur des balises, veuillez consulter Autorisation basée sur les WorkMail tags Amazon.

WorkMail Les administrateurs Amazon peuvent étiqueter les organisations à l'aide de la WorkMail console Amazon.

Pour ajouter des tags à une WorkMail organisation Amazon

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Tags.
4. Dans Organization tags (Balises d’organisation), choisissez Add new tag (Ajouter une nouvelle balise).
5. Pour Key, entrez un nom identifiant le tag.
6. (Facultatif) Dans Value (Valeur), entrez une valeur pour la balise.
7. (Facultatif) Répétez les étapes 4 à 6 pour ajouter d'autres balises à votre organisation. Vous pouvez ajouter jusqu’à 50 balises.
8. Choisissez Save pour enregistrer les changements.

Vous pouvez consulter les tags de votre organisation dans la WorkMail console Amazon.

Les développeurs peuvent également étiqueter les organisations à l'aide du AWS SDK ou AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez les `UntagResource` commandes `TagResourceListTagsForResource`, et dans le manuel Amazon WorkMail API Reference ou le AWS CLICommand Reference.

Vous pouvez supprimer les tags d'une organisation à tout moment à l'aide de la WorkMail console Amazon.

Pour supprimer des tags d'une WorkMail organisation Amazon

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Tags.
4. Pour Organization tags (Balises d'organisation), choisissez Remove (Supprimer) en regard de la balise à supprimer.
5. Choisissez Soumettre pour enregistrer vos modifications.

Utilisation des règles de contrôle d'accès

Les règles de contrôle d'accès pour Amazon WorkMail permettent aux administrateurs de contrôler la manière dont les utilisateurs et les rôles d'usurpation d'identité de leur organisation obtiennent l'accès à Amazon. WorkMail Chaque WorkMail organisation Amazon dispose d'une règle de contrôle d'accès par défaut qui accorde l'accès aux boîtes aux lettres à tous les utilisateurs et aux rôles d'emprunt d'identité ajoutés à l'organisation, quels que soient le protocole d'accès ou l'adresse IP utilisés. Les administrateurs peuvent modifier ou remplacer la règle par défaut par l'une des leurs, ajouter une règle ou en supprimer une.

> **Warning**
>
> Si un administrateur supprime toutes les règles de contrôle d'accès d'une organisation, Amazon WorkMail bloque tout accès aux boîtes aux lettres de l'organisation.

Les administrateurs peuvent appliquer des règles de contrôle d'accès qui autorisent ou refusent l'accès en fonction des critères suivants :

- Protocoles : protocole utilisé pour accéder à la boîte aux lettres. Les exemples incluent Autodiscover, EWS, IMAP, SMTP ActiveSync, Outlook pour Windows et Webmail.
- Adresses IP : plages IPv4 CIDR utilisées pour accéder à la boîte aux lettres.
- WorkMail Utilisateurs Amazon : utilisateurs de votre organisation utilisés pour accéder à la boîte aux lettres.
- Rôles d'emprunt d'identité : rôles d'emprunt d'identité utilisés dans votre organisation pour accéder à la boîte aux lettres. Pour de plus amples informations, veuillez consulter Gestion des rôles d'usurpation d'identité.

Les administrateurs appliquent des règles de contrôle d'accès en plus des autorisations de boîte aux lettres et de dossier de l'utilisateur. Pour plus d'informations, consultez Gestion des autorisations d'accès à une boîte aux lettres la section Partage de dossiers et autorisations de dossiers dans le guide de WorkMail l'utilisateur Amazon.

> **Note**
>
> - Lorsque vous activez l'accès pour Outlook pour Windows, il est recommandé d'activer également l'accès pour Autodiscover et EWS.
> - Les règles de contrôle d'accès ne s'appliquent pas à l'accès à WorkMail la console Amazon ou au SDK. Utilisez plutôt des rôles ou des politiques Gestion des identités et des accès AWS (IAM). Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon WorkMail.

Création de règles de contrôle d'accès

Créez de nouvelles règles de contrôle d'accès depuis la WorkMail console Amazon.

Pour créer une règle de contrôle d'accès

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Access control rules (Règles de contrôle d'accès).
4. Choisissez Créer une règle.
5. Dans Description, entrez une description de la règle.
6. Dans Effect (Effet), choisissez Allow (Autoriser) ou Deny (Refuser). Cette option autorise ou refuse l'accès en fonction des conditions que vous sélectionnez à l'étape suivante.
7. Pour Cette règle s'applique aux demandes qui... , sélectionnez les conditions à appliquer à la règle, par exemple s'il faut inclure ou exclure des protocoles, des adresses IP ou des utilisateurs spécifiques, ou des rôles d'usurpation d'identité.
8. (Facultatif) Si vous entrez des plages d'adresses IP, des utilisateurs ou des rôles d'usurpation d'identité, choisissez Ajouter pour les ajouter à la règle.
9. Choisissez Créer une règle.

Modification des règles de contrôle d'accès

Modifiez les nouvelles règles de contrôle d'accès par défaut depuis la WorkMail console Amazon.

Pour modifier une règle de contrôle d'accès

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Access control rules (Règles de contrôle d'accès).
4. Sélectionnez la règle à modifier.
5. Choisissez Edit rule.
6. Modifiez la description, l'effet et les conditions, selon vos besoins.
7. Sélectionnez Enregistrer les modifications.

> **Important**
>
> Lorsque vous modifiez une règle d'accès, les boîtes aux lettres concernées peuvent mettre cinq minutes pour suivre la règle mise à jour. Les clients qui accèdent aux boîtes aux lettres concernées peuvent présenter un comportement incohérent pendant cette période. Cependant, vous constaterez immédiatement un comportement correct lorsque vous testerez vos règles. Pour plus d'informations sur les règles de test, consultez les étapes décrites dans la section suivante.

Test des règles de contrôle d'accès

Pour voir comment les règles de contrôle d'accès de votre organisation sont appliquées, testez-les depuis la WorkMail console Amazon.

Pour tester les règles de contrôle d'accès pour votre organisation

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Access control rules (Règles de contrôle d'accès).
4. Choisissez Test rules (Tester les règles).
5. Dans Request context (Contexte de la demande), sélectionnez le protocole à tester.
6. Dans Source IP address (Adresse IP source), entrez l'adresse IP à tester.
7. Pour Requête exécutée par, choisissez le rôle d'utilisateur ou d'usurpation d'identité à tester.
8. Sélectionnez le rôle d'utilisateur ou d'usurpation d'identité à tester.
9. Sélectionnez Tester).

Les résultats du test apparaissent sous Effect (Effet).

Suppression de règles de contrôle d'accès

Supprimez les règles de contrôle d'accès dont vous n'avez plus besoin dans la WorkMail console Amazon.

> **Warning**
>
> Si un administrateur supprime toutes les règles de contrôle d'accès d'une organisation, Amazon WorkMail bloque tout accès aux boîtes aux lettres de l'organisation.

Pour supprimer une règle de contrôle d’accès

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Access control rules (Règles de contrôle d'accès).
4. Sélectionnez la règle à supprimer.
5. Choisissez Delete rule (Supprimer la règle).
6. Sélectionnez Delete (Supprimer).

Définition des stratégies de rétention des boîtes aux lettres

Vous pouvez définir des politiques de conservation des boîtes aux lettres pour votre WorkMail organisation Amazon. Les politiques de rétention suppriment automatiquement les e-mails des boîtes aux lettres des utilisateurs après une période que vous avez choisie. Vous pouvez choisir les dossiers de boîtes aux lettres auxquels appliquer les politiques de rétention. Vous pouvez également choisir de définir des politiques de rétention différentes pour les différents dossiers. Les stratégies de rétention des boîtes aux lettres s'appliquent aux dossiers sélectionnés dans toutes les boîtes aux lettres utilisateur de votre organisation. Les utilisateurs ne peuvent pas annuler les politiques de rétention.

Pour définir une stratégie de rétention de boîte aux lettres

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Choisissez Retention policy (Stratégie de rétention).
4. Pour Folder actions (Actions de dossier), en regard de chaque dossier de boîte aux lettres que vous souhaitez inclure dans la stratégie, sélectionnez Supprimer ou Supprimer définitivement.
5. Entrez le nombre de jours pendant lesquels les e-mails doivent être conservés dans chaque dossier de boîte aux lettres avant de les supprimer.
6. Choisissez Enregistrer.

Prévoyez 48 heures pour appliquer les politiques de rétention de votre organisation. Si vous choisissez l'action Supprimer le dossier, les utilisateurs peuvent récupérer les e-mails supprimés depuis l'application WorkMail Web Amazon et les clients pris en charge. Si vous choisissez l'action Supprimer définitivement le dossier, les e-mails ne peuvent pas être récupérés après leur suppression.

Le nombre de jours pendant lesquels une politique de rétention conserve un article dépend de sa date de création, de modification ou de déplacement. Par exemple, si une politique de rétention supprime des éléments au bout d'un an, elle compte les jours de rétention à compter de la date de création ou de dernière action sur cet élément. Il n'est pas affecté par la date à laquelle vous avez mis en œuvre la politique de rétention.

Utilisation des domaines

Vous pouvez configurer Amazon WorkMail pour utiliser un domaine personnalisé. Vous pouvez également définir un domaine comme domaine par défaut pour votre organisation et l'activer AutoDiscover pour Microsoft Outlook.

Rubriques

Ajout d'un domaine

Vous pouvez ajouter jusqu'à 100 domaines à votre WorkMail organisation Amazon. Lorsque vous ajoutez un nouveau domaine, une politique d'autorisation d'envoi Amazon Simple Email Service (Amazon SES) est automatiquement ajoutée à la politique d'identité du domaine. Cela permet à Amazon WorkMail d'accéder à toutes les actions d'envoi d'Amazon SES pour votre domaine et vous permet de rediriger les e-mails vers votre domaine. Vous pouvez également rediriger les e-mails vers des domaines externes.

> **Note**
>
> Il est recommandé d'ajouter des alias pour `<postmaster@ et <abuse@>>` à tous vos domaines. Vous pouvez créer des groupes de distribution pour ces alias si vous souhaitez que des utilisateurs spécifiques de votre organisation reçoivent le courrier envoyé à ces alias.

Lorsque vous configurez votre WorkMail organisation Amazon avec un domaine personnalisé, n'oubliez pas les points suivants concernant les enregistrements DNS de votre domaine :

- Pour les enregistrements MX et CNAME de découverte automatique, nous recommandons de définir la valeur Time to Live (TTL) sur 3600. La réduction du TTL garantit que vos serveurs de messagerie n'utilisent pas d'enregistrements MX périmés ou non valides une fois que vous les avez mis à jour ou que vous avez migré vos boîtes aux lettres.
- Une fois que vous avez créé vos utilisateurs et vos groupes de distribution, puis que vous avez migré avec succès vos boîtes aux lettres, vous devez mettre à jour l'enregistrement MX pour commencer à transférer les e-mails vers Amazon WorkMail. Le traitement des mises à jour des enregistrements DNS peut prendre jusqu'à 48 heures.
- Certains fournisseurs de DNS ajoutent automatiquement des noms de domaine à la fin des enregistrements DNS. L'ajout d'un enregistrement qui contient déjà le nom de domaine, tel que _amazonses.example.com, peut entraîner la duplication du nom de domaine, avec pour résultat _amazonses.example.com.exemple.com. Pour éviter la duplication du nom de domaine dans le nom d'enregistrement, ajoutez un point à la fin du nom de domaine dans l'enregistrement DNS. Cela indique à votre fournisseur DNS que le nom de l'enregistrement est entièrement qualifié et qu'il ne correspond plus au nom de domaine. Cela empêche également le fournisseur DNS d'ajouter un nom de domaine supplémentaire.
- Les noms d'enregistrement copiés incluent le nom de domaine. En fonction du service DNS que vous utilisez, le nom de domaine peut être déjà ajouté à l'enregistrement DNS du domaine.
- Après avoir créé un enregistrement DNS, cliquez sur l'icône d'actualisation sur la WorkMail console Amazon pour voir le statut de vérification et la valeur de l'enregistrement. Pour plus d'informations sur la vérification des domaines, consultez Vérification des domaines.
- Nous vous recommandons de configurer votre domaine en tant que `MAIL FROM` domaine. Pour l'activer AutoDiscover pour les appareils iOS, vous devez configurer votre domaine en tant que `MAIL FROM` domaine. Vous pouvez consulter le statut de votre `MAIL FROM` domaine dans la section Améliorer la délivrabilité de la console. Pour de plus amples informations, veuillez consulter Configuration d'un domaine MAIL FROM personnalisé.

Pour ajouter un domaine

1. Connectez-vous à la WorkMail console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/workmail/.

2. Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation à laquelle vous souhaitez ajouter un domaine.
4. Dans le volet de navigation, sélectionnez Domaines, puis sélectionnez Ajouter un domaine.
5. Sur l'écran Ajouter un domaine, entrez un nom de domaine. Les noms de domaine ne peuvent contenir que des caractères latins de base (ASCII).

> **Note**
>
> Si votre domaine est géré dans une zone hébergée publique Amazon Route 53, vous pouvez le sélectionner dans le menu déroulant qui apparaît lorsque vous entrez un nom de domaine.

6. Choisissez Ajouter un domaine.

   Une page apparaît et répertorie les enregistrements DNS du nouveau domaine. La page regroupe les enregistrements dans les sections suivantes :

   - Propriété du domaine
   - WorkMail configuration
   - Sécurité améliorée
   - Livraison d'e-mails améliorée

   Chacune de ces sections contient un ou plusieurs enregistrements DNS, et chaque enregistrement affiche une valeur d'état. La liste suivante indique les enregistrements et leurs valeurs de statut disponibles.

   Propriété TXT

   Vérifié : enregistrement résolu et vérifié.

   En attente — L'enregistrement n'a pas encore été vérifié.

   Échec : impossible de vérifier la propriété. Enregistrement non apparié ou inaccessible.

WorkMail Configuration MX

Vérifié : enregistrement résolu et vérifié.

Manquant — Impossible de résoudre l'enregistrement.

Incohérent — La valeur ne correspond pas à l'enregistrement attendu.

AutoDiscover

Vérifié : enregistrement résolu et vérifié.

Manquant — Impossible de résoudre l'enregistrement.

Incohérent — La valeur ne correspond pas à l'enregistrement attendu.

> **Note**
>
> Le processus AutoDiscover de vérification permet également de vérifier que la AutoDiscover configuration est correcte. Le processus vérifie les paramètres de configuration pour chaque phase. Une coche verte apparaît à côté de Vérifié dans la colonne État lorsque la vérification est terminée. Vous pouvez passer le curseur sur Vérifié et voir laquelle des phases a été vérifiée par le processus. Pour plus d'informations sur les AutoDiscover phases, consultezActivation de AutoDiscover la configuration des points de terminaison.

DKIM CNAME

Vérifié : enregistrement résolu et vérifié.

En attente — L'enregistrement n'a pas encore été vérifié

Échec : impossible de vérifier la propriété. Enregistrement non apparié ou inaccessible.

Pour plus d'informations sur la signature DKIM, consultez Authentification des e-mails avec DKIM dans Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.

TEXTE SPF

Vérifié : enregistrement résolu et vérifié.

Manquant — Impossible de résoudre l'enregistrement.

Incohérent — La valeur ne correspond pas à l'enregistrement attendu.

Pour plus d'informations sur la vérification SPF, consultez Authentification d'e-mails avec SPF.

TEXTE DMARC

Vérifié : enregistrement résolu et vérifié.

Manquant — Impossible de résoudre l'enregistrement.

Incohérent — La valeur ne correspond pas à l'enregistrement attendu

Pour plus d'informations sur les enregistrements DMARC sur Amazon WorkMail, consultez la section Se conformer au DMARC à l'aide d'Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.

MESSAGE TXT PROVENANT D'UN DOMAINE

Vérifié : enregistrement résolu et vérifié.

En attente — L'enregistrement n'a pas encore été vérifié.

Échec : impossible de vérifier la propriété. Enregistrement non apparié ou inaccessible.

MX MAIL FROM domain

Vérifié : enregistrement résolu et vérifié.

Manquant — Impossible de résoudre l'enregistrement.

Incohérent — La valeur ne correspond pas à l'enregistrement attendu.

7. Pour l'étape suivante, choisissez l'action appropriée en fonction du fournisseur DNS que vous utilisez.

   Si vous utilisez un domaine Route 53

   - En haut de la page, choisissez Tout mettre à jour dans Route 53.

Si vous utilisez un autre fournisseur DNS

- Copiez les enregistrements et collez-les dans votre fournisseur DNS. Vous pouvez copier les enregistrements en bloc ou un par un. Pour copier des enregistrements en bloc, choisissez Copier tout. Cela crée une zone de fichiers que vous pouvez importer dans votre fournisseur DNS. Pour copier les enregistrements un par un, choisissez les carrés qui se chevauchent à côté du nom de l'enregistrement, puis collez-les dans votre fournisseur DNS.

8. Cliquez sur l'icône d'actualisation pour mettre à jour le statut de chaque enregistrement. Cela permet de vérifier la propriété du domaine et la bonne configuration de votre domaine auprès d'Amazon WorkMail.

Suppression d'un domaine

Vous pouvez supprimer un domaine lorsque vous n'en avez plus besoin. Toutefois, vous devez d'abord supprimer les individus ou les groupes qui utilisent le domaine comme adresse e-mail.

Pour supprimer un domaine

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Nom de la région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans la liste des domaines, cochez la case en regard du nom de domaine, puis choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer le domaine, entrez le nom du domaine à supprimer et choisissez Supprimer.

Choix du domaine par défaut

Vous pouvez définir un domaine associé à votre organisation comme domaine par défaut pour les utilisateurs et les groupes de cette organisation. Définir un domaine comme valeur par défaut ne modifie pas les adresses e-mail existantes.

Pour définir un domaine comme valeur par défaut

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Nom de la région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans la liste des domaines, cochez la case à côté du nom de domaine que vous souhaitez utiliser et choisissez Définir par défaut.

Vérification des domaines

Vous devez vérifier votre domaine après l'avoir ajouté dans la WorkMail console Amazon. La vérification du domaine confirme que vous êtes le propriétaire du domaine et que vous utiliserez Amazon WorkMail comme service de messagerie pour le domaine.

Vous vérifiez un domaine en y ajoutant des enregistrements TXT et MX dans votre service DNS. Les enregistrements TXT vous permettent d'ajouter des notes à votre service DNS. Les enregistrements MX spécifient le serveur de courrier entrant.

Vous utilisez la console Amazon SES pour créer les enregistrements TXT et MX, puis vous utilisez la WorkMail console Amazon pour ajouter les enregistrements à votre service DNS. Procédez comme suit :

Pour créer des enregistrements TXT et MX

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le volet de navigation, choisissez Domaines, puis sélectionnez Vérifier un nouveau domaine.

   La boîte de dialogue Vérifier un nouveau domaine apparaît.
3. Dans le champ Domaine, entrez le nom du domaine que vous avez créé dans la Ajout d'un domaine section.
4. (Facultatif) Si vous souhaitez utiliser le courrier DomainKeys identifié (DKIM), cochez la case Générer les paramètres DKIM.

5. Choisissez Verify This Domain.

   La console affiche une liste d'enregistrements TXT et MX.

6. Choisissez le lien Télécharger l'ensemble d'enregistrements au format CSV, situé sous la liste TXT.

   La boîte de dialogue Enregistrer sous apparaît. Choisissez un emplacement pour le téléchargement, puis cliquez sur Enregistrer.

7. Ouvrez le fichier CSV téléchargé et copiez tout son contenu.

Une fois que vous avez créé les enregistrements TXT et MX, vous les ajoutez à votre fournisseur DNS. Les étapes suivantes utilisent Route 53. Si vous utilisez un autre fournisseur DNS et que vous ne savez pas comment ajouter des enregistrements, consultez la documentation de votre fournisseur.

