aws

Guide d’administration

Amazon Chime

Amazon Chime: Guide d’administration

Table of Contents

Vous devez être un administrateur système Amazon Chime pour effectuer les étapes décrites dans ce guide. Si vous avez besoin d'aide concernant le client de bureau, l'application Web ou l'application mobile Amazon Chime, consultez la section Obtenir de l'aide dans le guide de l'utilisateur Amazon Chime.

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.

Qu'est-ce Amazon Chime ?

Amazon Chime est un service de communication qui transforme les réunions en ligne grâce à une application sécurisée et complète. Amazon Chime fonctionne sur tous vos appareils afin que vous puissiez rester connecté. Vous pouvez utiliser Amazon Chime pour les réunions en ligne, les visioconférences, les appels et le chat. Vous pouvez également partager du contenu à l'intérieur et à l'extérieur de votre organisation. Amazon Chime est un service entièrement géré qui s'exécute en toute sécuritéAWS dans le cloud, ce qui évite au service informatique de déployer et de gérer des infrastructures complexes.

Pour plus d'informations, consultez Amazon Chime.

Présentation de l'administration

En tant qu'administrateur, vous utilisez la console Amazon Chime pour effectuer des tâches clés, telles que la création de comptes Amazon Chime et la gestion des utilisateurs et des autorisations. Pour accéder à la console Amazon Chime et créer un compte administrateur Amazon Chime, créez d'abord unAWS compte. Pour plus d'informations, veuillez consulter Conditions requises pour les administrateurs système Amazon Chime.

Comment démarrer

Après avoir terminéConditions requises pour les administrateurs système Amazon Chime, vous pouvez créer et configurer votre compte administratif Amazon Chime, puis y ajouter des utilisateurs. Choisissez les autorisations Pro ou De base pour vos utilisateurs.

Si vous êtes prêt à commencer maintenant, consultez le didacticiel suivant :

- Démarrer

Pour en savoir plus sur les accès et autorisations utilisateur, consultez Gestion des autorisations et des accès des utilisateurs. Pour plus d'informations sur les fonctionnalités accessibles par les utilisateurs disposant d'autorisations Pro et de base, consultez la section Plans et tarification.

Tarification

Amazon Chime propose une tarification basée sur l'utilisation. Vous payez uniquement pour les utilisateurs disposant d'autorisations Pro qui hébergent des réunions, et uniquement les jours où ces réunions sont hébergées. Les participants de la réunion et les utilisateurs de la messagerie instantanée ne sont pas facturés.

Il n'y a aucuns frais pour les utilisateurs avec des autorisations de base. Les utilisateurs de base ne peuvent pas héberger des réunions, mais ils peuvent participer aux réunions et utiliser la messagerie instantanée. Pour plus d'informations sur la tarification et les fonctionnalités accessibles par les utilisateurs disposant d'autorisations Pro et de base, consultez la section Plans et tarification.

Ressources

Pour plus d'informations sur Amazon Chime, consultez les ressources suivantes :

- Centre d'aide Amazon Chime
- Vidéos de formation Amazon Chime

Conditions requises pour les administrateurs système Amazon Chime

Vous devez disposer d'un AWS compte pour accéder à la console Amazon Chime et créer un compte administrateur Amazon Chime.

Création d'un compte Amazon Web Services

Avant de créer un compte administrateur pour Amazon Chime, vous devez d'abord créer un AWS compte. chime

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

   Lorsque vous vous inscrivez à un Compte 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. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

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

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif 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, accordez 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.

Connectez-vous en tant qu'utilisateur disposant 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 AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Pour plus d'informations sur la configuration de votre compte administrateur Amazon Chime, consultez. Démarrer

Démarrer

Le moyen le plus simple pour vos utilisateurs de démarrer avec Amazon Chime est de télécharger et d'utiliser la version Amazon Chime Pro gratuitement pendant 30 jours. Pour plus d'informations, consultez Télécharger Amazon Chime.

Acquisition Amazon Chime

Pour continuer à utiliser la version Amazon Chime Pro après la période d'essai gratuite de 30 jours, vous devez créer un compte administrateur Amazon Chime et y ajouter vos utilisateurs. Pour commencer, vous devez tout d'abord effectuer les Conditions requises pour les administrateurs système Amazon Chime, qui comprennent la création d'un compte AWS. Vous pouvez ensuite créer et configurer un compte administrateur Amazon Chime et y ajouter des utilisateurs en effectuant les tâches suivantes.