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Hosted Zones (Zones hébergées). Cliquez ensuite sur le bouton radio à côté du domaine que vous souhaitez vérifier.
3. Dans la liste des enregistrements DNS de votre domaine, sélectionnez Importer un fichier de zone.
4. Sous Fichier de zone, collez les enregistrements copiés dans la zone de texte. La liste des fichiers apparaît sous la zone de texte.
5. Faites défiler la liste jusqu'à la fin de la liste et choisissez Importer.

> **Note**
>
> Prévoyez jusqu'à 72 heures pour terminer le processus de vérification.

Vérification des enregistrements MX et TXT avec votre service DNS Records

Assurez-vous que l'enregistrement TXT qui vérifie que vous possédez le domaine est ajouté correctement à votre service DNS. Cette procédure utilise l'outil nslookup, disponible pour Windows et Linux. Sous Linux, vous pouvez également utiliser dig.

Pour utiliser l'`nslookup`outil, vous devez d'abord trouver les serveurs DNS qui desservent votre domaine. Ensuite, vous interrogez ces serveurs pour afficher les enregistrements TXT. Vous pouvez interroger les serveurs DNS de votre domaine, car ce sont eux qui contiennent le plus up-to-date d'informations sur votre domaine. La propagation de ces informations vers d'autres serveurs DNS peut prendre du temps.

Utilisez nslookup pour vérifier que votre enregistrement TXT est ajouté à votre service DNS

1. Trouvez les serveurs de noms de votre domaine :

   a. Ouvrez une invite de commande (Windows) ou un terminal (Linux).

   b. Exécutez la commande suivante pour répertorier tous les serveurs de noms qui desservent votre domaine. Remplacez *`example.com`* par votre domaine.

   ```
   nslookup -type=NS example.com
   ```

   Vous allez interroger l'un de ces serveurs de noms à l'étape suivante.

2. Vérifiez que l'enregistrement Amazon WorkMail TXT est correctement ajouté.

   a. Exécutez la commande suivante, en *`example.com`* remplaçant par votre domaine et *`ns1.name-server.net`* par un serveur de noms à partir de l'étape 1.

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. Vérifiez la `"text ="` chaîne affichée dans la sortie denslookup. Vérifiez que cette chaîne correspond à la valeur TXT de votre domaine dans la liste des expéditeurs vérifiés de la WorkMail console Amazon.

   Dans l'exemple suivant, vous souhaitez voir un enregistrement TXT pour _amazonses.example.com avec une valeur de. `fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=` Si vous mettez correctement à jour l'enregistrement, le résultat de la commande est le suivant :

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
   ```

Utilisez dig pour vérifier que votre enregistrement TXT est ajouté à votre service DNS

1. Ouvrez une session de terminal.

2. Exécutez la commande suivante pour répertorier les enregistrements TXT de votre domaine. Remplacez *example.com* par votre domaine.

```
dig +short example.com txt
```

3. Vérifiez que la chaîne qui suit TXT dans le résultat de la commande correspond à la valeur TXT que vous voyez lorsque vous sélectionnez le domaine dans la liste des expéditeurs vérifiés de la WorkMail console Amazon.

Pour utiliser nslookup afin de vérifier que votre enregistrement MX est ajouté à votre service DNS

1. Trouvez les serveurs de noms de votre domaine :

   a. Ouvrir une invite de commande.

   b. Exécutez la commande suivante pour répertorier tous les serveurs de noms de votre domaine.

```
nslookup -type=NS example.com
```

   Vous allez interroger l'un de ces serveurs de noms à l'étape suivante.

2. Vérifiez que l'enregistrement MX est correctement ajouté :

   a. Exécutez la commande suivante en *example.com* remplaçant par votre domaine et *ns1.name-server.net* par l'un des serveurs de noms que vous avez identifiés à l'étape précédente.

```
nslookup -type=MX example.com ns1.name-server.net
```

   b. Dans le résultat de la commande, vérifiez que la chaîne qui suit `mail exchange =` correspond à l'une des valeurs suivantes :

   Région de l'Est des États-Unis (Virginie du Nord) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Région ouest des États-Unis (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Région Europe (Irlande) — `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> `10` représente le numéro de préférence ou la priorité MX.

Utilisez dig pour vérifier que votre enregistrement MX est ajouté à votre service DNS

1. Ouvrez une session de terminal.
2. Exécutez la commande suivante pour répertorier les enregistrements MX de votre domaine.

```
dig +short example.com mx
```

3. Vérifiez que la chaîne qui suit `MX` correspond à l'une des valeurs suivantes :

   Région de l'Est des États-Unis (Virginie du Nord) — `10 inbound-smtp.us-east-1.amazonaws.com`

   Région ouest des États-Unis (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

   Région Europe (Irlande) — `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > `10` représente le numéro de préférence ou la priorité MX.

Résolution des problèmes de vérification de domaine

Pour résoudre les problèmes courants liés à la vérification de domaine, consultez les suggestions suivantes :

Votre service DNS n'autorise pas les traits de soulignement dans les noms d'enregistrement TXT

Omettre dans le nom `_amazonses` de l'enregistrement TXT.

Vous souhaitez vérifier le même domaine plusieurs fois, mais vous ne pouvez pas avoir plusieurs enregistrements TXT portant le même nom

Si votre service DNS ne vous autorise pas à avoir plusieurs enregistrements TXT portant le même nom, appliquez l'une des solutions suivantes :

- (Recommandé) Si votre service DNS le permet, attribuez plusieurs valeurs à l'enregistrement TXT. Par exemple, si votre DNS est géré par Amazon Route 53, vous pouvez configurer plusieurs valeurs pour le même enregistrement TXT comme suit :
  1. Dans la console Route 53, choisissez l'enregistrement `_amazonses` TXT que vous avez ajouté lorsque vous avez vérifié votre domaine dans la première région.
  2. Pour Valeur, appuyez sur Entrée après la première valeur.
  3. Ajoutez la valeur de la région supplémentaire, puis enregistrez le jeu d'enregistrements.
- Si vous n'avez besoin de vérifier votre domaine que deux fois, vous pouvez le vérifier une fois en créant un enregistrement TXT avec le nom, puis `_amazonses` en créant un autre enregistrement sans `_amazonses` le nom de l'enregistrement.

La WorkMail console Amazon indique que la vérification du domaine a échoué

Amazon ne WorkMail trouve pas l'enregistrement TXT nécessaire pour votre service DNS. Vérifiez que l'enregistrement TXT requis est correctement ajouté à votre service DNS en suivant la procédure décrite dansVérification des enregistrements MX et TXT avec votre service DNS Records.

Votre fournisseur DNS a ajouté le nom de domaine à la fin de l'enregistrement TXT

L'ajout d'un enregistrement TXT qui contient déjà le nom de domaine, tel que _amazonses.exemple.com, peut entraîner la duplication du nom de domaine, tel que _amazonses.exemple.com.exemple.com. Pour éviter la duplication du nom de domaine, ajoutez un point à la fin du nom de domaine dans l'enregistrement TXT. Cela indique à votre fournisseur DNS que le nom de l'enregistrement est entièrement qualifié et que le nom de domaine est déjà inclus dans l'enregistrement TXT.

Amazon WorkMail signale que l'enregistrement MX est incohérent

Lors de la migration à partir de serveurs de messagerie existants, l'enregistrement MX peut renvoyer le statut Incohérent. Mettez à jour votre enregistrement MX pour qu'il pointe vers Amazon WorkMail au lieu de pointer vers votre ancien serveur de messagerie. L'enregistrement MX est également renvoyé comme étant incohérent lorsqu'un proxy de messagerie tiers est utilisé avec Amazon WorkMail. Dans ce cas, on peut ignorer l'avertissement Inconsistent (Incohérent).

Activation de AutoDiscover la configuration des points de terminaison

AutoDiscover vous permet de configurer Microsoft Outlook et les clients mobiles en utilisant uniquement votre adresse e-mail et votre mot de passe. Le service maintient une connexion à Amazon WorkMail et met à jour les paramètres locaux chaque fois que vous modifiez les points de terminaison ou les paramètres. AutoDiscover Permet également à votre client d'utiliser des WorkMail fonctionnalités supplémentaires d'Amazon, telles que le carnet d'adresses hors ligne, l' Out-of-Officeassistant et la possibilité de consulter l' free/busy heure dans le calendrier.

Le client exécute les AutoDiscover phases suivantes pour détecter le point de terminaison du serveur URLs :

- Phase 1 — Le client effectue une recherche SCP (Secure Copy Protocol) dans l'Active Directory local. Si votre client n'est pas joint au domaine, AutoDiscover ignore cette étape.
- Phase 2 — Le client envoie une demande à l'adresse suivante URLs et valide les résultats. Ces points de terminaison ne sont disponibles qu'avec HTTPS.
  - https ://*company.tld*/autodiscover/autodiscover.xml
  - https://autodiscover. *company.tld*/autodiscover/autodiscover.xml
- Phase 3 — Le client effectue une recherche DNS sur autodiscover.company.tld et envoie une requête GET non authentifiée au point de terminaison dérivé à partir de l'adresse e-mail de l'utilisateur. Si le serveur renvoie une redirection 302, le client renvoie la AutoDiscover demande au point de terminaison HTTPS renvoyé.

Si toutes ces phases échouent, le client ne peut pas être configuré automatiquement. Pour de plus amples informations sur la configuration manuelle des appareils mobiles, veuillez consulter Connexion manuelle de votre appareil mobile.

Vous êtes invité à ajouter l'enregistrement AutoDiscover DNS à votre fournisseur lorsque vous ajoutez votre domaine à Amazon WorkMail. Cela permet au client d'exécuter la phase 3 du AutoDiscover processus. Cependant, ces étapes ne fonctionnent pas pour tous les appareils mobiles, tels que l'application de messagerie Android standard. Par conséquent, il se peut que vous deviez configurer AutoDiscover la phase 2 manuellement.

Vous pouvez utiliser les méthodes suivantes pour configurer AutoDiscover la phase 2 pour votre domaine :

(Recommandé) Utilisez Route 53 et Amazon CloudFront

> **Note**
>
> Les étapes suivantes expliquent comment créer un proxy pour https://autodiscover.*company.tld*/autodiscover/autodiscover.xml. Pour créer un proxy pour https ://*company.tld*/autodiscover/autodiscover.xml, supprimez le `autodiscover.` préfixe des domaines en procédant comme suit.
> L'utilisation CloudFront de la Route 53 peut entraîner des frais. Pour plus d'informations sur les tarifs applicables, consultez CloudFront les tarifs Amazon et Amazon Route 53.

Pour activer AutoDiscover la phase 2 avec Route 53 et CloudFront

1. Obtenez un certificat SSL pour la découverte automatique. *company.tld*et téléchargez-le sur Gestion des identités et des accès AWS (IAM) ouAWS Certificate Manager. Pour plus d'informations, consultez la section Utilisation des certificats de serveur dans le Guide de l'utilisateur IAM ou Getting started dans le Guide de l'AWS Certificate Managerutilisateur.
2. Créez une nouvelle CloudFront distribution :
    1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Dans le volet de navigation, sélectionnez Distributions.
    3. Choisissez Create Distribution.
    4. Sous Web, choisissez Get Started.
    5. Dans les paramètres d'origine, entrez les valeurs suivantes :
        - Nom de domaine d'origine — Le nom de domaine approprié pour votre région :
            - Est des États-Unis (Virginie du Nord) — **`autodiscover-service.mail.us-east-1.awsapps.com`**
            - Ouest des États-Unis (Oregon) — **`autodiscover-service.mail.us-west-2.awsapps.com`**
            - Europe (Irlande) — **`autodiscover-service.mail.eu-west-1.awsapps.com`**
        - Politique du protocole d'origine — La politique souhaitée : **`Match Viewer`**

> **Note**
>
> Laissez le chemin d'origine vide. Ne modifiez pas la valeur renseignée automatiquement pour Origin ID.

6. Dans Paramètres de comportement du cache par défaut, sélectionnez les valeurs suivantes pour les paramètres répertoriés :
   - Stratégie de protocole d'utilisateur : HTTPS uniquement
   - Méthodes HTTP autorisées : GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Mise en cache basée sur des en-têtes de demande sélectionnés : Tout
   - Réacheminer les cookies : Tous
   - Réacheminement et mise en cache des chaînes de requête : Aucun (optimise la mise en cache)
   - Smooth Streaming : Non
   - Limiter l'accès utilisateur : Non
7. Sélectionnez les valeurs suivantes pour Distribution Settings (Paramètres de distribution) :
   - Catégorie de tarifs : Utiliser uniquement États-Unis, Canada et Europe
   - Pour Noms de domaine alternatifs (CNAMEs), entrez **`autodiscover.company.tld`** ou**`company.tld`**, où *`company.tld`* est votre nom de domaine.
   - Certificat SSL : certificat SSL personnalisé (stocké dans IAM)
   - Prise en charge d'un client SSL personnalisé : Choisissez Tous les clients ou Seuls les clients qui prennent en charge Server Name Indication (SNI). Les anciennes versions d'Android peuvent ne pas fonctionner avec la dernière option.

     > **Note**
     >
     > Si vous choisissez Tous les clients, laissez vide l'option Objet racine par défaut.

   - Journalisation : Choisissez Activé ou Désactivé. Activé active la journalisation.
   - Dans Commentaire, saisissez **`AutoDiscover type2 for autodiscover.company.tld`**
   - État de distribution : choisissez Activé.
8. Choisissez Create Distribution.

3. Dans la console Route 53, créez un enregistrement qui achemine le trafic Internet de votre nom de domaine vers votre CloudFront distribution.

> **Note**
>
> Ces étapes supposent que l'enregistrement DNS de example.com est hébergé sur Route 53. Si vous n'utilisez pas Route 53, suivez les procédures de la console de gestion de votre fournisseur DNS.

1. Dans le volet de navigation de la console, choisissez Hosted Zones, puis choisissez un domaine.
2. Dans la liste des domaines, choisissez le nom de domaine que vous souhaitez utiliser.
3. Dans Enregistrements, choisissez Créer un enregistrement.
4. Sous Création rapide d'un enregistrement, définissez les paramètres suivants :
   - Sous Nom de l'enregistrement, entrez le nom de l'enregistrement.
   - Sous Politique de routage, sélectionnez Routage simple.
   - Cliquez sur le curseur Alias pour l'activer. Le curseur devient bleu lorsqu'il est activé.
   - Dans la liste Type d'enregistrement, choisissez A - Route le trafic vers une IPv4 adresse et certaines ressources AWS.
   - Dans la liste Acheminer le trafic vers, choisissez Alias vers CloudFront la distribution.
   - Un champ de recherche apparaîtra sous la liste Router le trafic vers. Entrez le nom de votre CloudFront distribution dans la zone de texte. Vous pouvez également sélectionner votre distribution dans la liste qui apparaît lorsque vous sélectionnez le champ de recherche.
5. Choisissez Créer un registre.

Utiliser un serveur Web Apache

Les étapes suivantes expliquent comment utiliser un serveur Web Apache pour créer un proxy pour https://autodiscover. *company.tld*/autodiscover/autodiscover.xml. Pour créer un proxy pour https ://*company.tld*/autodiscover/autodiscover.xml, supprimez le « autodiscover ». préfixe à partir des domaines dans les étapes suivantes.

Pour activer AutoDiscover la phase 2 avec un serveur Web Apache

1. Exécutez les directives suivantes sur un serveur Apache compatible SSL :

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. Le cas échéant, activez les modules Apache suivants. Si vous ne savez pas comment procéder, consultez l'aide d'Apache :

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

Consultez la section suivante pour plus d'informations sur les tests et le dépannage AutoDiscover.

AutoDiscover résolution des problèmes de phase 2

Une fois que vous avez configuré votre fournisseur DNS pour AutoDiscover, vous pouvez tester la configuration de votre AutoDiscover point de terminaison. Si vous avez correctement configuré votre terminal, il répond par un message de demande non autorisé.

Pour effectuer une demande non autorisée de base

1. À partir d'un terminal, créez une requête POST non authentifiée à destination du AutoDiscover point de terminaison.

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
```

   Si votre point de terminaison est correctement configuré, il doit renvoyer un `401 unauthorized` message, comme illustré dans l'exemple suivant :

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
...
HTTP/1.1 401 Unauthorized
```

2. Ensuite, testez une vraie AutoDiscover demande. Créez un `request.xml` fichier avec le contenu XML suivant :

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
requestschema/2006">
    <Request>
        <EMailAddress>testuser@company.tld</EMailAddress>
        <AcceptableResponseSchema>
            http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006
        </AcceptableResponseSchema>
    </Request>
</Autodiscover>
```

3. Utilisez le `request.xml` fichier que vous avez créé et envoyez une AutoDiscover demande authentifiée au point de terminaison. N'oubliez pas de *`testuser@company.tld`* remplacer par une adresse e-mail valide :

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

La réponse ressemblera à l'exemple suivant si le point de terminaison est correctement configuré :

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
```

```
        <Settings>
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
        </Settings>
    </Action>
</Response>
```

Modification des stratégies d'identité de domaine

Les politiques d'identité de domaine spécifient les autorisations pour les actions par e-mail, telles que la redirection des e-mails. Par exemple, vous pouvez rediriger les e-mails vers n'importe quelle adresse e-mail de votre WorkMail organisation Amazon.

> **Note**
>
> À compter du 1er avril 2022, Amazon WorkMail a commencé à utiliser des principes de service pour l'autorisation plutôt que des principes de AWS compte. Si vous avez ajouté un domaine avant le 1er avril 2022, vous avez peut-être une ancienne politique qui utilise un principal de AWS compte pour l'autorisation. Si tel est le cas, nous vous recommandons de mettre à jour la politique la plus récente. Les étapes décrites dans cette section expliquent comment procéder. Votre organisation continue d'envoyer des e-mails normalement pendant la mise à jour.

Vous ne devez suivre ces étapes que si vous n'utilisez pas de politique Amazon SES personnalisée. Si vous utilisez une politique Amazon SES personnalisée, vous devez la mettre à jour vous-même. Pour plus d'informations, voirPolitique principale de service personnalisée d'Amazon SES, plus loin dans cette rubrique.

> **Important**
>
> Ne supprimez pas vos domaines existants. Si vous le faites, vous perturberez le service de messagerie. Il vous suffit de saisir à nouveau vos domaines existants.

Pour mettre à jour une politique d'identité de domaine

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Pour ce faire, ouvrez la liste Sélectionnez une région située à droite du champ de recherche, puis choisissez la région souhaitée. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Domains.
4. Sélectionnez et copiez le nom du domaine que vous souhaitez saisir à nouveau, puis choisissez Ajouter un domaine.

   La boîte de dialogue Ajouter un domaine apparaît.
5. Collez le nom copié dans le champ Nom de domaine, puis choisissez Ajouter un domaine.
6. Répétez les étapes 3 à 5 pour les autres domaines de votre organisation.

Politique principale de service personnalisée d'Amazon SES

Si vous utilisez une politique Amazon SES personnalisée, adaptez cet exemple pour l'utiliser dans votre domaine.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuthorizeWorkMail",
            "Effect": "Allow",
            "Principal": {
                "Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "ses:*"
            ],
```

```
            "Resource": "arn:aws:ses:us-east-1:111122223333:identity/WORKMAIL-
DOMAIN-NAME",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:workmail:us-
east-1:111122223333:organization/WORKMAIL_ORGANIZATION_ID"
                }
            }
        }
    ]
}
```

Authentification d'e-mails avec SPF

Sender Policy Framework (SPF) est une norme de validation des e-mails conçue pour lutter contre l'usurpation de messagerie. L'usurpation d'identité consiste à faire en sorte qu'un e-mail envoyé par un acteur malveillant ressemble à un e-mail envoyé par un utilisateur légitime. Pour plus d'informations sur la configuration du SPF pour votre domaine WorkMail compatible Amazon, consultez Authentification des e-mails avec le SPF dans Amazon SES.

Configuration d'un domaine MAIL FROM personnalisé

Par défaut, Amazon WorkMail utilise le sous-domaine amazonses.com comme `MAIL FROM` domaine pour vos e-mails sortants. Cela peut entraîner un échec de livraison si la politique DMARC de votre domaine est uniquement configurée pour le SPF. Pour résoudre ce problème, configurez votre propre domaine en tant que `MAIL FROM` domaine. Pour savoir comment configurer votre domaine de messagerie en tant que `MAIL FROM` domaine, consultez la section Configuration d'un domaine MAIL FROM personnalisé dans le manuel Amazon Simple Email Service Developer Guide.

> **Important**
>
> Un domaine MAIL FROM personnalisé est requis lorsque vous l'activez AutoDiscover pour les appareils iOS.

Pour plus d'informations sur `MAIL FROM` les domaines personnalisés, consultez Amazon SES prend désormais en charge les domaines MAIL FROM personnalisés.

Utilisation des utilisateurs

Vous pouvez créer et supprimer des utilisateurs sur Amazon WorkMail. En outre, vous pouvez réinitialiser leurs mots de passe de messagerie, gérer leurs quotas de boîte aux lettres et l'accès aux appareils, ainsi que contrôler leurs autorisations de boîte aux lettres.

Rubriques

Afficher une liste d'utilisateurs

Pour consulter la liste des utilisateurs

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez utilisateurs.
4. En outre, vous pouvez filtrer les utilisateurs par nom d'utilisateur, nom d'affichage ou adresse e-mail principale.

> **Note**
>
> La recherche fait la distinction majuscules/minuscules.

Ajout d'un utilisateur

Lorsque vous ajoutez un utilisateur, Amazon crée WorkMail automatiquement des boîtes aux lettres pour celui-ci. Les utilisateurs peuvent se connecter et accéder à leur courrier depuis l'application WorkMail Web Amazon, leur appareil mobile ou en utilisant Microsoft Outlook sur macOS ou PC.

Pour ajouter un utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation à laquelle vous souhaitez ajouter des utilisateurs.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez Ajouter un utilisateur.

   L'écran Ajouter un utilisateur apparaît.
4. Sous Détails de l'utilisateur, dans le champ Nom d'utilisateur, entrez le nom de l'utilisateur. Le nom apparaît également dans le champ Adresse e-mail. Si vous souhaitez que l'utilisateur ait une adresse e-mail différente de son nom d'utilisateur, vous pouvez modifier le champ Adresse e-mail.
5. (Facultatif) Entrez le prénom et le nom de famille de l'utilisateur dans les zones Prénom et Nom de famille.
6. Dans le champ Nom d'affichage, entrez le nom d'affichage de l'utilisateur.
7. Dans le champ Adresse e-mail, acceptez l'alias d'e-mail ou saisissez-en un autre.
8. Par défaut, les utilisateurs sont affichés dans la liste d'adresses globale. Pour masquer l'utilisateur de la liste d'adresses globale, décochez la case Afficher dans la liste d'adresses globale.
9. Sélectionnez Ne pas créer de boîte aux lettres pour ajouter un utilisateur en tant qu'utilisateur distant à l'organisation.

10. Sous Configuration du mot de passe, entrez le mot de passe de l'utilisateur dans les zones Mot de passe et Répéter le mot de passe.
11. Sélectionnez Ajouter un utilisateur.

Activation des utilisateurs

Lorsque vous intégrez Amazon WorkMail à votre annuaire Active Directory d'entreprise, ou que vous avez déjà des utilisateurs disponibles dans votre annuaire Simple AD, vous pouvez activer ces utilisateurs dans Amazon WorkMail. Vous devez également suivre ces étapes pour réactiver un utilisateur dont le compte a été désactivé.

Pour activer un utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation pour laquelle vous souhaitez activer les utilisateurs.
3. Dans le panneau de navigation, choisissez utilisateurs.

   La liste des utilisateurs s'affiche. Les comptes utilisateur dont l'état est activé, désactivé et utilisateur du système sont affichés dans la liste.
4. Dans la liste des utilisateurs dont les comptes sont désactivés, cochez les cases correspondant aux utilisateurs que vous souhaitez activer, puis choisissez Activer.

   La boîte de dialogue Activer les utilisateurs s'affiche.
5. Le cas échéant, vérifiez et modifiez l'adresse e-mail principale de chaque utilisateur, puis sélectionnez Activer.

Gestion des alias d'utilisateur

Vous pouvez ajouter ou supprimer des alias d'e-mail pour les utilisateurs.

Pour ajouter un alias d'e-mail à un utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation pour laquelle vous souhaitez ajouter des utilisateurs.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez le nom de l'utilisateur auquel vous souhaitez ajouter un alias.
4. Dans la section Informations sur l'utilisateur, choisissez l'onglet Alias.
5. Dans l'onglet Alias, choisissez Ajouter un alias.
6. Dans le champ Alias, entrez un alias.
7. Sélectionnez un domaine pour un alias.
8. Choisissez Ajouter.

Pour supprimer un alias d'e-mail d'un utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation dont vous souhaitez supprimer des utilisateurs.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez le nom de l'utilisateur dont vous souhaitez supprimer les alias.
4. Dans la section Informations sur l'utilisateur, choisissez l'onglet Alias.
5. Dans l'onglet Alias, cochez la case correspondant aux alias que vous souhaitez supprimer.
6. Vérifiez les alias qui seront supprimés.
7. Dans la fenêtre Supprimer les alias, choisissez Supprimer.

Désactivation d'utilisateurs

Vous pouvez désactiver n'importe quel utilisateur d'une organisation à tout moment. Lorsque vous désactivez un utilisateur, il devient immédiatement inaccessible. Les utilisateurs désactivés pendant plus de 30 jours verront leur boîte de réception supprimée d'Amazon WorkMail.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation qui contient les utilisateurs que vous souhaitez désactiver.
3. Dans le panneau de navigation, choisissez utilisateurs.

   La liste de tous les utilisateurs apparaît, indiquant les comptes dont l'état est activé, désactivé et les comptes utilisateur du système.
4. Dans la liste des utilisateurs autorisés, cochez les cases correspondant aux comptes que vous souhaitez désactiver, puis choisissez Désactiver.

   La boîte de dialogue Désactiver les utilisateurs s'affiche.
5. Choisissez Désactiver.

Modification des informations utilisateur

Lorsque vous modifiez les informations de l'utilisateur, vous pouvez modifier les éléments suivants :

- Données personnelles : noms, adresses e-mail, numéros de téléphone et autres informations personnelles.
- Quotas de boîte aux lettres (tailles) : les quotas peuvent aller de 1 Mo à 51 200 Mo (50 Go). Amazon WorkMail informe les utilisateurs lorsqu'ils atteignent 90 % de leur quota. De plus, la modification du quota de boîtes aux lettres d'un utilisateur n'aura aucune incidence sur la tarification. Pour plus d'informations sur les tarifs, consultez Amazon WorkMail Pricing.
- Accès aux appareils mobiles : supprimez et effacez les appareils, et consultez les détails des appareils.

- Autorisations d'accès aux boîtes aux lettres : accordez aux utilisateurs l'autorisation d'utiliser une boîte aux lettres et accordez-leur différents niveaux d'accès à la boîte aux lettres.
- Jetons d'accès personnels (lorsque le centre d'identité IAM est activé) : affichez et supprimez les jetons d'accès personnels.

> **Note**
>
> Si vous intégrez Amazon WorkMail à un annuaire AD Connector, vous ne pouvez pas modifier ces informations depuis le AWS Management Console. Vous devez plutôt les modifier avec les outils de gestion Active Directory. Des limitations s'appliquent lorsque votre organisation est en mode interopérabilité. Pour de plus amples informations, veuillez consulter Limitations applicables au mode interopérabilité.

Pour modifier les informations de l'utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation que vous souhaitez utiliser.
3. Dans le volet de navigation, choisissez Utilisateurs, puis le nom de l'utilisateur à modifier.

Pour modifier les données personnelles

1. Dans la section Informations sur l'utilisateur, choisissez Modifier.
2. Sous Détails de l'utilisateur, entrez ou modifiez les informations personnelles de l'utilisateur selon vos besoins.
3. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Pour s'associer à un utilisateur d'IAM Identity Center

1. Sous Informations sur l'utilisateur, choisissez Modifier.

2. Entrez l'ID utilisateur de l'utilisateur IAM Identity Center que vous souhaitez associer. Vous pouvez consulter ces informations dans le tableau Utilisateurs assignés sur la page IAM Identity Center ou dans la console IAM Identity Center.
3. Sélectionnez Enregistrer les modifications.

Pour modifier les quotas de boîtes aux lettres

1. Sous Détails de l'utilisateur, cliquez sur l'onglet Quota, puis sur Modifier.
2. Dans le champ Mettre à jour le quota de boîte aux lettres, entrez la taille de la boîte aux lettres. Vous pouvez saisir des valeurs comprises entre **1** et**51200**.
3. Sélectionnez Enregistrer les modifications.

Pour gérer les données des appareils mobiles

> **Note**
>
> Pour gérer les appareils mobiles, vos utilisateurs doivent d'abord connecter leurs appareils à votre instance d'Amazon WorkMail. Pour plus d'informations sur la connexion d'appareils mobiles, reportez-vous à la section Configuration des clients d'appareils mobiles pour Amazon WorkMail.

1. Sous Détails de l'utilisateur, choisissez l'onglet Appareils mobiles.
2. Pour voir la liste actuelle des appareils, choisissez Actualiser.
3. Pour afficher les détails d'un appareil, choisissez le nom de l'appareil dans la colonne Device ID.
4. Pour supprimer ou effacer l'appareil, cliquez sur le bouton radio à côté du nom de l'appareil, puis choisissez Supprimer ou Effacer selon vos besoins.
5. Dans la boîte de dialogue qui apparaît, confirmez l'opération de suppression ou d'effacement. N'oubliez pas que les utilisateurs réapparaîtront lorsqu'ils synchroniseront à WorkMail nouveau leurs appareils avec Amazon.

Pour modifier les autorisations d'accès à une boîte aux lettres

1. Sélectionnez l'onglet Autorisations.
2. Effectuez l'une des actions suivantes :

1. Pour ajouter des autorisations, choisissez Ajouter des autorisations. Ouvrez la liste Ajouter de nouvelles autorisations et choisissez un utilisateur ou un groupe, choisissez les paramètres d'autorisation pour l'utilisateur ou le groupe, puis sélectionnez Enregistrer.
2. Pour modifier les autorisations des utilisateurs, cliquez sur le bouton situé à côté du nom de l'utilisateur. Choisissez Modifier, sélectionnez les options souhaitées, puis cliquez sur Enregistrer.

Pour plus d'informations sur les options d'autorisation, reportez-vous àGestion des autorisations d'accès à une boîte aux lettres.

3. Pour supprimer toutes les autorisations, choisissez Supprimer, puis confirmez la suppression.

Pour supprimer des jetons d'accès personnels

> **Note**
>
> Assurez-vous que le jeton que vous supprimez n'est utilisé activement par aucun client de messagerie. La suppression d'un jeton lorsqu'il est utilisé interrompt l'authentification des clients utilisant le jeton.

1. Choisissez l'onglet Personal Access Tokens.
2. Dans la liste des jetons d'accès personnels, sélectionnez le jeton d'accès personnel à supprimer.
3. Choisissez Supprimer le jeton.
4. Entrez Type dans la zone de texte de confirmation.

Réinitialisation du mot de passe utilisateur

Si un utilisateur oublie son mot de passe ou rencontre des difficultés pour se connecter à Amazon WorkMail, vous pouvez le réinitialiser.

> **Note**
>
> - Si vous avez intégré Amazon WorkMail à un annuaire AD Connector, vous devez réinitialiser le mot de passe utilisateur dans Active Directory.

- Si vous avez intégré Amazon WorkMail à IAM Identity Center, vous pouvez choisir de réinitialiser le mot de passe utilisateur. Pour plus d'informations, voir Réinitialiser le mot de passe utilisateur d'IAM Identity Center pour un utilisateur final dans le guide de l'AWS IAM Identity Center utilisateur.

Pour réinitialiser un mot de passe utilisateur

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez utilisateurs.
4. Dans la liste des utilisateurs, cochez la case à côté du nom de l'utilisateur, puis choisissez Réinitialiser le mot de passe.
5. Dans la boîte de dialogue Réinitialiser le mot de passe, entrez le nouveau mot de passe, puis choisissez Réinitialiser.

Résolution des problèmes liés aux politiques WorkMail de mot de passe Amazon

Si la réinitialisation du mot de passe échoue, vérifiez que le nouveau mot de passe respecte les exigences de la stratégie de mot de passe.

Les exigences de la politique de mot de passe dépendent du type de répertoire utilisé par votre WorkMail organisation Amazon.

Politique de mot de passe pour les annuaires Amazon WorkMail et Simple AD

Par défaut, les mots de passe d'un WorkMail annuaire Amazon ou d'un annuaire Simple AD doivent être les suivants :

- Non vide

- Au moins huit caractères
- Moins de 64 caractères
- Composé de caractères supplémentaires en latin de base ou en latin-1

Les mots de passe doivent également contenir des caractères issus de trois des cinq groupes suivants :

- Caractères majuscules
- Caractères minuscules
- Chiffres numériques (0 à 9)
- Caractères spéciaux (par exemple <, ~, ou !)
- Caractères Latin-1 (par exemple é, ü, ou ñ)

Les politiques relatives aux mots de passe des WorkMail annuaires Amazon ne peuvent pas être modifiées.

Pour modifier une politique de mot de passe Simple AD, utilisez les outils d'administration AD sur une instance Windows Amazon Elastic Compute Cloud (Amazon EC2) de votre annuaire Simple AD. Pour plus d'informations, consultez la section Installation des outils d'administration Active Directory dans le Guide d'AWS Directory Service administration.

AWS Managed Microsoft AD Politique de mot de passe du répertoire

Pour plus d'informations sur la politique de mot de passe par défaut pour un AWS Managed Microsoft AD annuaire, consultez la section Gérer les politiques de mot AWS Managed Microsoft AD de passe du Guide d'AWS Directory Service administration.

Politique de mot de passe AD Connector

AD Connector utilise la politique de mot de passe du domaine Active Directory auquel il est connecté. Consultez la documentation de votre domaine Active Directory pour plus d'informations sur les paramètres de politique de mot de passe.

Utilisation des notifications

Grâce à l'API Amazon WorkMail Push Notifications, vous pouvez recevoir des notifications push concernant les modifications apportées à votre boîte aux lettres, notamment les nouveaux e-

mails et les mises à jour du calendrier. Vous devez enregistrer le URLs (ou les répondeurs aux notifications push) pour recevoir des notifications. Grâce à cette fonctionnalité, les développeurs peuvent créer des applications réactives pour WorkMail les utilisateurs d'Amazon, car les applications sont rapidement informées des modifications depuis la boîte aux lettres d'un utilisateur.

Pour de plus amples informations, veuillez consulter Abonnements à des notifications, événements de boîte aux lettres et EWS dans Exchange.

Vous pouvez vous abonner à des dossiers spécifiques, tels que la boîte de réception ou le calendrier, ou à tous les dossiers pour les événements de modification de boîte aux lettres (y compris Nouveau courrier, créé et modifié).

Vous pouvez utiliser des bibliothèques clientes telles que l'API Java EWS ou l'API Managed EWS C# pour accéder à cette fonctionnalité. Un exemple complet d'application de répondeur push, développé à l'aide d'AWS Lambda et d'API Gateway (à l'aide du framework AWS Serverless), est disponible sur cette page. AWS GitHub Cet exemple utilise l'API Java EWS.

Vous trouverez ci-dessous un exemple de demande d'abonnement push :