Tâches

- Étape 1 : Création d'un compte administrateur Amazon Chime
- Étape 2 (facultative) : Configuration des paramètres du compte
- Étape 3 : Ajout des utilisateurs à votre compte
- (Facultatif) Configuration des numéros de téléphone pour votre compte Amazon Chime

Étape 1 : Création d'un compte administrateur Amazon Chime

Après avoir exécutéConditions requises pour les administrateurs système Amazon Chime, vous pouvez créer un compte administrateur Amazon Chime.

Pour créer un compte administrateur Amazon Chime

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans la page Accounts (Comptes), choisissez New account (Nouveau compte).
3. Pour Nom du compte, entrez un nom de compte et choisissez Créer un compte.
4. (Facultatif) Choisissez de laisser Amazon Chime sélectionner laAWS région optimale pour vos réunions parmi toutes les régions disponibles, ou d'utiliser uniquement les régions que vous avez sélectionnées. Pour plus d'informations, veuillez consulter Gestion des paramètres de réunion.

Étape 2 (facultative) : Configuration des paramètres du compte

Par défaut, les nouveaux comptes sont créés en tant que comptes Équipe. Si vous préférez revendiquer un domaine et vous connecter à votre propre fournisseur d'identité, ou à Okta SSO, vous pouvez le convertir en compte Enterprise. Pour plus d'informations sur les types de compte Équipe et Entreprise, consultez Choisir entre un compte Amazon Chime Team ou un compte Enterprise.

Pour convertir un compte Team en compte Enterprise

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour Comptes, choisissez le nom du compte.
3. Pour Identité, choisissez Mise en route.
4. Suivez les étapes de la console pour demander votre domaine.
5. (Facultatif) Suivez les étapes de la console pour configurer votre fournisseur d'identité et votre groupe d'annuaires.

Pour plus d'informations sur la demande de domaines, consultez Revendication d'un domaine. Pour plus d'informations sur la configuration des fournisseurs d'identité, consultez Connexion à Active Directory et Connexion à Okta SSO.

Vous pouvez également autoriser ou désactiver les politiques relatives aux comptes pour certaines options, telles que le contrôle à distance des écrans partagés et la fonctionnalité Amazon Chime Call Me.

Pour configurer les stratégies de compte

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, choisissez le nom du compte à configurer.
3. Sous Settings (Paramètres), choisissez Meetings (Réunions).
4. Dans Policies (Stratégies), sélectionnez ou désactivez les options de stratégie de compte que vous souhaitez autoriser ou interdire.
5. Choisissez Change (Modifier).

Pour plus d'informations, veuillez consulter Gestion des paramètres de réunion.

Étape 3 : Ajout des utilisateurs à votre compte

Une fois votre compte Amazon Chime Team créé, invitez-vous, ainsi que vos utilisateurs, à le rejoindre. Si vous mettez à niveau votre compte vers un compte Entreprise, vous n'avez pas besoin d'inviter vos utilisateurs. Vous pouvez en revanche mettre à niveau vers un compte Entreprise et revendiquer votre domaine. Pour plus d'informations, veuillez consulter Étape 2 (facultative) : Configuration des paramètres du compte.

Pour ajouter des utilisateurs à votre compte Amazon Chime

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, choisissez le nom de votre compte.
3. Sur la page Users (Utilisateurs), choisissez Invite users (Inviter des utilisateurs).
4. Saisissez les adresses e-mail des utilisateurs à inviter, y compris la vôtre, puis choisissez Inviter les utilisateurs.

Les utilisateurs invités reçoivent des invitations par e-mail pour rejoindre le compte Amazon Chime Team que vous avez créé. Lorsqu'ils enregistrent leur compte utilisateur Amazon Chime, ils reçoivent des autorisations Pro par défaut et leur période d'essai de 30 jours prend fin. S'ils ont déjà créé un compte utilisateur Amazon Chime avec leur adresse e-mail professionnelle, ils peuvent continuer à utiliser ce compte. Ils peuvent également télécharger l'application client Amazon Chime à tout moment en choisissant Télécharger Amazon Chime et en se connectant à leur compte utilisateur.

Vous êtes facturé pour un utilisateur avec des autorisations Pro uniquement lorsqu'il héberge une réunion. Il n'y a aucuns frais pour les utilisateurs avec des autorisations de base. Les utilisateurs de base ne peuvent pas héberger des réunions, mais ils peuvent participer aux réunions et utiliser la messagerie instantanée. Pour plus d'informations sur les tarifs et les fonctionnalités auxquelles les utilisateurs disposant d'autorisations Pro et Basic peuvent accéder, consultez la section Forfaits et tarifs.