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
```

```
</soap:Envelope>
```

Vous trouverez ci-dessous un résultat de demande d'abonnement réussie :

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

Ensuite, les notifications sont envoyées à l'URL indiquée dans la demande d'abonnement. Voici un exemple de notification :

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
```

```
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
                    <m:Notification>
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
                            <t:Watermark>ywwAAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

Pour confirmer que le répondeur de notification push a reçu la notification, celui-ci doit répondre avec ce qui suit :

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

Pour se désabonner de la réception des notifications push, les clients doivent envoyer une réponse de désabonnement dans le champ `SubscriptionStatus`, similaire à ce qui suit :

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
```

```
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

Pour vérifier l'état de votre répondeur de notifications push, Amazon WorkMail envoie un « battement de cœur » (également appelé a`StatusEvent`). La fréquence à laquelle les pulsations sont envoyées est déterminée par le paramètre `StatusFrequency` fourni dans la demande d'abonnement initiale. Par exemple, s'il `StatusFrequency` est égal**1**, a `StatusEvent` est envoyé toutes les 1 minute. Cette valeur peut être comprise entre 1 et 1440 minutes. Ce `StatusEvent` se présente comme suit :

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

Si le répondeur de notifications push d'un client ne répond pas avec le même 0K statut qu'auparavant, la notification est réessayée pendant un maximum de `StatusFrequency` minutes.

Par exemple, si la valeur de `StatusFrequency` est égale à 5 et que la première notification échoue, celle-ci est retentée pendant 5 minutes maximum avec un backoff exponentiel entre chaque nouvelle tentative. Si la notification n'est pas envoyée après l'expiration du délai de nouvelle tentative, l'abonnement est invalidé et aucune nouvelle notification n'est envoyée. Vous devez créer un nouvel abonnement pour continuer à recevoir des notifications sur les événements de boîte aux lettres. Actuellement, vous pouvez souscrire à trois abonnements maximum par boîte aux lettres.

Activation d'un e-mail signé ou chiffré

Vous pouvez l'utiliser S/MIME pour permettre aux utilisateurs d'envoyer des e-mails signés ou chiffrés à la fois à l'intérieur et à l'extérieur de l'organisation.

> **Note**
>
> Les certificats utilisateur contenus dans la liste d'adresses globale sont pris en charge uniquement dans une configuration Active Directory connecté.

Pour autoriser les utilisateurs à envoyer des e-mails signés ou chiffrés

1. Configurez un connecteur Active Directory (AD Connector). La configuration d'un connecteur AD avec votre annuaire sur site permet aux utilisateurs de continuer à utiliser leurs informations d'identification d'entreprise existantes.
2. Configurez l'inscription automatique des certificats pour émettre et stocker automatiquement les certificats utilisateur dans Active Directory. Amazon WorkMail reçoit les certificats utilisateur d'Active Directory et les publie auprès du GAL. Pour de plus amples informations, veuillez consulter Configuration de l'inscription automatique aux certificats.
3. Distribuez les certificats générés aux utilisateurs en exportant les certificats depuis le serveur exécutant Microsoft Exchange et en les envoyant par la poste.
4. Chaque utilisateur installe le certificat dans son programme de messagerie électronique (par exemple, Windows Outlook) et sur ses appareils mobiles.

Utilisation des groupes de

Vous pouvez utiliser des groupes comme listes de distribution sur Amazon WorkMail pour recevoir des e-mails pour des adresses e-mail génériques, telles que <sales@example.com> ou <support@example.com>. Vous pouvez créer plusieurs alias d'e-mail pour un groupe.

Vous pouvez également utiliser des groupes en tant que groupes de sécurité pour partager une boîte aux lettres ou un calendrier avec une équipe en particulier.

Les groupes n'ont pas leur propre boîte aux lettres, ce qui affecte les autorisations de boîte aux lettres que vous pouvez accorder à un groupe. Pour plus d'informations sur la configuration des autorisations de boîte aux lettres pour un groupe, consultezGestion des autorisations de boîte aux lettres pour les groupes.

> **Note**
>
> Cela peut prendre jusqu'à 2 heures avant que les groupes récemment ajoutés apparaissent dans votre carnet d'adresses hors connexion de Microsoft Outlook.

Rubriques

Afficher la liste des groupes

Pour consulter la liste des groupes

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Groupes .
4. En outre, vous pouvez filtrer les groupes par nom de groupe ou adresse e-mail principale.

> **Note**
>
> La recherche fait la distinction majuscules/minuscules.

Ajouter un groupe

Vous pouvez ajouter des groupes depuis la WorkMail console Amazon.

Pour ajouter un groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la région AWS. Dans la barre en haut de la fenêtre de la console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Groupes, puis Ajouter un groupe.

   La page Ajouter un groupe apparaît.
4. Sous Nom du groupe, entrez le nom du groupe.
5. Sous Adresse e-mail, entrez l'adresse e-mail principale du groupe.
6. Vérifiez l'adresse e-mail du groupe, mettez-la à jour si nécessaire.

7. Par défaut, le groupe est affiché dans la liste d'adresses globale. Pour masquer le groupe dans la liste d'adresses globale, décochez la case Afficher dans la liste d'adresses globale.
8. Choisissez Add Group (Ajouter un groupe).

Groupes habilitants

Lorsque vous intégrez Amazon WorkMail à l'Active Directory de votre entreprise, ou lorsque des groupes sont déjà disponibles dans votre Active Directory simple, vous pouvez utiliser ces groupes comme groupes de sécurité ou listes de distribution sur Amazon WorkMail.

Pour activer un groupe d'annuaires existant

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Groupes .
4. Cochez la case à côté du groupe que vous souhaitez activer, puis sélectionnez Activer.

   La boîte de dialogue Activer les groupes apparaît et vous demande de confirmer l'opération.
5. Le cas échéant, vérifiez et modifiez l'adresse e-mail principale de chaque groupe, puis sélectionnez Activer.

Ajouter des membres à un groupe

Après avoir créé et activé un WorkMail groupe Amazon, utilisez la WorkMail console Amazon pour ajouter des membres à ce groupe.

> **Note**
>
> Si Amazon WorkMail est intégré à un service Active Directory connecté ou à Microsoft Active Directory, vous pouvez utiliser Active Directory pour gérer les membres de votre groupe. Toutefois, la propagation des modifications sur Amazon WorkMail peut prendre plus de temps.

Pour ajouter des membres à un groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Groupes .
4. Sélectionnez le nom du groupe.
5. Sur la page des détails du groupe, choisissez l'onglet Membres.
6. Choisissez un groupe ou un utilisateur à ajouter sous Groupe ou utilisateur.
7. Sélectionnez l'utilisateur ou le groupe dans le menu déroulant.
8. Choisissez Enregistrer.

La propagation de vos modifications peut prendre quelques minutes.

Modification des détails du groupe

Vous pouvez modifier les détails d'un groupe.

Pour modifier les détails du groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Groupes, puis sélectionnez le groupe à modifier.
4. Sur la page des détails du groupe, mettez à jour l'adresse e-mail selon vos besoins.
5. Par défaut, les groupes sont affichés dans la liste d'adresses globale. Pour masquer le groupe dans la liste d'adresses globale, décochez la case Afficher dans la liste d'adresses globale.
6. Sélectionnez Enregistrer les modifications.

Supprimer des membres d'un groupe

Utilisez la WorkMail console Amazon pour supprimer des membres d'un groupe.

> **Note**
>
> Si Amazon WorkMail est intégré à un Active Directory ou à Microsoft Active Directory connecté, vous pouvez utiliser Active Directory pour gérer les membres de votre groupe. Cependant, cela peut créer le temps nécessaire pour transmettre vos modifications à Amazon WorkMail.

Pour supprimer des membres d'un groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Groups, puis choisissez le nom du groupe.
4. Sur la page des détails du groupe, choisissez l'onglet Membres.
5. Sélectionnez le membre à supprimer du groupe.
6. Sélectionnez Remove (Supprimer).

La propagation de vos modifications peut prendre quelques minutes.

Gestion des alias de groupe

Vous pouvez ajouter ou supprimer des alias d'e-mail aux groupes.

Pour ajouter un alias d'e-mail à un groupe.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation pour laquelle vous souhaitez ajouter un alias.
3. Dans le volet de navigation, choisissez Groups, puis sélectionnez le nom du groupe auquel vous souhaitez ajouter un alias.
4. Dans la section Détails du groupe, sélectionnez Alias.
5. Sous Alias, choisissez Ajouter un alias.
6. Dans le champ Alias, entrez un alias.
7. Sélectionnez un domaine pour un alias.
8. Choisissez Ajouter.

Pour supprimer les alias d'un e-mail d'un groupe.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation dont vous souhaitez supprimer un alias.
3. Dans le volet de navigation, choisissez Groupes, puis sélectionnez le nom du groupe dont vous souhaitez supprimer les alias.
4. Dans la section Détails du groupe, sélectionnez Alias.
5. Sous Alias, cochez la case correspondant aux alias que vous souhaitez supprimer.
6. Sélectionnez Remove (Supprimer).
7. Vérifiez les alias qui seront supprimés.
8. Dans la fenêtre Supprimer les alias, choisissez Supprimer.

Désactivation de groupes

Vous pouvez désactiver un groupe lorsque vous n'en avez plus besoin.

Pour désactiver un groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Groupes .
4. Sous Nom du groupe, sélectionnez les groupes à désactiver, puis choisissez Désactiver.
5. Dans la boîte de dialogue Désactiver le(s) groupe(s) choisissez Désactiver.

Suppression d'un groupe

Avant de pouvoir supprimer un groupe, vous devez d'abord le désactiver. Pour plus d'informations sur la désactivation des groupes, consultezDésactivation de groupes.

Pour supprimer un groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Groupes .
4. Cochez la case à côté du groupe désactivé que vous souhaitez supprimer et choisissez Supprimer.

   La boîte de dialogue Supprimer apparaît.
5. Dans le champ Entrez le nom du groupe pour confirmer la suppression, entrez le nom du groupe, puis choisissez Supprimer.

> **Note**
>
> Pour supprimer définitivement un groupe, utilisez l'action `DeleteGroup` API pour Amazon WorkMail. Pour plus d'informations, consultez DeleteGrouple Amazon WorkMail API Reference.

Utilisation des ressources

Amazon WorkMail peut aider vos utilisateurs à réserver des ressources. Par exemple, les utilisateurs peuvent réserver des salles de réunion ou des équipements tels que des projecteurs, des téléphones ou des voitures. Pour réserver une ressource, l'utilisateur ajoute la ressource à l'invitation à la réunion.

Rubriques

Afficher une liste de ressources

Pour consulter la liste des ressources

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, choisissez Resources (Ressources).
4. En outre, vous pouvez filtrer les ressources par nom de ressource ou par adresse e-mail principale.

> **Note**
>
> La recherche fait la distinction majuscules/minuscules.

Ajouter une ressource

Vous pouvez ajouter une nouvelle ressource à votre organisation et autoriser vos utilisateurs à la réserver.

Pour ajouter une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Ressources, puis Ajouter une ressource.

   La page Ajouter une ressource apparaît.
4. Dans le champ Nom de la ressource, entrez le nom de la ressource.
5. Dans le champ Description de la ressource, entrez éventuellement une description de la ressource.
6. Sous Type de ressource, choisissez une option.
7. Vérifiez l'adresse e-mail de la ressource, mettez-la à jour si nécessaire.
8. Par défaut, la ressource est affichée dans la liste d'adresses globale. Pour masquer la ressource dans la liste d'adresses globale, décochez la case Afficher dans la liste d'adresses globale.
9. Choisissez Add resource (Ajouter ressource).

Modification des détails des ressources

Vous pouvez modifier les informations générales d'une ressource, notamment le nom, la description, le type et l'adresse e-mail, les options de réservation et les délégués.

Pour modifier les informations générales de ressources

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Ressources, puis sélectionnez la ressource à modifier.
4. Sur la page Détails de la ressource, mettez à jour le nom, la description, le type de ressource ou l'adresse e-mail de la ressource selon vos besoins.
5. Par défaut, les ressources sont affichées dans la liste d'adresses globale. Pour masquer la ressource dans la liste d'adresses globale, décochez la case Afficher dans la liste d'adresses globale.
6. Sélectionnez Enregistrer les modifications.

Vous pouvez configurer une ressource pour accepter ou refuser automatiquement des demandes de réservation.

Vous pouvez modifier les options de réservation de la ressource.

Pour modifier les options de réservation d'une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, sélectionnez Ressources, puis sélectionnez la ressource à modifier. Une page apparaît et affiche les détails des ressources.
4. Sous Options de réservation, choisissez Modifier.
5. Le cas échéant, cochez ou décochez la case à côté d'une option pour l'activer ou la désactiver.

> **Note**
>
> Lorsque vous désactivez l'une des options de réservation automatique, vous devez créer un délégué chargé de gérer les demandes de réservation. Les étapes suivantes expliquent comment créer un délégué.

Vous pouvez ajouter un délégué pour contrôler les demandes de réservation pour une ressource pour laquelle aucune option de réservation automatique n'est configurée. Les délégués de la ressource reçoivent automatiquement une copie de toutes les demandes de réservation et ont un accès total au calendrier de la ressource. En outre, ils doivent accepter toutes les demandes de réservation pour une ressource.

Pour ajouter un délégué de ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Resources, puis sélectionnez le nom de la ressource à laquelle vous souhaitez ajouter un délégué.
4. (Facultatif) Dans l'onglet Options de réservation, choisissez Modifier, désactivez la case à cocher Accepter automatiquement toutes les demandes de ressources, puis choisissez Enregistrer.
5. Choisissez l'onglet Délégués, puis sélectionnez Ajouter un délégué.

   La boîte de dialogue Ajouter un délégué apparaît.
6. Ouvrez la liste Rechercher des délégués et choisissez un délégué, puis cliquez sur Enregistrer.

Pour supprimer un délégué de ressources

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation dont vous souhaitez supprimer des délégués.
3. Dans le volet de navigation, choisissez Resources, puis sélectionnez le nom de la ressource dont vous souhaitez supprimer un délégué.
4. Choisissez Délégués, puis choisissez le délégué à supprimer.
5. Choisissez Supprimer.

Gestion des alias de ressources

Vous pouvez ajouter ou supprimer des alias d'e-mail aux ressources.

Pour ajouter un alias d'e-mail à une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation à laquelle vous souhaitez ajouter un alias.
3. Dans le volet de navigation, choisissez Resources, puis sélectionnez le nom de la ressource à laquelle vous souhaitez ajouter un alias.
4. Dans la section Détails de la ressource, sélectionnez Alias.
5. Sous Alias, choisissez Ajouter un alias.
6. Dans le champ Alias, entrez un alias.
7. Sélectionnez un domaine pour un alias.
8. Choisissez Ajouter.

Pour supprimer les alias d'un e-mail d'une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation dont vous souhaitez supprimer les alias.
3. Dans le volet de navigation, choisissez Resources, puis sélectionnez le nom de la ressource dont vous souhaitez supprimer les alias.
4. Dans la section Détails de la ressource, sélectionnez Alias.
5. Sous Alias, cochez la case correspondant aux alias que vous souhaitez supprimer.
6. Sélectionnez Remove (Supprimer).
7. Vérifiez les alias qui seront supprimés.
8. Dans la fenêtre Supprimer les alias, choisissez Supprimer.

Activation d'une ressource

Par défaut, Amazon WorkMail crée une ressource. Si vous ou quelqu'un d'autre désactivez une ressource, vous pouvez la réactiver dans les 30 jours.

Pour activer une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation qui contient la ressource que vous souhaitez activer.
3. Dans le panneau de navigation, choisissez Resources (Ressources).
4. Dans la liste des ressources, sélectionnez le bouton à côté de la ressource que vous souhaitez activer, puis sélectionnez Activer.

   La boîte de dialogue Activer la ressource s'affiche.
5. Sélectionnez Activer.

Désactivation d'une ressource

Lorsque vous désactivez une ressource, vous la rendez indisponible pour la réservation. Par exemple, vous pouvez désactiver une salle de conférence pendant qu'elle est en cours de rénovation, puis activer la salle une fois qu'elle sera prête à être utilisée.

Pour désactiver une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation qui contient la ressource que vous souhaitez désactiver.
3. Dans le panneau de navigation, choisissez Resources (Ressources).
4. Dans la liste des ressources, sélectionnez le bouton à côté de la ressource que vous souhaitez désactiver, puis choisissez Désactiver.

   La boîte de dialogue Désactiver la ressource s'affiche.
5. Choisissez Désactiver.

Supprimer une ressource

Lorsque vous n'avez plus besoin d'une ressource, vous pouvez la supprimer. Cependant, vous devez d'abord désactiver la ressource. Pour plus d'informations sur la désactivation d'une ressource, consultez les étapes décrites dans la section précédente.

Pour supprimer une ressource

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations sur les régions, consultez la section Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis choisissez l'organisation souhaitée.
3. Dans le panneau de navigation, choisissez Resources (Ressources).
4. Dans la liste des ressources, sélectionnez le bouton à côté de la ressource désactivée que vous souhaitez supprimer, puis choisissez Supprimer.

   La boîte de dialogue Supprimer la ressource apparaît.
5. Dans la zone Entrez le nom de la ressource pour confirmer la suppression, entrez le nom de la ressource que vous souhaitez supprimer, puis choisissez Supprimer la ressource.

Travailler avec IAM Identity Center

Vous pouvez activer l'authentification multifactorielle (MFA) sur Amazon en WorkMail associant vos utilisateurs WorkMail Amazon à IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce qu'IAM Identity Center ?

Le tableau ci-dessous décrit les étapes à suivre pour aborder différents scénarios.

Scénario	Étapes
Associer des WorkMail utilisateurs Amazon à IAM Identity Center	1. Activation du centre d'identité IAM sur Amazon WorkMail 2. Affectation d'utilisateurs et de groupes IAM Identity Center à l'application Amazon WorkMail 3. Associer WorkMail les utilisateurs d'Amazon aux utilisateurs d'IAM Identity Center
WorkMail Utilisateurs Amazon existants	1. Créez des utilisateurs IAM Identity Center avec le même nom d'utilisateur, regroupez les utilisateurs et attribuez le groupe à l' WorkMail application Amazon. 2. Associez les WorkMail utilisateurs Amazon aux utilisateurs de l'IAM Identity Center.
Utilisateurs actuels de l'IAM Identity Center	1. Créez des WorkMail utilisateurs Amazon avec le même nom d'utilisateur que les utilisateurs d'IAM Identity Center. 2. Attribuez les utilisateurs ou les groupes IAM Identity Center à l' WorkMailapplication Amazon. 3. Associez les WorkMail utilisateurs Amazon aux utilisateurs d'IAM Identity Center.
Connexion d'un annuaire externe à IAM Identity Center	1. Synchronisez les utilisateurs de l'annuaire externe avec le groupe IAM Identity Center.

Scénario	Étapes
	Pour plus d'informations, consultez les didacticiels sur les sources d'identité d'IAM Identity Center 2. Attribuez le groupe IAM Identity Center à l' WorkMail application Amazon. 3. Connectez le répertoire externe à Amazon WorkMail et assurez-vous que les noms d'utilisateur correspondent 4. Associez les WorkMail utilisateurs Amazon aux utilisateurs de l'IAM Identity Center.

Une fois les étapes ci-dessus terminées, vous pouvez consulter l'état du centre d'identité IAM, le lien vers le centre d'identité AWS IAM pour gérer les utilisateurs et les groupes, l'URL de l'application Web WorkMail Amazon compatible MFA, le mode d'authentification, le statut du jeton d'accès personnel et la chronologie sous IAM Identity Center sous Paramètres de la console Amazon. WorkMail Pour plus d'informations sur la gestion de l'authentification multifacteur dans la console IAM Identity Center, voir Authentification multifactorielle pour les utilisateurs d'IAM Identity Center.

> **Note**
>
> Assurez-vous que la configuration entre Amazon WorkMail et IAM Identity Center est bien testée et vérifiée. Les utilisateurs risquent de perdre l'accès à leurs boîtes aux lettres si la configuration n'est pas correcte et complète.

Rubriques

Activation du centre d'identité IAM sur Amazon WorkMail

Lorsque vous activez IAM Identity Center, il agit comme une couche d'authentification pour les WorkMail utilisateurs d'Amazon. Les utilisateurs d'IAM Identity Center sont gérés séparément de l' WorkMail annuaire Amazon. Il est recommandé d'utiliser les mêmes noms d'utilisateur sur IAM Identity Center et Amazon. WorkMail

> **Note**
>
> Assurez-vous qu'Amazon WorkMail et IAM Identity Center sont installés dans la même région.

Pour activer IAM Identity Center, procédez comme suit.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Identity Center.

   La page Paramètres du centre d'identité IAM apparaît.
3. Sélectionnez Activer.

   La fenêtre Activer le centre d'identité IAM apparaît.
4. Sélectionnez Activer.

   La page Paramètres du centre d'identité apparaît avec l'état du centre d'identité affiché.
5. Pour ajouter des utilisateurs et des groupes IAM Identity Center à votre WorkMail organisation Amazon, suivez le lien sous État du centre d'identité. Pour plus d'informations sur la façon d'ajouter des utilisateurs et des groupes, voir Gérer les identités dans IAM Identity Center. .

Affectation d'utilisateurs et de groupes IAM Identity Center à l'application Amazon WorkMail

Lorsque vous activez IAM Identity Center dans Amazon WorkMail, vous WorkMail créez une application dans IAM Identity Center en votre nom. Par défaut, les utilisateurs d'IAM Identity Center doivent être affectés à cette application ou appartenir à un groupe affecté à cette application afin d'accéder à une boîte aux lettres de l' WorkMailorganisation Amazon. Pour plus d'informations, consultez la section Applications AWS gérées dans le Guide de AWS IAM Identity Center l'utilisateur.

Vous pouvez attribuer des utilisateurs et des groupes IAM Identity Center à Amazon de la WorkMail manière suivante :

- Par les utilisateurs d'IAM Identity Center : vous pouvez attribuer des utilisateurs d'IAM Identity Center à Amazon. WorkMail
- Par groupe IAM Identity Center : vous pouvez attribuer des groupes IAM Identity Center à Amazon. WorkMail En ajoutant un groupe, tous les utilisateurs d'un groupe auront accès à Amazon WorkMail.

  Pour plus d'informations sur l'ajout d'utilisateurs et de groupes, consultez Utilisateurs, groupes et approvisionnement dans IAM Identity Center.

> **Note**
>
> Si vous connectez votre source d'identité existante à IAM Identity Center, consultez les points suivants avant de modifier la source de votre répertoire.
>
> - Votre authentification est gérée par IAM Identity Center.
> - Amazon WorkMail conservera tous les WorkMail utilisateurs et groupes Amazon.
> - IAM Identity Center conservera tous les utilisateurs, groupes et attributions d'IAM Identity Center.
> - Vous devez gérer les WorkMail utilisateurs et les groupes Amazon dans WorkMail la console Amazon.
> - Vous devez gérer les utilisateurs et les groupes IAM Identity Center dans IAM Identity Center.
> - Les utilisateurs ne disposant pas d'une attribution ou d'une association d'utilisateurs IAM Identity Center ne peuvent pas accéder à Amazon WorkMail.

- Vous devez gérer les contrôles des politiques MFA dans IAM Identity Center.
- Lorsque vous modifiez la source du IAM Identity Center vers et depuis Manage Active Directory dans IAM Identity Center, vous devez désactiver les configurations IAM Identity Center existantes dans Amazon WorkMail et les reconfigurer pour associer vos WorkMail utilisateurs Amazon à IAM Identity Center.

Les utilisateurs et les groupes synchronisés avec votre annuaire IAM Identity Center peuvent être affectés à votre application Amazon WorkMail. Pour plus d'informations sur la gestion des utilisateurs et des groupes IAM Identity Center, voir Commencer les tâches courantes dans IAM Identity Center. .

Pour attribuer des utilisateurs et des groupes IAM Identity Center à Amazon WorkMail, procédez comme suit.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Identity Center.

   La page Paramètres du centre d'identité IAM apparaît.
3. Choisissez Assign users and groups (Attribuer des utilisateurs et des groupes).

   Vous pouvez ajouter et attribuer de nouveaux utilisateurs ou assigner des utilisateurs et des groupes existants.

   - Attribuer des utilisateurs : vous pouvez attribuer des utilisateurs individuels de l'IAM Identity Center à Amazon WorkMail. Vous pouvez créer un nouvel utilisateur IAM Identity Center ou rechercher un utilisateur existant.
   - Attribuer des groupes : vous pouvez également attribuer un groupe IAM Identity Center à Amazon WorkMail. Tous les membres du groupe seront ensuite affectés à Amazon WorkMail.

> **Note**
>
> Tous les nouveaux utilisateurs d'IAM Identity Center sont activés par défaut dans IAM Identity Center. Pour autoriser l'accès à Amazon WorkMail, vous devez définir leur mot de passe

dans IAM Identity Center et l'attribuer à Amazon WorkMail. Pour plus d'informations, voir Ajouter des utilisateurs à votre répertoire Identity Center.

Associer WorkMail les utilisateurs d'Amazon aux utilisateurs d'IAM Identity Center

Lorsqu'un utilisateur se connecte au client WorkMail Web Amazon avec ses informations d'identification utilisateur IAM Identity Center, le client ouvre la boîte aux lettres de l' WorkMail utilisateur Amazon associé. Si aucun utilisateur de l' WorkMailorganisation n'est associé à l'utilisateur IAM Identity Center, une association WorkMail sera créée entre l'utilisateur IAM Identity Center qui se connecte et l' WorkMail utilisateur ayant le même nom d'utilisateur, si un tel WorkMail utilisateur existe. Dans le cas contraire, le client affichera un message d'erreur à l'attention de l'utilisateur.

> **Note**
>
> Il est recommandé d'utiliser le même nom d'utilisateur pour un utilisateur sur Amazon WorkMail et IAM Identity Center, car l'association WorkMail sera créée automatiquement lorsque l'utilisateur se connectera pour la première fois au client WorkMail Web Amazon avec ses informations d'identification utilisateur IAM Identity Center. Lorsque les noms d'utilisateur sont différents, vous êtes responsable de créer l'association.

Pour associer des utilisateurs, procédez comme suit.

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Identity Center.

   La page Paramètres du centre d'identité IAM apparaît.
3. Choisissez Associer des utilisateurs.
4. Sous Sélectionnez un WorkMail utilisateur, sélectionnez l' WorkMail utilisateur Amazon que vous souhaitez associer.

5. Sous Entrez l'ID utilisateur IAM Identity Center, entrez l'ID de l'utilisateur IAM Identity Center que vous souhaitez associer. Vous pouvez copier l'identifiant depuis l'onglet Utilisateurs assignés de la page Identity Center.

   > **Note**
   >
   > L'utilisateur de l'IAM Identity Center doit être autorisé à accéder à l' WorkMail application Amazon.

6. Choisissez Associer des utilisateurs.

   Une fois l'association réussie, l' WorkMail utilisateur Amazon peut se connecter à Amazon à WorkMail l'aide des informations d'identification MFA IAM Identity Center.

> **Note**
>
> Vous pouvez également associer des WorkMail utilisateurs Amazon aux utilisateurs d'IAM Identity Center lorsque vous modifiez les informations WorkMail utilisateur Amazon. Pour de plus amples informations, veuillez consulter Modification des informations utilisateur.

Mode d’authentification

Vous pouvez utiliser le mode d'authentification pour permettre aux utilisateurs de se connecter en utilisant leurs informations d'identification d' WorkMailannuaire Amazon ou leurs informations d'identification IAM Identity Center, ou en limitant la connexion aux seules informations d'identification IAM Identity Center.

Deux modes d'authentification sont disponibles sur Amazon WorkMail.

> **Note**
>
> Le choix du mode d'authentification dépend des exigences de sécurité de votre organisation et des préférences en matière d'expérience utilisateur. Il est recommandé d'utiliser uniquement le mode IAM Identity Center, car il améliore la sécurité en renforçant les informations d'identification et le MFA d'IAM Identity Center. Toutefois, avant de passer du mode Amazon WorkMail Directory au mode IAM Identity Center, assurez-vous de tester le

processus MFA auprès de tous vos utilisateurs afin de garantir une transition fluide et d'éviter tout impact sur l'accès au client de messagerie existant.

- Amazon WorkMail Directory et IAM Identity Center (recommandé pour les tests) : il s'agit de l'option par défaut qui vous permet de tester les associations IAM Identity Center avant de passer en mode production. Le mode test permet aux utilisateurs de se connecter au client WorkMail Web Amazon en utilisant à la fois l' WorkMail annuaire Amazon et les informations d'identification du IAM Identity Center. Lorsque vous partagez l'URL de l'application WorkMail Web Amazon depuis les paramètres de l'organisation, votre utilisateur peut se connecter à l'aide de ses informations d'identification dans l' WorkMail annuaire Amazon. Lorsque vous partagez l'URL compatible MFA depuis les paramètres de l'IAM Identity Center, l'utilisateur peut se connecter à l'aide de ses informations d'identification IAM.
- IAM Identity Center uniquement (recommandé pour la production) : ce mode d'authentification vous permet uniquement de vous connecter à la boîte aux lettres du WorkMail client Amazon à l'aide des informations d'identification IAM Identity Center. Pour tous les WorkMail utilisateurs Amazon existants, les informations d'identification de l' WorkMailannuaire Amazon ne sont plus valides ni pour l'application WorkMail Web Amazon ni pour les clients de messagerie existants. Vous pouvez demander un jeton d'accès personnel pour accéder à la boîte aux lettres à l'aide de n'importe quel client de messagerie. Pour éviter de perdre l'accès aux boîtes aux lettres, assurez-vous que le MFA est activé pour tous les utilisateurs d'Amazon WorkMail .

Pour activer le mode d'authentification, procédez comme suit.

1. Sur la page Paramètres du centre d'identité, choisissez l'onglet Mode d'authentification.
2. Choisissez Modifier.

   La page Modifier le mode d'authentification apparaît.
3. Sélectionnez l’un des éléments suivants :

   - IAM Identity Center uniquement
   - Amazon WorkMail Directory et IAM Identity Center
4. Choisissez Enregistrer.

Configuration des jetons d'accès personnels

Vous pouvez activer le jeton d'accès personnel pour permettre aux WorkMail utilisateurs d'Amazon d'accéder à leurs boîtes aux lettres à l'aide de clients de messagerie de bureau et mobiles. Une fois le centre d'identité IAM activé, le statut du jeton d'accès personnel est défini par défaut sur actif et est valide pendant 365 jours. Après avoir activé IAM Identity Center, les informations d'identification existantes de vos utilisateurs ne seront plus valides pour se connecter à leurs clients de messagerie. Vos utilisateurs peuvent générer le jeton d'accès personnel depuis l'application WorkMail Web Amazon et l'utiliser pour se connecter à n'importe quel client de messagerie. Vous pouvez modifier l'expiration du jeton d'accès personnel et lorsque le jeton expire, votre utilisateur peut en générer un nouveau.

> **Note**
>
> - Votre utilisateur ne peut consulter et copier votre jeton d'accès personnel qu'une seule fois lorsque vous le créez sur Amazon WorkMail. Si vous perdez votre jeton d'accès personnel, vous devrez en générer un nouveau pour des raisons de sécurité.
> - Amazon WorkMail n'autorise les jetons d'accès personnels pour l'accès aux boîtes aux lettres que lorsque WorkMail l'utilisateur Amazon est associé à un utilisateur IAM Identity Center autorisé à accéder à l' WorkMailapplication Amazon.

Les configurations des jetons d'accès personnels sont répertoriées ci-dessous :

- Actif : lorsque le statut du jeton d'accès personnel est défini sur Actif, votre utilisateur peut générer un jeton d'accès personnel auprès d'Amazon WorkMail et l'utiliser pour se connecter à n'importe quel client de messagerie pendant la durée de vie du jeton.
- Inactif : lorsque le statut du jeton d'accès personnel est défini sur Inactif, votre utilisateur ne sera pas en mesure de générer ou d'utiliser des jetons d'accès personnels pour accéder aux boîtes aux lettres.
- Durée de vie du jeton — Par défaut, le jeton d'accès personnel est valide pendant 365 jours. Vous avez la possibilité de modifier la durée de vie du jeton d'accès personnel. Lorsque vous laissez le paramètre de durée de vie vide, le jeton aura une durée de vie indéfinie et n'expirera jamais.

Pour configurer des jetons d'accès personnels, procédez comme suit.

1. Sur la page Paramètres du centre d'identité, choisissez l'onglet Configuration du jeton d'accès personnel.
2. Choisissez Modifier.

   La page Modifier la configuration du jeton personnel apparaît.
3. Sous État du jeton, faites glisser le bouton Actif pour activer le jeton d'accès personnel.
4. Dans la zone de texte Durée de vie du jeton (en jours), entrez le nombre de jours pendant lesquels le jeton d'accès personnel peut être activé.
5. Choisissez Enregistrer.

Désactivation du centre d'identité IAM

Vous pouvez désactiver IAM Identity Center depuis la WorkMail console Amazon. Une fois désactivée, vous ne pouvez pas accéder à la boîte aux lettres à l'aide des informations d'identification IAM Identity Center ou des jetons d'accès personnels. Il est recommandé de réinitialiser tous les mots de passe utilisateur et les WorkMail utilisateurs Amazon recommenceront à utiliser les informations d'identification Amazon WorkMail Directory.

> **Note**
>
> Vérifiez les éléments suivants :
>
> - Après avoir désactivé IAM Identity Center, vos utilisateurs et groupes Amazon WorkMail et IAM Identity Center resteront inchangés.
> - Les associations d'utilisateurs existantes continueront d'exister.
> - Votre authentification sera à nouveau gérée par l' WorkMail annuaire Amazon, au lieu d'IAM Identity Center.

Pour désactiver IAM Identity Center, procédez comme suit.

1. Sur la page Paramètres du centre d'identité, choisissez Désactiver.

   La page Désactiver le centre d'identité IAM apparaît.
2. Choisissez Confirmer.

Travailler avec des appareils mobiles

Les rubriques de cette section expliquent comment gérer les appareils mobiles connectés à Amazon WorkMail.

Rubriques

Modification de la stratégie des dispositifs mobiles de votre organisation

Vous pouvez modifier la politique relative aux appareils mobiles de votre entreprise afin de modifier la façon dont les appareils mobiles interagissent avec Amazon WorkMail.

Pour modifier la stratégie de dispositif mobile de votre organisation

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la Région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Nom de la région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le panneau de navigation, sélectionnez Mobile Policies (Stratégies mobiles), puis sur l'écran Mobile policy (Stratégie mobile), choisissez Edit (Modifier).
4. Mettez à jour les informations suivantes si nécessaire :

   a. Require encryption on device (Exiger le chiffrement sur le dispositif) : Chiffre les données de messagerie sur le dispositif mobile.
   b. Require encryption on storage card (Exiger le chiffrement sur la carte de stockage) : Chiffre les données de messagerie sur le stockage amovible du dispositif mobile.

c. Mot de passe requis : nécessite un mot de passe pour déverrouiller un appareil mobile.

d. Autoriser le mot de passe simple : utilisez le code PIN de l'appareil comme mot de passe.

e. Longueur minimale du mot de passe : définissez le nombre de caractères requis pour un mot de passe valide.

f. Exiger un mot de passe alphanumérique : exige des mots de passe composés de lettres et de chiffres.

g. Nombre de tentatives infructueuses autorisées : Spécifiez le nombre de tentatives infructueuses de déverrouillage autorisées avant que l'appareil de l'utilisateur ne soit effacé. Toutes les données, y compris les fichiers personnels, seront supprimées lors de l'effacement de l'appareil.

h. Password expiration (Expiration du mot de passe) : Spécifie le nombre de jours avant qu'un mot de passe expire ou doive être modifié.

i. Enable screen lock (Activer l'écran de verrouillage) : Spécifie le nombre de secondes devant s'écouler sans interaction de la part de l'utilisateur avant de verrouiller l'écran.

j. Enforce password history (Appliquer l'historique des mots de passe) : Spécifie le nombre de mots de passe pouvant être saisis avant de répéter le même mot de passe.

5. Choisissez Enregistrer.

Gestion des appareils mobiles

Les rubriques de cette section expliquent comment effacer à distance les appareils mobiles, supprimer des appareils de votre organisation et consulter les détails des appareils. Pour plus d'informations sur la modification de la stratégie des appareils mobiles de votre organisation, consultez Modification de la stratégie des dispositifs mobiles de votre organisation.

Rubriques

- Effacement des appareils mobiles à distance
- Suppression d'appareils mobiles d'utilisateur de la liste des appareils mobiles
- Affichage des détails d'un dispositif mobile

Effacement des appareils mobiles à distance

Les étapes décrites dans cette section expliquent comment effacer à distance les appareils mobiles. Rappelez-vous ce qui suit :

- Les appareils doivent être en ligne et connectés à Amazon WorkMail. Si quelqu'un déconnecte l'appareil, l'opération d'effacement reprend lorsque l'utilisateur le reconnecte.
- Les opérations d'effacement peuvent prendre cinq minutes pour se propager.

> **Important**
>
> Sur la plupart des dispositifs mobiles, l'effacement à distance rétablit les paramètres d'usine du dispositif. Toutes les données, y compris les fichiers personnels, peuvent être supprimés lorsque vous effectuez cette procédure.

Pour effacer le dispositif mobile d'un utilisateur à distance

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la Région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez la section Nom de la région et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Utilisateurs, puis dans la liste des utilisateurs, sélectionnez le nom de l'utilisateur dont vous devez effacer l'appareil.
4. Choisissez l'onglet Appareils mobiles.
5. Dans la liste des appareils, cliquez sur le bouton situé à côté de l'appareil, puis sur Effacer.
6. Vérifiez le statut dans l'aperçu pour voir si l'effacement est demandé.
7. Une fois l'appareil effacé, supprimez-le de la liste des appareils. Les étapes décrites dans la section suivante expliquent comment procéder.

   > **Important**
   >
   > Pour réintégrer un appareil effacé dans la liste des appareils d'un utilisateur, assurez-vous de le supprimer d'abord de la liste des appareils. Dans le cas contraire, le système efface à nouveau l'appareil.

Suppression d'appareils mobiles d'utilisateur de la liste des appareils mobiles

Si quelqu'un cesse d'utiliser un appareil mobile en particulier, ou si vous avez effacé l'appareil à distance, vous pouvez le supprimer de la liste des appareils. Lorsque l'utilisateur reconfigure le dispositif, ce dernier apparaît dans la liste.

Pour supprimer des dispositifs mobiles d'utilisateur(s) de la liste des dispositifs mobiles

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la Région AWS. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez le nom de l'utilisateur.
4. Choisissez l'onglet Appareils mobiles.
5. Dans la liste des appareils, sélectionnez le bouton situé à côté de l'appareil et choisissez Supprimer.

Affichage des détails d'un dispositif mobile

Vous pouvez consulter les détails de l'appareil mobile d'un utilisateur.

> **Note**
>
> Certains appareils n'envoient pas toutes leurs informations au serveur. Il se peut que vous ne voyiez pas tous les détails de l'appareil disponible.

Pour afficher les détails du dispositif

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. À partir de la barre de navigation, sélectionnez la région répondant à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez l'onglet Appareils mobiles.
4. Dans la liste des appareils, sélectionnez l'identifiant de l'appareil dont vous souhaitez consulter les détails.

   Le tableau suivant répertorie les codes d'état des appareils.

Statut	Description
`PROVISIONING_REQUIRED`	Un utilisateur ou un administrateur a demandé que l'appareil soit configuré pour être utilisé avec Amazon WorkMail. Les appareils sont également définis sur ce statut si la politique actuelle pour cet appareil est modifiée dans la WorkMail console Amazon.
`PROVISIONING_SUCCEEDED`	L'appareil a été correctement approvisionné. L'appareil a appliqué la politique donnée.
`WIPE_REQUIRED`	Un administrateur a demandé un effacement de la WorkMail console Amazon.
`WIPE_SUCCEEDED`	Le périphérique a été effacé avec succès.

Gestion des règles d'accès aux appareils mobiles

Les règles d'accès aux appareils mobiles d'Amazon WorkMail permettent aux administrateurs de contrôler l'accès aux boîtes aux lettres pour certains types d'appareils mobiles. Par défaut, chaque WorkMail organisation Amazon utilise une règle qui accorde l'accès aux boîtes aux lettres à tous les appareils, quels que soient leur type, leur modèle, leur système d'exploitation ou leur agent utilisateur. Vous pouvez modifier ou remplacer cette règle par défaut par la vôtre. Vous pouvez également ajouter, modifier et supprimer des règles.

> **Warning**
>
> Si vous supprimez toutes les règles d'accès aux appareils mobiles d'une organisation, Amazon WorkMail bloque tous les accès aux appareils mobiles.

Vous pouvez créer des règles qui autorisent ou refusent l'accès en fonction des propriétés de l'appareil suivantes :

- Type d'appareil : « iPhone », « iPad » ou « Android ».
- Modèle d'appareil : « iPhone 10C1 », « iPad 5C1 » ou « X » HTCOne
- Système d'exploitation de l'appareil : « iOS 12.3.1 16F203 » ou « Android 8.1.0 ».
- Agent utilisateur de l'appareil : « iOS/14.2 (18B92) exchangesyncd/1.0 » ou « Android-Mail/7.7.16.163886392.release ».

Pour consulter les propriétés de l'appareil sur la console AWS de gestion, consultez la section Affichage des informations relatives aux appareils mobiles.

> **Note**
>
> Il est possible que certains appareils et clients ne signalent pas les propriétés de tous les champs. Pour plus d'informations sur la manière de contourner ces cas, voir Dealing with empty fields

> **Important**
>
> Les règles d'accès aux appareils WorkMail mobiles Amazon s'appliquent uniquement aux appareils utilisant le ActiveSync protocole Microsoft Exchange. Les clients mobiles qui utilisent un protocole différent, tel que IMAP, ne signalent pas les propriétés de l'appareil répertoriées ici. Ces règles ne s'appliquent donc pas.
> Si vous devez restreindre l'accès aux appareils utilisant d'autres protocoles, vous pouvez créer des règles de contrôle d'accès. Pour plus d'informations à leur sujet, consultez la section Utilisation des règles de contrôle d'accès. Par exemple, vous pouvez restreindre l'accès à d'autres protocoles et à la messagerie Web à un certain nombre d'adresses IP d'entreprise, mais autoriser Microsoft ActiveSync à utiliser d'autres adresses, puis utiliser

les règles d'accès aux appareils mobiles pour limiter davantage les types et les versions des clients autorisés.

Rubriques

Comment fonctionnent les règles d'accès aux appareils mobiles

Les règles d'accès aux appareils mobiles s'appliquent uniquement aux appareils utilisant le ActiveSync protocole Microsoft Exchange. Chaque règle comporte un ensemble de conditions qui spécifient le moment où la règle s'applique, ainsi qu'un effet d'accès de `ALLOW` ou `DENY` pour l'appareil. Une règle s'applique à une demande d'accès uniquement si toutes les conditions de la règle correspondent aux propriétés de l'appareil mobile de l'utilisateur. Des règles sans conditions s'appliquent à toutes les demandes. Chaque condition utilise une correspondance de préfixe sans distinction majuscules/majuscules par rapport aux propriétés signalées de l'appareil.

Amazon WorkMail évalue les règles comme suit :

- Si une `DENY` règle correspond à une propriété de l'appareil, la politique bloque l'appareil. `DENY`les règles ont priorité sur `ALLOW` les règles.
- Si au moins une `ALLOW` règle correspond et qu'aucune `DENY` règle ne correspond, la politique autorise l'appareil.
- Si aucune règle ne s'applique, l'appareil est bloqué.

Important

Les appareils mobiles indiquent les propriétés utilisées par les règles pour fonctionner. Les appareils signalent leurs propriétés au cours du processus de provisionnement des ActiveSync appareils Microsoft. Amazon WorkMail ne peut pas vérifier de manière indépendante que les clients mobiles fournissent des up-to-date informations correctes.

Utilisation des règles d'accès aux appareils mobiles

Vous pouvez utiliser APIs l'interface de ligne de commande (CLI) AWS pour créer et gérer les règles d'accès aux appareils mobiles. Pour plus d'informations à ce sujet AWS CLI, consultez le guide de l'utilisateur de l'interface de ligne de commande AWS.

> **Important**
>
> Lorsque vous modifiez une règle d'accès pour une WorkMail organisation Amazon, les appareils concernés peuvent mettre cinq minutes pour suivre la règle mise à jour, et les appareils peuvent présenter un comportement incohérent pendant cette période. Cependant, vous constatez immédiatement un comportement correct lorsque vous testez des règles. Pour de plus amples informations, veuillez consulter Testing mobile device access rules.

Répertorier les règles d'accès aux appareils mobiles

L'exemple suivant montre comment répertorier les règles d'accès des appareils mobiles.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Création de règles d'accès aux appareils mobiles

L'exemple suivant crée une règle qui empêche tous les appareils Android d'accéder aux boîtes aux lettres.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

L'exemple suivant crée une règle qui n'autorise qu'une version spécifique d'iOS. Assurez-vous de supprimer la `ALLOW-all` règle par défaut.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

Mise à jour des règles d'accès aux appareils mobiles

L'exemple suivant met à jour une règle de terminal en ajoutant un identifiant.

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

Supprimer une règle d'accès aux appareils mobiles

L'exemple suivant supprime la règle d'accès aux appareils mobiles avec l'identifiant donné.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Tester les règles d'accès aux appareils mobiles

Pour tester les règles d'accès, vous pouvez utiliser l'GetMobileDeviceAccessEffectAPI ou la commande get-mobile-device-access -effect du AWS CLI . Pour plus d'informations à ce sujet AWS CLI, consultez le Guide de l'utilisateur de l'interface de ligne de AWS commande.

Lorsque vous effectuez un test, vous transmettez les propriétés d'un appareil mobile simulé, et l'API ou la CLI renvoie l'effet d'accès DENY (ALLOWou) qu'un appareil mobile réel doté de ces propriétés recevrait. Par exemple, cette commande teste si un iPhone exécutant iOS 14.2, ainsi que l'application de messagerie par défaut, peut accéder à une boîte aux lettres.

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

Gérer les champs vides

Certains appareils mobiles ou clients peuvent ne pas fournir d'informations pour un ou plusieurs champs, laissant les valeurs vides. Les règles peuvent correspondre à celles de ces appareils en utilisant la valeur $NONE spéciale d'une condition. Par exemple, une règle avec DeviceTypes=["iphone", "ipad", "$NONE"] correspondra aux appareils qui signalent un type d'"iphone"appareil ou qui ne signalent aucun type d'appareil. "ipad"

Des conditions négatives telles que NotDeviceTypes ou NotDeviceUserAgents ne correspondront pas à ces valeurs vides. Par exemple, une règle avec

`NotDeviceTypes=["android"]` correspondra aux appareils qui signalent un type d'appareil autre que`"android"`. Toutefois, la règle ne s'appliquera pas aux appareils qui ne signalent aucun type d'appareil.

Gestion des annulations d'accès aux appareils mobiles

Vous utilisez les dérogations d'accès aux appareils mobiles pour annuler les résultats des règles d'accès aux appareils mobiles. Les dérogations s'appliquent à des utilisateurs et à des appareils spécifiques, et elles inversent la règle d'accès par défaut. Vous pouvez également utiliser des dérogations pour créer des exceptions ponctuelles aux règles d'accès et autoriser ou refuser des paires utilisateur/appareil spécifiques. En outre, vous pouvez utiliser des dérogations avec une règle d'accès pour appareils `DefaultDenyAll` mobiles. Cela permet de reporter les décisions d'accès à une solution de gestion des appareils mobiles (MDM) tierce. Pour plus d'informations, consultez Gestion des dérogations et Intégration aux solutions de gestion des appareils mobiles

Rubriques

- Comment fonctionnent les dérogations à l'accès aux appareils mobiles
- Gestion des dérogations

Comment fonctionnent les dérogations à l'accès aux appareils mobiles

Vous créez des dérogations d'accès aux appareils mobiles pour une paire utilisateur/appareil spécifique. La dérogation inverse le résultat d'accès par défaut lors de l'évaluation des règles d'accès aux appareils mobiles pour un utilisateur et un appareil donnés. Par exemple, si une règle d'accès refuse normalement l'accès, une dérogation d'accès permet à l'utilisateur et à l'appareil de synchroniser leurs e-mails. À l'inverse, si une règle d'accès autorise normalement l'accès, vous pouvez créer une dérogation qui empêche l'utilisateur et l'appareil de synchroniser leur courrier. Lorsque vous supprimez une dérogation d'accès à un appareil mobile, Amazon respecte WorkMail à nouveau le résultat des règles d'accès actuelles pour les appareils mobiles lorsqu'il décide d'accorder ou non l'accès à cet utilisateur et à cet appareil.

> **Important**
>
> Lorsque vous modifiez une dérogation d'accès aux appareils mobiles pour une WorkMail organisation Amazon, les appareils concernés peuvent mettre cinq minutes à suivre la modification de la dérogation.

Gestion des dérogations

Les dérogations d'accès aux appareils mobiles peuvent être créées, mises à jour ou supprimées à l'aide de l'API ou AWS Command Line Interface. Pour plus d'informations à ce sujet AWS CLI, consultez le guide de l'utilisateur de l'interface de ligne de commande AWS.

Pour trouver l'identifiant de l'appareil, utilisez le AWS Management Console. Pour plus d'informations, consultez la section Affichage des informations relatives aux appareils mobiles.

Répertorier les dérogations à l'accès aux appareils mobiles

Cet exemple montre comment répertorier toutes les dérogations d'accès aux appareils mobiles pour une WorkMail organisation Amazon spécifiée.

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

Création et mise à jour des dérogations d'accès aux appareils mobiles

Cela créera une dérogation d'accès aux appareils mobiles pour refuser l'accès à l' WorkMailorganisation, à l'utilisateur et à l'identifiant de l'appareil Amazon spécifiés.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

Une dérogation d'accès aux appareils mobiles existante peut être modifiée pour avoir un effet différent. Cela mettra à jour la dérogation d'accès aux appareils mobiles créée précédemment pour autoriser l'accès au lieu de le refuser.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

Supprimer les annulations d'accès aux appareils mobiles

Cela supprimera l'annulation de l'accès aux appareils mobiles pour l' WorkMail organisation, l'utilisateur et l'identifiant de l'appareil Amazon spécifiés.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

Intégration aux solutions de gestion des appareils mobiles

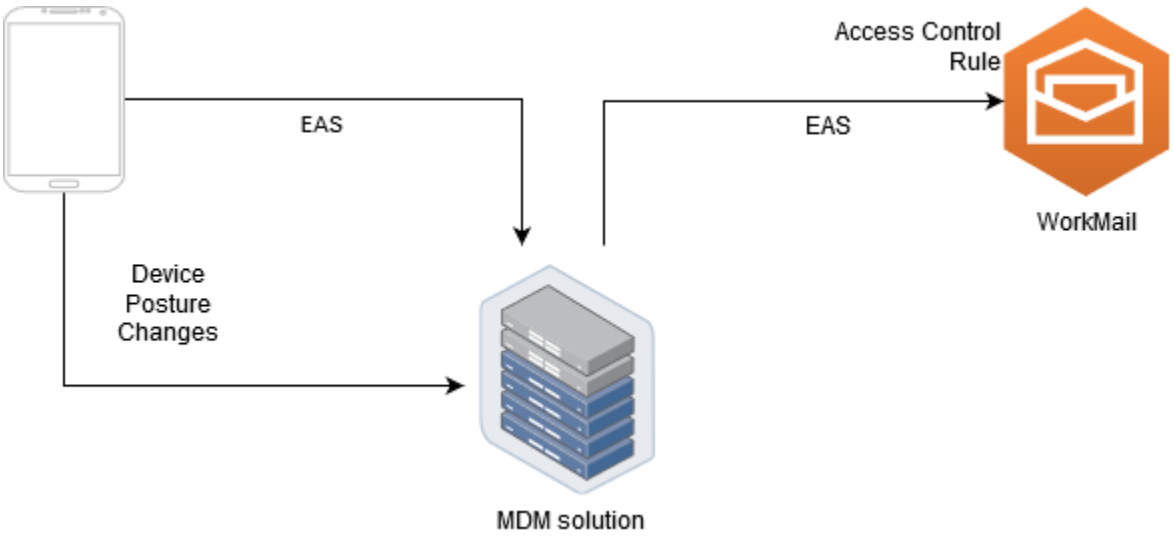
Amazon WorkMail prend en charge certaines fonctionnalités de base de gestion des appareils mobiles par le biais de politiques relatives aux appareils mobiles et de règles d'accès aux appareils mobiles. Cependant, ces fonctionnalités ne peuvent interagir avec les appareils mobiles que par le biais du protocole Microsoft Exchange ActiveSync (EAS), de sorte qu'elles ont une capacité limitée d'introspection et de renforcement de la posture de sécurité des appareils. Les administrateurs qui ont besoin d'un meilleur contrôle de la sécurité et de la conformité des appareils peuvent utiliser une solution tierce de gestion des appareils mobiles (MDM).

Présentation des solutions de gestion des appareils mobiles

Vous pouvez configurer votre solution MDM en deux modes, proxy ou direct. Consultez votre documentation MDM pour connaître les modes pris en charge par votre solution.

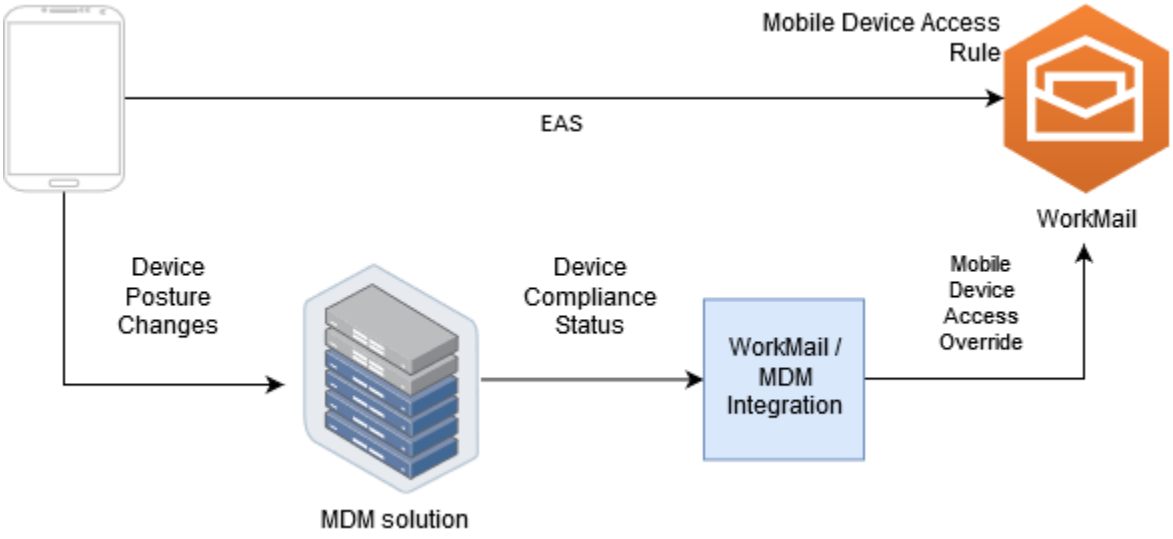
En mode proxy, les appareils mobiles utilisent le protocole Exchange Active Sync (EAS) via votre solution MDM pour accéder à Amazon WorkMail. La solution MDM utilise la position de l'appareil pour autoriser ou refuser l'accès aux WorkMail données Amazon. WorkMail Du côté d'Amazon, utilisez une règle de contrôle d'accès qui autorise l'accès EAS uniquement à partir de l'adresse ou des adresses IP de la solution MDM. Pour plus d'informations, reportez-vous à la section Utilisation des règles de contrôle d'accès.

L'image suivante montre une configuration typique du mode proxy.



En mode direct, les appareils mobiles utilisent EAS pour accéder WorkMail directement à Amazon. Votre solution MDM reçoit les changements de posture des appareils et évalue en permanence si chaque appareil répond à ces exigences. Lorsque la solution MDM détecte un changement de posture, comme la non-conformité d'un appareil, elle peut prendre plusieurs mesures et émet généralement des notifications ou des événements. Un WorkMail administrateur Amazon peut configurer un système pour écouter ces événements relatifs à l'état de conformité et créer automatiquement des dérogations d'accès aux appareils mobiles qui autorisent ou refusent l'accès aux appareils lorsqu'ils entrent ou ne sont pas conformes aux exigences des appareils MDM.

L'image suivante montre une configuration typique du mode direct.



Configuration d'une WorkMail organisation pour l'intégrer à une solution MDM tierce en mode direct

Pour intégrer une solution tierce de gestion des appareils mobiles (MDM) en mode direct, vous devez répondre aux exigences suivantes :

- Créez des règles de contrôle d'accès qui limitent l'accès aux appareils des utilisateurs au seul ActiveSync protocole.
- Créez une règle d'accès aux appareils mobiles deny-to-all « » par défaut pour garantir que tous les appareils mobiles inconnus ou non gérés sont refusés par défaut.
- Adoptez une solution de gestion des appareils mobiles qui émet des notifications ou des événements personnalisés lorsqu'un appareil change de posture de sécurité, ce qui signifie qu'il entre en conformité ou non.
- Créez un composant logiciel personnalisé pour écouter ces notifications et appelez le WorkMail SDK Amazon pour annuler l'accès aux appareils mobiles.

Ces composants garantissent que tous les appareils des utilisateurs répondent à leurs exigences de conformité MDM avant d'être autorisés à accéder à leurs WorkMail boîtes aux lettres Amazon.

Utilisez des règles de contrôle d'accès pour restreindre l'accès des appareils mobiles à ActiveSync

Vous devez vous assurer que tous les appareils utilisent uniquement le ActiveSync protocole, et vous pouvez utiliser les règles de contrôle d'accès pour ce faire. Par exemple, vous pouvez autoriser l'accès à d'autres protocoles de messagerie uniquement à partir d'une plage d'adresses IP internes à l'entreprise, puis autoriser uniquement ActiveSync lorsque vous accédez au courrier électronique depuis l'extérieur du pare-feu de l'entreprise. Vous devez le faire car cela vous ActiveSync permet uniquement d'identifier les appareils à l'aide d'un identifiant d'appareil. Vous ne pouvez pas utiliser de protocoles tels que le protocole IMAP (Internet Message Access Protocol) ou les services Web Exchange. Pour de plus amples informations, veuillez consulter Utilisation des règles de contrôle d'accès.

Créez une règle d'accès « refuser à tout » par défaut

Pour renvoyer toutes les décisions d'accès aux appareils mobiles à la solution de gestion des appareils mobiles tierce, créez une règle d'accès qui refuse automatiquement tous les appareils, sauf si elle est annulée par utilisateur ou par appareil. Pour plus d'informations, consultez Gestion des règles d'accès aux appareils mobiles.

Cet exemple montre une règle « refuser à tout ».

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Réagissez aux changements de posture de l'appareil et créez des annulations d'accès aux appareils mobiles

Vous devez configurer votre solution MDM pour envoyer des notifications en cas de modification de la position de l'appareil. Ces notifications doivent être consommées par un composant capable d'utiliser le WorkMail SDK Amazon pour créer ou mettre à jour les dérogations d'accès aux appareils mobiles. Par défaut, Amazon WorkMail refuse l'accès aux appareils non gérés ou récemment configurés en raison de la règle d'accès par défaut « refuser à tous » les appareils mobiles présentée plus haut dans cette rubrique. Lorsque la solution MDM détermine que l'appareil répond à toutes les exigences et émet une notification indiquant que l'appareil est conforme, ce composant peut réagir à cette notification en créant une dérogation d'accès au périphérique mobile avec un effet `ALLOW` pour l'utilisateur et l'appareil spécifiés. Si l'appareil n'est plus conforme par la suite, la solution de gestion des appareils mobiles émet une autre notification, et la dérogation d'accès peut être supprimée ou modifiée pour refuser l'accès à cet appareil. Pour de plus amples informations, veuillez consulter Gestion des annulations d'accès aux appareils mobiles.

Pour un exemple d' WorkMail intégration d'Amazon au MDM, consultez cet AWS exemple d'application.

Gestion des autorisations d'accès à une boîte aux lettres

Vous pouvez utiliser les autorisations de boîte aux lettres dans Amazon WorkMail pour accorder aux utilisateurs et aux groupes le droit de travailler dans les boîtes aux lettres d'autres utilisateurs. Les autorisations de boîte aux lettres s'appliquent à l'ensemble de la boîte aux lettres. Ils permettent à plusieurs utilisateurs d'accéder à la même boîte aux lettres sans partager les informations d'identification de cette boîte aux lettres. Les utilisateurs disposant d'autorisations sur une boîte aux lettres peuvent lire et modifier les données qu'elle contient et envoyer des e-mails à partir de la boîte aux lettres partagée.

> **Note**
>
> Les utilisateurs autorisés à accéder à une boîte aux lettres appartenant à un utilisateur masqué dans la liste d'adresses globale peuvent toujours accéder à la boîte aux lettres de l'utilisateur masqué.

La liste suivante présente les autorisations que vous pouvez accorder :

- Accès complet : permet un accès complet en lecture et en écriture à la boîte aux lettres, y compris les autorisations permettant de modifier les autorisations au niveau des dossiers.

  > **Note**
  >
  > Cette option n'est disponible que pour les utilisateurs. Les groupes ne peuvent pas bénéficier de droits d'accès complets.

- Envoyer au nom : permet à un utilisateur ou à un groupe d'envoyer des e-mails au nom d'un autre utilisateur. Le propriétaire de la boîte aux lettres apparaît dans l'en-tête From: (De :) et l'expéditeur apparaît dans l'en-tête Sender: (Expéditeur :).
- Envoyer en tant que : permet à un utilisateur ou à un groupe d'envoyer un e-mail en tant que propriétaire de la boîte aux lettres, sans indiquer l'expéditeur réel du message. Le propriétaire de la boîte aux lettres apparaît à la fois dans l'en-tête From: (De :) et dans l'en-tête Sender: (Expéditeur :).
- Aucun — Empêche un utilisateur ou un groupe d'envoyer des e-mails.

> **Note**
>
> Lorsque vous accordez des autorisations d'accès à une boîte aux lettres à un groupe, ces autorisations s'étendent à tous les membres de ce groupe, y compris les membres des groupes imbriqués.

Lorsque vous accordez des autorisations aux boîtes aux lettres, le WorkMail AutoDiscover service Amazon met automatiquement à jour l'accès à ces boîtes aux lettres pour les utilisateurs ou les groupes que vous avez ajoutés.

Pour le client Microsoft Outlook sous Windows, les utilisateurs ayant des autorisations d'accès complet peuvent automatiquement accéder aux boîtes aux lettres partagées. Attendez jusqu'à 60 minutes pour que les modifications se propagent, puis redémarrez Microsoft Outlook.

Pour l'application WorkMail Web Amazon et les autres clients de messagerie, les utilisateurs disposant d'autorisations d'accès complètes peuvent ouvrir manuellement les boîtes aux lettres partagées. Les boîtes aux lettres ouvertes restent ouvertes, même entre les sessions, sauf si l'utilisateur les ferme.

Rubriques

À propos des autorisations de boîte aux lettres et de dossiers

Les autorisations de boîte aux lettres s'appliquent à tous les dossiers d'une boîte aux lettres. Ces autorisations ne peuvent être activées que par le titulaire du AWS compte ou par un utilisateur IAM autorisé à appeler l'API de WorkMail gestion Amazon. Pour définir et modifier les autorisations pour les boîtes aux lettres ou pour les groupes dans leur ensemble, utilisez l'API AWS Management Console ou l' WorkMail API Amazon. Vous pouvez gérer jusqu'à 100 boîtes aux lettres et autorisations de groupe à partir de la console. Pour gérer les autorisations d'un plus grand nombre d'utilisateurs et de groupes, utilisez l' WorkMail API Amazon.

Les autorisations sur les dossiers s'appliquent uniquement à un seul dossier. Les utilisateurs finaux peuvent définir les autorisations relatives aux dossiers à l'aide d'un client de messagerie ou de

l'application WorkMail Web Amazon. Pour plus d'informations sur l'utilisation de l'application WorkMail Web Amazon pour partager des dossiers, consultez Partage de dossiers et autorisations de dossiers dans le guide de WorkMail l'utilisateur Amazon.

Gestion des autorisations de boîte aux lettres pour les utilisateurs

Vous pouvez utiliser la WorkMail console Amazon pour gérer les autorisations de boîte aux lettres pour les utilisateurs, ainsi que pour les groupes. Les sections suivantes expliquent comment gérer les autorisations des utilisateurs. Pour plus d'informations sur la gestion des autorisations pour les groupes, reportez-vous àGestion des autorisations de boîte aux lettres pour les groupes.

Rubriques

Ajout d'autorisations

Lorsque vous ajoutez des autorisations, vous accordez à un utilisateur le droit d'effectuer une ou plusieurs tâches dans la boîte aux lettres d'un autre utilisateur. Supposons par exemple que l'employé A doive envoyer des messages au nom de son supérieur, l'employé B. Pour accorder cette autorisation, vous devez accéder aux paramètres de la boîte aux lettres de l'employé B et accorder à l'employé A l'autorisation d'effectuer la tâche demandée.

Pour ajouter des autorisations aux boîtes aux lettres

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation pour laquelle vous souhaitez gérer les autorisations.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez le nom de l'utilisateur pour lequel vous souhaitez gérer les autorisations.
4. Choisissez l'onglet Autorisations, puis Add permissions (Ajouter des autorisations).

   La boîte de dialogue Ajouter des autorisations apparaît.

5. Ouvrez la liste Ajouter de nouvelles autorisations et sélectionnez l'utilisateur ou le groupe qui doit accéder à la boîte aux lettres.
6. Sous Autorisations de boîte aux lettres et Autorisations d'envoi, choisissez les options souhaitées.
7. Choisissez Ajouter.

Les nouvelles autorisations peuvent prendre jusqu'à cinq minutes pour être transmises aux utilisateurs.

Modification des autorisations de boîte aux lettres pour les utilisateurs

Lorsque vous modifiez les autorisations de boîte aux lettres d'un utilisateur, vous modifiez l'accès des autres utilisateurs à la boîte aux lettres de cet utilisateur. La modification des autorisations de boîte aux lettres ne modifie pas l'accès de l'utilisateur d'origine de la boîte aux lettres.

Pour modifier les autorisations d'accès à une boîte aux lettres

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation pour laquelle vous souhaitez gérer les autorisations.
3. Dans le volet de navigation, choisissez Utilisateurs, puis sélectionnez le nom de l'utilisateur dont vous souhaitez modifier les autorisations.
4. Sélectionnez l'onglet Autorisations.

   La liste des utilisateurs et des groupes ayant accès à la boîte aux lettres apparaît.
5. Sélectionnez le bouton radio à côté de l'utilisateur ou du groupe que vous souhaitez modifier, puis effectuez l'une des opérations suivantes :

   Pour supprimer les autorisations d'un utilisateur

   1. Sélectionnez Remove (Supprimer).

      La boîte de dialogue Supprimer les autorisations s'affiche.
   2. Dans la boîte de dialogue Supprimer les autorisations, choisissez Supprimer.

Pour modifier les autorisations d'un utilisateur

1. Choisissez Modifier.

   La boîte de dialogue Modifier les autorisations apparaît.
2. Définissez les autorisations nécessaires, puis choisissez Enregistrer.

Pour accorder à un autre utilisateur des autorisations d'accès à la boîte aux lettres

1. Choisissez Add permissions (Ajouter des autorisations).

   La boîte de dialogue Ajouter des autorisations apparaît.
2. Ouvrez la liste Ajouter de nouvelles autorisations et sélectionnez l'utilisateur que vous souhaitez ajouter.
3. Définissez les autorisations nécessaires, puis choisissez Ajouter.

Les modifications apportées aux autorisations peuvent prendre jusqu'à cinq minutes pour être transmises aux utilisateurs.

Gestion des autorisations de boîte aux lettres pour les groupes

Vous pouvez ajouter ou supprimer des autorisations de groupe pour Amazon WorkMail.

> **Note**
>
> Vous ne pouvez pas appliquer d'autorisations d'accès complet à un groupe, car les groupes n'ont pas de boîte aux lettres à laquelle accéder.

Pour gérer les autorisations de groupe

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la Région AWS case Dans la barre en haut de la fenêtre de la console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.

2. Dans le volet de navigation, choisissez Organizations, puis le nom de l'organisation pour laquelle vous souhaitez gérer les autorisations.
3. Dans le volet de navigation, choisissez Groupes, puis sélectionnez le nom du groupe pour lequel vous souhaitez définir des autorisations.
4. Choisissez l'onglet Autorisations, puis choisissez Ajouter des autorisations.

   La boîte de dialogue Ajouter des autorisations apparaît.
5. Ouvrez la liste Ajouter de nouvelles autorisations et sélectionnez l'utilisateur ou le groupe auquel accorder des autorisations pour la boîte aux lettres.
6. Sous Autorisations de boîte aux lettres et Autorisations d'envoi, choisissez les options souhaitées.
7. Choisissez Ajouter.

Les modifications apportées aux autorisations peuvent prendre jusqu'à cinq minutes pour être transmises aux utilisateurs.

Accès programmatique aux boîtes aux lettres

Pour accéder par programmation aux WorkMail boîtes aux lettres Amazon, utilisez le protocole Exchange Web Services (EWS). Avec EWS, vous pouvez accéder à tous les types d'articles d'une boîte aux lettres. Voici quelques bibliothèques EWS que vous pouvez utiliser avec Amazon WorkMail :

- Java — API Java EWS
- .Net — API gérée EWS
- Python — Exchangelib

Amazon prend WorkMail également en charge les protocoles IMAP et SMTP, que vous pouvez utiliser pour envoyer et recevoir des e-mails. Vous pouvez voir les WorkMail protocoles URLs pris en charge par Amazon dans la section WorkMailPoints de terminaison et quotas Amazon.

Lorsque vous utilisez le protocole EWS, Amazon WorkMail prend en charge les méthodes d'authentification suivantes :

- Authentification de base — Avec l'authentification de base, vous entrez une adresse e-mail et un mot de passe.
- Rôles d'emprunt d'identité : avec les rôles d'emprunt d'identité, vous accédez aux boîtes aux lettres des utilisateurs sans saisir les informations d'identification de l'utilisateur.

Rubriques

Gestion des rôles d'usurpation d'identité

Avec les rôles d'usurpation d'identité, les administrateurs configurent l'accès par programmation aux boîtes aux lettres des utilisateurs sans saisir les informations d'identification de l'utilisateur. Les services et outils peuvent assumer un rôle d'usurpation d'identité pour effectuer des actions dans les boîtes aux lettres des utilisateurs. L'usurpation d'identité n'est prise en charge qu'avec le protocole EWS.

Présentation des rôles d'usurpation d'identité

Pour autoriser l'emprunt d'identité, les administrateurs doivent créer un rôle d'usurpation d'identité doté des propriétés suivantes :

- Type de rôle : choisissez Accès complet ou Lecture seule. Le type de rôle limite le type d'opérations qu'un rôle peut effectuer.
- Règles : liste de règles qui définissent les utilisateurs que le rôle d'usurpation d'identité peut emprunter.

Amazon WorkMail évalue les règles selon les conditions suivantes :

- Si une règle DENY correspond, la politique refuse l'usurpation d'identité. Les règles DENY ont priorité sur les règles ALLOW.
- Si au moins une règle ALLOW correspond et qu'aucune règle DENY ne correspond, la politique autorise l'usurpation d'identité.
- Si aucune règle ne s'applique, l'usurpation d'identité est refusée.

> **Note**
>
> Pour autoriser l'usurpation d'identité à tous les utilisateurs d'une WorkMail organisation Amazon, créez une règle avec l'effet ALLOW et sans conditions.

> **Warning**
>
> Vous devez créer des règles pour permettre à un rôle d'usurpation d'identité de se faire passer pour un utilisateur. Si vous ne spécifiez pas de règles, un rôle d'usurpation d'identité ne peut pas assumer les droits d'accès d'un utilisateur.

Une fois le rôle d'usurpation d'identité créé, vous pouvez l'utiliser pour accéder aux boîtes aux lettres des utilisateurs. Pour de plus amples informations, veuillez consulter Utilisation de rôles d'usurpation d'identité.

Considérations sur la sécurité

L'utilisation de rôles d'usurpation d'identité peut entraîner des problèmes de sécurité au sein de votre WorkMail organisation Amazon et. Compte AWS Voici certains des problèmes potentiels à prendre en compte lors de la création d'un rôle d'usurpation d'identité :

- Autorisations transitives : si l'utilisateur A a accès à la boîte aux lettres de l'utilisateur B et qu'un rôle d'emprunt d'identité est autorisé à se faire passer pour l'utilisateur A, ce rôle d'usurpation d'identité peut se faire passer pour les autorisations d'accès de l'utilisateur A et accéder à la boîte aux lettres B de l'utilisateur.
- Contrôle d'accès : vous pouvez utiliser des règles de contrôle d'accès pour limiter l'accès aux rôles d'usurpation d'identité. Pour de plus amples informations, veuillez consulter Utilisation des règles de contrôle d'accès.
- Politique IAM — Vous pouvez attribuer une `AssumeImpersonationRole` action à une WorkMail organisation Amazon et un rôle d'usurpation d'identité spécifiques en utilisant cette condition. `workmail:ImpersonationRoleId` Pour voir un exemple de politique IAM, consultezComment Amazon WorkMail travaille avec IAM.

Création de rôles d'usurpation d'identité

Vous pouvez créer des rôles d'usurpation d'identité depuis la console Amazon WorkMail .

Pour créer un rôle d'usurpation d'identité

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom de l'organisation.
3. Choisissez Rôles d'usurpation d'identité, puis choisissez Créer un rôle.
4. La boîte de dialogue Créer un rôle d'usurpation d'identité s'affiche. Sous Rôle, entrez les informations suivantes :

   - Nom — Entrez un nom unique pour le rôle d'usurpation d'identité.
   - Description (Facultatif) — Entrez une description pour le rôle d'usurpation d'identité.
   - Type de rôle : choisissez Lecture seule ou Accès complet.

5. Sous Règles, sélectionnez Ajouter une règle.
6. La boîte de dialogue Ajouter une règle apparaît. Entrez les informations suivantes :
   - Nom — Entrez un nom unique pour la règle.
   - Description (Facultatif) — Entrez une description pour la règle.
   - Sous Effet, choisissez Autoriser ou Refuser. Cela autorise ou refuse l'accès en fonction des conditions que vous sélectionnez à l'étape suivante.
   - (Facultatif) Sous cette règle :, choisissez Correspond aux demandes qui se font passer pour les utilisateurs sélectionnés pour inclure des utilisateurs spécifiques. Choisissez Correspond aux demandes qui se font passer pour des utilisateurs autres que les utilisateurs sélectionnés pour ajouter des utilisateurs autres que les utilisateurs sélectionnés.
7. Choisissez Ajouter une règle.

   > **Note**
   >
   > Les règles ne sont enregistrées que lorsque vous enregistrez le rôle correspondant.

8. Choisissez Créer un rôle.

Modification des rôles d'usurpation d'identité

Vous pouvez modifier les rôles d'usurpation d'identité depuis la console Amazon WorkMail .

Pour modifier un rôle d'usurpation d'identité

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom de l'organisation.
3. Choisissez les rôles d'usurpation d'identité.
4. Sélectionnez le nom du rôle d'usurpation d'identité que vous souhaitez modifier, puis choisissez Modifier.
5. La boîte de dialogue Modifier le rôle d'usurpation d'identité s'affiche. Sous Rôle, entrez les informations suivantes :

- Nom — Entrez un nom unique pour le rôle d'usurpation d'identité.
- Description (Facultatif) — Entrez une description pour le rôle d'usurpation d'identité.
- Type de rôle : pour accorder au rôle d'usurpation d'identité un accès en lecture seule à la boîte aux lettres d'un utilisateur, choisissez Lecture seule. Pour donner au rôle d'usurpation d'identité le droit de lire et de modifier des éléments dans la boîte aux lettres d'un utilisateur, choisissez Accès complet.

6. Sous Règles, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur Modifier.
7. La boîte de dialogue Modifier la règle apparaît. Entrez les informations suivantes :

- Nom — Modifiez le nom de la règle.
- Description (Facultatif) — Mettez à jour ou entrez une description pour la règle.
- Sous Effet, choisissez Autoriser pour autoriser l'accès lorsque les conditions définies dans les règles sont remplies. Pour refuser l'accès, choisissez Refuser.
- (Facultatif) Sous cette règle :, choisissez Correspond aux demandes qui se font passer pour les utilisateurs sélectionnés pour inclure des utilisateurs spécifiques. Choisissez Correspond aux demandes qui se font passer pour des utilisateurs autres que les utilisateurs sélectionnés pour ajouter des utilisateurs autres que les utilisateurs sélectionnés.

8. Choisissez Enregistrer.
9. Sélectionnez Enregistrer les modifications.

> **Important**
>
> Lorsque vous modifiez une règle d'usurpation d'identité, la mise à jour des boîtes aux lettres concernées peut prendre jusqu'à cinq minutes. Au cours du processus de mise à jour des règles, il est possible que vous observiez un comportement incohérent dans votre boîte aux lettres. Toutefois, si vous testez un rôle, Amazon WorkMail répond comme prévu en fonction de la règle mise à jour. Pour de plus amples informations, veuillez consulter Tester les rôles d'usurpation d'identité.

Tester les rôles d'usurpation d'identité

Vous pouvez tester un rôle d'usurpation d'identité depuis la console Amazon WorkMail .

Pour tester un rôle d'usurpation d'identité

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom de l'organisation.
3. Choisissez les rôles d'usurpation d'identité.
4. Sélectionnez le rôle d'usurpation d'identité que vous souhaitez tester.
5. Choisissez le rôle de test.
6. La boîte de dialogue Tester le rôle d'usurpation d'identité s'affiche. Sous Utilisateur cible, sélectionnez l'utilisateur pour lequel vous souhaitez tester l'accès par emprunt d'identité.
7. Sélectionnez Tester).

Supprimer des rôles d'usurpation d'identité

Vous pouvez supprimer un rôle d'usurpation d'identité depuis la console Amazon WorkMail .

Pour supprimer un rôle d'usurpation d'identité

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, changez la région. Dans la barre de navigation, choisissez la région qui répond à vos besoins. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis choisissez le nom de l'organisation.
3. Choisissez les rôles d'usurpation d'identité.
4. Sélectionnez le nom du rôle d'usurpation d'identité que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. La boîte de dialogue Supprimer le rôle apparaît. Pour confirmer la suppression, entrez le nom du rôle dans la boîte de dialogue et choisissez Supprimer.

Utilisation de rôles d'usurpation d'identité

Pour accéder aux données des boîtes aux lettres, utilisez l'action Amazon WorkMail API`AssumeImpersonationRole`. Pour plus de détails sur Amazon WorkMail APIs, consultez la référence des API.

`AssumeImpersonationRole`renvoie un`Token`. Cela `Token` doit être transmis dans les 15 minutes au protocole EWS via l'en-tête HTTP`Authorization`.

Les exemples suivants montrent comment utiliser les rôles d'usurpation d'identité avec le protocole EWS. Les constantes utilisées dans les exemples spécifient les détails suivants propres à votre organisation et à votre compte :

- *`WORKMAIL_ORGANIZATION_ID`*— ID d' WorkMail organisation Amazon
- *`IMPERSONATION_ROLE_ID`*— ID du rôle d'usurpation d'identité
- *`WORKMAIL_EWS_URL`*— Point de terminaison EWS disponible sur les WorkMail points de terminaison et quotas Amazon
- *`EMAIL_ADDRESS`*— Adresse e-mail de la boîte aux lettres de l'utilisateur

Example Java — API Java EWS

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
```

```
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net — API gérée EWS

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python — Exchangelib

```
import boto3

from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
```

```
        )["Token"]

    def __call__(self, r):
        r.headers["Authorization"] = "Bearer " + self.token
        return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(
    service_endpoint=WORKMAIL_EWS_URL,
    version=Version(build=EXCHANGE_2010_SP2),
    auth_type="ImpersonationRoleAuth"
)
ews_account = Account(
    config=ews_config,
    primary_smtp_address=EMAIL_ADDRESS,
    access_type=IMPERSONATION
)
```

Exportation du contenu d'une boîte

Utilisez l'action d'StartMailboxExportJobAPI dans le Amazon WorkMail API Reference pour exporter le contenu d'une WorkMail boîte aux lettres Amazon vers un compartiment Amazon Simple Storage Service (Amazon S3). Cette action exporte tous les e-mails et éléments de calendrier de la boîte aux lettres spécifiée vers un `.zip` fichier du compartiment Amazon S3, au format MIME. Les autres éléments, tels que les contacts et les tâches, ne sont pas exportés.

Le temps nécessaire à la fin de la tâche d'exportation de la boîte aux lettres dépend de la taille et du nombre d'éléments contenus dans la boîte aux lettres. Comme la tâche d'exportation de la boîte aux lettres s'étend sur une certaine période, elle ne représente pas un instantané du contenu de la boîte aux lettres à un moment précis. Pour connaître le statut d'une tâche d'exportation, utilisez les actions d'ListMailboxExportJobsAPI DescribeMailboxExportJobor dans le Amazon WorkMail API Reference.

Lorsqu'une tâche d'exportation de boîte aux lettres est terminée, le `.zip` fichier du compartiment Amazon S3 est chiffré à l'aide de la clé principale client AWS Key Management Service (CMKAWS KMS) symétrique () que vous fournissez. AWS KMSLe chiffrement étant intégré à Amazon S3, les données déchiffrées sont visibles par l'utilisateur qui les télécharge, tant que celui-ci a accès à la clé CMK. AWS KMS

Conditions préalables

Les conditions requises pour exporter le contenu d'une boîte aux lettres sont les suivantes :

- La capacité de programmer.
- Un compte d' WorkMail administrateur Amazon.
- Un compartiment Amazon S3 qui n'autorise pas l'accès public. Pour plus d'informations, consultez la section Utilisation d'Amazon S3 pour bloquer l'accès public dans le Guide de l'utilisateur d'Amazon Simple Storage Service et le Guide de l'utilisateur d'Amazon Simple Storage Service.
- Une AWS KMS CMK symétrique. Pour de plus amples informations, veuillez consulter Mise en route dans le Manuel du développeur AWS Key Management Service.
- Rôle Gestion des identités et des accès AWS (IAM) doté d'une politique autorisant l'écriture dans le compartiment Amazon S3 et le chiffrement des fichiers envoyés à l'aide de la clé CMK. AWS KMS Pour de plus amples informations, veuillez consulter Comment Amazon WorkMail travaille avec IAM.

Exemples de politiques IAM et création de rôles

L'exemple suivant montre une politique IAM qui accorde l'autorisation d'écrire dans le compartiment Amazon S3 et de chiffrer les fichiers envoyés avec le AWS KMS CMK. Pour utiliser cet exemple de stratégie dans la Exemple : exportation du contenu d'une boîte aux lettres procédure suivante, enregistrez la politique sous forme de fichier JSON avec un nom de fichier`mailbox-export-policy.json`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/S3-PREFIX*"
                }
```

```
            }
        }
    ]
}
```

L'exemple suivant montre une politique de confiance IAM attachée au rôle IAM que vous créez. Pour utiliser cet exemple de stratégie dans la Exemple : exportation du contenu d'une boîte aux lettres procédure suivante, enregistrez la politique sous forme de fichier JSON avec un nom de fichier`mailbox-export-trust-policy.json`.

Vous n'êtes pas obligé d'utiliser les `aws:SourceAccount` conditions `aws:SourceArn` et en même temps. Par exemple, vous pouvez supprimer `aws:SourceArn` de la politique si vous devez utiliser le même rôle pour exporter des messages provenant de différentes WorkMail organisations Amazon sous le même AWS compte. Pour plus d'informations sur les clés de condition, reportez-vous aux clés contextuelles de condition AWS globales dans le guide de l'utilisateur d'AWSIdentity and Access Management.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-
east-1:111122223333:organization/m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
```

```
}
```

Vous pouvez utiliser le AWS CLI pour créer le rôle IAM dans votre compte en exécutant les commandes suivantes.

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

Pour plus d'informations à ce sujetAWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Exemple : exportation du contenu d'une boîte aux lettres

Après avoir créé le rôle et les politiques IAM dans la section précédente, procédez comme suit pour exporter le contenu de votre boîte aux lettres. Vous devez disposer de votre identifiant d' WorkMailorganisation Amazon et de votre identifiant utilisateur (ID d'entité), auxquels vous pouvez accéder dans la WorkMail console Amazon ou à l'aide de l' WorkMail API Amazon.

Exemple : pour exporter le contenu d'une boîte aux lettres

1. Utilisez le AWS CLI pour démarrer la tâche d'exportation de la boîte aux lettres.

   ```
   aws workmail start-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --entity-
   id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
   arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
    arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-
   demo-bucket --s3-prefix S3-PREFIX
   ```

2. Utilisez le AWS CLI pour surveiller l'état des tâches d'exportation de boîtes aux lettres pour votre WorkMail organisation Amazon.

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

Vous pouvez également utiliser l'ID de tâche généré par la **`start-mailbox-export-job`** commande pour surveiller uniquement l'état de cette tâche d'exportation de boîte aux lettres.

```
aws workmail describe-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
```

Lorsque l'état de la tâche d'exportation de boîte aux lettres est COMPLETED, les éléments de boîte aux lettres exportés sont disponibles dans un `.zip` fichier du compartiment Amazon S3 spécifié.

Voici un exemple du journal de sortie de la boîte aux lettres exportée :

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableLes éléments ne sont pas pris en charge, tels que les notes et les contacts.

Considérations

Les considérations suivantes s'appliquent lors de l'exportation de tâches de boîte aux lettres pour Amazon WorkMail :

- Vous pouvez exécuter jusqu'à 10 tâches d'exportation de boîtes aux lettres simultanées pour une WorkMail organisation Amazon donnée.
- Vous pouvez exécuter une tâche d'exportation de boîte aux lettres pour une boîte aux lettres donnée jusqu'à une fois toutes les 24 heures.

- Les ressources suivantes doivent toutes se trouver dans la même AWS région :
  - WorkMail Organisation Amazon
  - AWS KMSCMK
  - Compartiment Amazon S3

Résolution des problèmes

Les rubriques de cette section expliquent comment résoudre les problèmes sur Amazon WorkMail.

Rubriques

Affichage des en-têtes d'e-mail

Les informations contenues dans les en-têtes des e-mails peuvent vous aider à résoudre les problèmes de messagerie courants des utilisateurs. Amazon vous WorkMail permet de consulter les informations d'en-tête de n'importe quel message.

Pour afficher les en-têtes des e-mails sur Amazon WorkMail

1. Dans l'application WorkMail Web Amazon, double-cliquez sur le message électronique pour l'ouvrir.
2. Choisissez les options du message (icône représentant un engrenage et une enveloppe) situées dans le coin supérieur droit du message, à côté de la date d'envoi.

Les en-têtes des e-mails apparaissent sous Internet Headers (En-têtes Internet).

Routage du courrier

Si un utilisateur cesse de recevoir des e-mails, il se peut que votre WorkMail organisation Amazon rencontre un problème de routage des e-mails. Les étapes décrites dans cette section expliquent les méthodes courantes de résolution des problèmes de livraison et de routage.

Problèmes liés au courrier entrant :

- Vérifiez l'enregistrement MX du domaine associé à votre WorkMail organisation Amazon. `WorkMail`doit être la seule entrée et doit avoir la priorité la plus basse. Plusieurs enregistrements MX peuvent entraîner la réception de messages par le mauvais service. Pour plus d'informations sur les enregistrements MX, consultezVérification des domaines.

- Vérifiez les paramètres DMARC (Domain-based Message Authentication, Reporting, and Conformance) de votre organisation dans la console Amazon. WorkMail Les enregistrements DMARC sont utilisés pour se protéger contre les attaques courantes, telles que l'usurpation d'identité ou le phishing, qui peuvent compromettre les informations d'identification du compte d'un utilisateur. Pour plus d'informations sur le DMARC, consultezApplication de stratégies DMARC sur les e-mails entrants.
- Vérifiez la règle d'envoi entrant d'Amazon Simple Email Service. Si la règle contient des actions autres qu'Amazon WorkMail, celles-ci peuvent échouer et empêcher Amazon WorkMail de recevoir des e-mails. Pour plus d'informations sur les règles d'Amazon SES, consultez l' WorkMail action Intégrer à Amazon dans le manuel Amazon Simple Email Service Developer Guide.
- Activez le suivi des messages sur Amazon WorkMail, puis consultez les journaux pour détecter les problèmes de livraison. Pour plus d'informations sur le suivi des messages, consultezActivation de l'enregistrement des événements par e-mail.

Problèmes liés au courrier sortant

- Assurez-vous que votre enregistrement SPF inclut Amazon SES. Consultez la page des domaines dans la WorkMail console Amazon pour vérifier. Pour plus d'informations sur le SPF, consultezAuthentification d'e-mails avec SPF.
- Assurez-vous qu'Amazon WorkMail est autorisé à utiliser le domaine. Si ce n'est pas le cas, ajoutez à nouveau le domaine. Ajout d'un domainedans ce guide, vous trouverez les étapes à suivre.

Utilisation de la journalisation des e-mails avec Amazon WorkMail

Vous pouvez configurer la journalisation afin d'enregistrer vos communications par e-mail à l'aide d'outils tiers intégrés d'archivage et de découverte électronique. Vous pouvez ainsi veiller à ce que les réglementations en matière de stockage des e-mails pour la protection de la confidentialité, le stockage des données et la protection des informations soient respectées.

Utilisation de la journalisation

Amazon WorkMail enregistre tous les e-mails envoyés à n'importe quel utilisateur de l'organisation spécifiée, ainsi que tous les e-mails envoyés par les utilisateurs de cette organisation. Une copie de tous les messages électroniques est envoyée à une adresse spécifiée par l'administrateur système, dans un format appelé`journal record`. Ce format est compatible avec les programmes de messagerie Microsoft. La journalisation des e-mails n'implique aucun coût supplémentaire.

Deux adresses e-mail sont utilisées pour la journalisation des e-mails : une adresse e-mail de journalisation et une adresse e-mail de rapport. L'adresse e-mail de journalisation est l'adresse d'une boîte aux lettres dédiée ou d'un appareil tiers intégré à votre compte, vers lequel(laquelle) les rapports de journalisation sont envoyés. L'adresse e-mail du rapport correspond à l'adresse de votre administrateur système, à laquelle les notifications des rapports de journal en échec sont envoyées.

Tous les enregistrements du journal sont envoyés à partir d'une adresse e-mail qui est automatiquement ajoutée à votre domaine et ressemble à ce qui suit.

```
amazonjournaling@yourorganization.awsapps.com
```

Aucune boîte aux lettres n'est associée à cette adresse, et vous ne pourrez pas en créer une avec ce nom ou cette adresse.

> **Note**
>
> ne supprimez pas l'enregistrement de domaine suivant de la console Amazon Simple Email Service (Amazon SES), sinon la journalisation des e-mails cessera de fonctionner.
>
> ```
> yourorganization.awsapps.com
> ```

Chaque e-mail entrant ou sortant génère un enregistrement journal, quel que soit le nombre de destinataires ou de groupes d'utilisateurs. Un e-mail qui ne parvient pas à générer un enregistrement de journal génère une notification d'erreur, qui est envoyée à l'adresse e-mail des rapports.

Pour activer la journalisation des e-mails

1. Ouvrez la WorkMail console Amazon à l'adresse https://console.aws.amazon.com/workmail/.

   Si nécessaire, modifiez la AWS région. Dans la barre en haut de la fenêtre de console, ouvrez la liste Sélectionnez une région et choisissez une région. Pour plus d'informations, consultez Régions et points de terminaison dans le Référence générale d'Amazon Web Services.
2. Dans le volet de navigation, choisissez Organizations, puis le nom de votre organisation.
3. Dans le volet de navigation, Paramètres de l'organisation, choisissez l'onglet Journalisation, puis sélectionnez Modifier.
4. Déplacez le curseur d'état de la journalisation sur la position activée.
5. dans le champ Adresse e-mail de journalisation, entrez l'adresse e-mail fournie par votre fournisseur de journalisation des e-mails.

   > **Note**
   >
   > Nous vous recommandons d'utiliser un fournisseur de journalisation dédié.
6. Dans l'adresse e-mail du rapport, entrez l'adresse de l'administrateur de messagerie.
7. Choisissez Enregistrer. Les modifications s'appliquent immédiatement.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à chaque version de l'Amazon WorkMail Administrator Guide. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Support pour la journalisation des audits	Les journaux d'audit peuvent être utilisés pour surveiller l'accès des utilisateurs aux boîtes aux lettres, vérifier les activités suspectes et déboguer les configurations des fournisseurs de contrôle d'accès et de disponibilité. Pour plus d'informations, consultez les sections Activation de la journalisation des audits et Journalisation et surveillance dans Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	20 mars 2024
Support du protocole TLS (Transport Layer Security)	Amazon WorkMail a interrompu le support pour Transport Layer Security (TLS) 1.0 et 1.1. Si vous utilisez TLS 1.0 ou 1.1, vous devez mettre à niveau la version TLS vers la version 1.2.	2 novembre 2023
Utilisateurs distants	Les utilisateurs distants sont des WorkMail utilisateurs Amazon hébergés en dehors de WorkMail l'organisation	18 septembre 2023

	Amazon ou hébergés sur un autre domaine de messageri e. Pour plus d'informations, consultez la section Utilisate urs du manuel Amazon WorkMail Administrator Guide.	
Accès programmatique aux boîtes aux lettres	Amazon propose WorkMail désormais des rôles d'usurpat ion d'identité pour accorder un accès programmatique aux boîtes aux lettres. Pour plus d'informations, consultez la section Accès programmatique aux boîtes aux lettres dans le manuel Amazon WorkMail Administrator Guide.	4 octobre 2022
Configurer des fournisseurs de disponibilité personnalisés sur Amazon WorkMail	Amazon WorkMail prend en charge l'utilisation de fournisseurs de disponibilité personnalisés ()CAPs. Pour plus d'informations, consultez la section Configuration d'un fournisseur de disponibilité personnalisé dans le manuel Amazon WorkMail Administr ator Guide.	30 juin 2022
Modifications apportées à la console pour créer une organisation	L'expérience de WorkMail la console Amazon pour créer une organisation est mise à jour. Pour plus d'informations, consultez la section Création d'une organisation dans le manuel Amazon WorkMail Administrator Guide.	23 octobre 2020

Exportation du contenu d'une boîte	Utilisez l'action `StartMailboxExportJob` API pour exporter le contenu d'une WorkMail boîte aux lettres Amazon vers un compartiment Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez Exporter le contenu d'une boîte aux lettres dans le manuel Amazon WorkMail Administrator Guide.	22 septembre 2020
Règles de conservation des boîtes aux lettres	Définissez des politiques de conservation des boîtes aux lettres pour votre WorkMail organisation Amazon qui suppriment automatiquement les e-mails après une période de votre choix. Pour plus d'informations, consultez la section Définition des politiques de conservation des boîtes aux lettres dans le manuel Amazon WorkMail Administrator Guide.	28 mai 2020

Actions Run Lambda synchrones et asynchrones	Choisissez des configurations synchrones ou asynchron es pour exécuter les actions Lambda dans les règles de flux de messagerie Amazon WorkMail . Pour plus d'informa tions, consultez la section Configuration AWS Lambda pour Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	11 mai 2020
Utilisation des règles de contrôle d'accès	Les règles de contrôle d'accès permettent WorkMail aux administrateurs Amazon de contrôler la manière dont les boîtes aux lettres de leur organisation sont accessibl es. Pour plus d'informations, consultez la section Utilisation des règles de contrôle d'accès dans le manuel Amazon WorkMail Administrator Guide.	12 février 2020
Marquer une organisation	Marquez une WorkMail organisation Amazon pour différencier les organisations dans la AWS Billing and Cost Management console ou pour contrôler l'accès aux ressource s de l'organisation. Pour plus d'informations, consultez la section Marquage d'une organisation dans le manuel Amazon WorkMail Administr ator Guide.	23 janvier 2020

Appliquer les politiques DMARC aux e-mails entrants	Pour plus d'informations, consultez la section Appliquer les politiques DMARC aux e-mails entrants dans le manuel Amazon WorkMail Administrator Guide.	17 octobre 2019
Récupération du contenu des messages avec Lambda	Utilisez l'API Amazon WorkMail Message Flow AWS Lambda pour récupérer le contenu des messages. Pour plus d'informations, consultez la section Extraction du contenu des messages avec Lambda dans le manuel WorkMail Amazon Administrator Guide.	12 septembre 2019
Enregistrement des événements d' WorkMail e-mail Amazon	Activez la journalisation des événements par e-mail dans la WorkMail console Amazon pour suivre les e-mails de votre organisation. Pour plus d'informations, consultez la section Messages de suivi dans le manuel Amazon WorkMail Administrator Guide.	13 mai 2019

Insertion d'un enregistrement DNS Route 53	Lorsque vous configurez un domaine géré dans une zone hébergée publique Route 53, Amazon insère WorkMail automatiquement les enregistrements DNS pour vous. Pour plus d'informations, consultez la section Ajouter un domaine dans le manuel Amazon WorkMail Administrator Guide.	13 février 2019
Configuration de Lambda pour les actions relatives aux règles relatives aux e-mails entrants	Amazon WorkMail prend en charge la configuration des fonctions Lambda à utiliser avec les règles de flux de courrier entrant. Pour plus d'informations, consultez la section Gestion des flux d'e-mails dans le manuel Amazon WorkMail Administrator Guide.	24 janvier 2019
Configuration de Lambda pour Amazon WorkMail	Amazon WorkMail prend en charge la configuration des fonctions Lambda à utiliser avec les règles de flux de courrier sortant. Pour plus d'informations, consultez la section Configuration de Lambda pour Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	19 novembre 2018

Routage SMTP	Amazon WorkMail prend en charge la configuration des passerelles SMTP à utiliser avec les règles de flux de courrier sortant. Pour plus d'informations, consultez la section Configuration des passerelles SMTP dans le manuel Amazon WorkMail Administrator Guide.	1er novembre 2018
Outils de débogage pour les domaines personnalisés	Amazon WorkMail a ajouté des outils de débogage pour les domaines personnalisés. Pour plus d'informations, consultez la section Ajouter un domaine dans le manuel Amazon WorkMail Administrator Guide.	15 octobre 2018
Support pour Outlook 2019	Amazon WorkMail prend en charge Outlook 2019 pour Windows et macOS. Pour plus d'informations, consultez la configuration WorkMail requise pour Amazon dans le manuel Amazon WorkMail Administrator Guide.	1 octobre 2018
Diverses mises à jour	Diverses mises à jour apportées à la mise en page et l'organisation des rubriques.	12 juillet 2018

Autorisations relatives aux boîtes	Vous pouvez utiliser les autorisations de boîte aux lettres dans Amazon WorkMail pour accorder à des utilisateurs ou à des groupes le droit de travailler dans les boîtes aux lettres d'autres utilisateurs. Pour plus d'informations, consultez la section Utilisation des autorisations de boîte aux lettres dans le manuel Amazon WorkMail Administrator Guide.	9 avril 2018
Support pour AWS CloudTrail	Amazon WorkMail est intégré à AWS CloudTrail. Pour plus d'informations, consultez la section Journalisation des appels d' WorkMail API Amazon AWS CloudTrail dans le manuel Amazon WorkMail Administrator Guide.	12 décembre 2017
Support pour les flux d'e-mails	Vous pouvez configurer des règles de flux de messagerie pour le traitement des messages entrants en fonction de l'adresse ou du domaine du destinataire. Pour plus d'informations, consultez la section Gestion des flux d'e-mails dans le manuel Amazon WorkMail Administrator Guide.	5 juillet 2017

Mises à jour de Quick Setup	Quick Setup crée désormais un WorkMail répertoire Amazon pour vous. Pour plus d'informations, consultez Configurer Amazon WorkMail avec Quick Setup dans le manuel Amazon WorkMail Administrator Guide.	10 mai 2017
Support pour un plus large éventail de clients de messagerie	Vous pouvez désormais utiliser Amazon WorkMail avec Microsoft Outlook 2016 pour Mac et les clients de messagerie IMAP. Pour plus d'informations, consultez la section Configuration requise pour Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	9 janvier 2017
Support pour la journalisation SMTP	Vous pouvez configurer la journalisation afin d'enregis trer vos communications par e-mail. Pour plus d'informations, consultez la section Utilisation de la journalisation des e-mails avec Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	25 novembre 2016

Support pour la redirection d'e-mails vers des adresses e-mail externes	Vous pouvez configurer des règles de redirection d'e-mails en mettant à jour la politique d'identité Amazon SES pour votre domaine. Pour plus d'informations, consultez Modifier les politiques d'identité de domaine dans le manuel Amazon WorkMail Administrator Guide.	26 octobre 2016
Support pour l'interopérabilité	Vous pouvez activer l'interopérabilité entre Amazon WorkMail et Microsoft Exchange. Pour plus d'informations, consultez Interopérabilité entre Amazon WorkMail et Microsoft Exchange dans le manuel Amazon WorkMail Administrator Guide.	25 octobre 2016
Disponibilité générale	Version de disponibilité générale d'Amazon WorkMail.	4 janvier 2016
Support pour la réservation de ressources	Prise en charge de la réservation de ressources, telles que des salles de réunion et des équipements. Pour plus d'informations, consultez la section Utilisation des ressources dans le manuel Amazon WorkMail Administrator Guide.	19 octobre 2015

Support pour l'outil de migration des e-mails	Support de l'outil de migration d'e-mails. Pour plus d'informations, consultez la section Migration vers Amazon WorkMail dans le manuel Amazon WorkMail Administrator Guide.	16 août 2015
Version préliminaire d'Amazon WorkMail	La version préliminaire d'Amazon WorkMail.	28 janvier 2015

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.