Pour modifier les autorisations des utilisateurs

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, choisissez le nom de votre compte.
3. Sur la page Utilisateurs, sélectionnez le ou les utilisateurs dont vous souhaitez modifier les autorisations.
4. Choisissez Actions utilisateur, Attribuer l'autorisation utilisateur.

5. Pour Autorisations, sélectionnez Pro ou De base.
6. Choisissez Attribuer.

Vous pouvez accorder à d'autres utilisateurs des autorisations d'administrateur et également contrôler leur accès à la console Amazon Chime pour votre compte. Pour plus d'informations, veuillez consulter Gestion des identités et des accès pour Amazon Chime.

(Facultatif) Configuration des numéros de téléphone pour votre compte Amazon Chime

Les options téléphoniques suivantes sont disponibles pour les comptes administratifs Amazon Chime :

Appels Amazon Chime

Permet à vos utilisateurs d'envoyer et de recevoir des appels téléphoniques et des SMS directement depuis Amazon Chime. Fournissez vos numéros de téléphone dans la console Amazon Chime ou insérez des numéros de téléphone existants. Attribuez les numéros de téléphone à vos utilisateurs Amazon Chime et accordez-leur les autorisations nécessaires pour envoyer et recevoir des appels téléphoniques et des SMS à l'aide d'Amazon Chime. Pour plus d'informations, consultez Gestion des numéros de téléphone dans Amazon Chime et Transfert de numéros de téléphone existants.

Connecteur Amazon Chime

Fournit un service de jonction SIP pour un système téléphonique existant. Importez des numéros de téléphone existants ou attribuez de nouveaux numéros de téléphone dans la console Amazon Chime. Pour plus d'informations, consultez la section Gestion des connecteurs vocaux Amazon Chime dans le guide d'administration du SDK Amazon Chime.

Gestion de vos comptes Amazon Chime

Vous pouvez utiliser Amazon Chime en tant qu'utilisateur individuel ou en tant que groupe sans administrateur. Mais si vous souhaitez ajouter des fonctionnalités d'administrateur ou acheter Amazon Chime Pro, vous devez créer un compte Amazon Chime dans le. AWS Management Console Pour savoir comment créer un compte administrateur Amazon Chime ou pour plus d'informations sur l'achat d'Amazon Chime Pro, consultez. Démarrer

Pour plus d'informations sur les différents types de comptes d'administrateur Amazon Chime, consultez. Choisir entre un compte Amazon Chime Team ou un compte Enterprise Pour plus d'informations sur la gestion d'un compte administrateur existant, consultez les rubriques suivantes.

Rubriques

Choisir entre un compte Amazon Chime Team ou un compte Enterprise

Lorsque vous créez un compte administrateur Amazon Chime, vous choisissez de créer un compte d'équipe ou un compte d'entreprise. Pour plus d'informations sur la création d'un compte administrateur Amazon Chime, consultez. Démarrer

Compte d'équipe

Avec un compte Team, vous pouvez inviter des utilisateurs et leur accorder des autorisations Amazon Chime Pro sans revendiquer de domaine de messagerie. Pour plus d'informations sur les autorisations Pro et Basic, consultez la section Forfaits et tarifs.

Vous pouvez inviter des utilisateurs depuis n'importe quel domaine de messagerie qui n'a pas été revendiqué par une autre organisation. Vous payez uniquement pour les utilisateurs lorsqu'ils hébergent des réunions. Les utilisateurs de votre compte Team peuvent utiliser l'application Amazon Chime pour rechercher et contacter d'autres utilisateurs Amazon Chime enregistrés sur le même compte. Nous recommandons également un compte Team pour payer les utilisateurs Pro extérieurs à votre organisation.

Compte d'entreprise

Avec un compte Enterprise, vous avez un meilleur contrôle sur les utilisateurs des domaines de votre organisation. Vous pouvez choisir de vous connecter à votre propre fournisseur d'identité ou à Okta SSO pour vous authentifier et attribuer des autorisations Pro ou Basic. Amazon Chime prend également en charge Microsoft Active Directory.

Pour créer un compte Enterprise, vous devez revendiquer au moins un domaine de messagerie. Cela garantit que tous les utilisateurs qui se connectent à Amazon Chime à l'aide des domaines que vous revendiquez sont inclus dans votre compte Amazon Chime géré de manière centralisée. Les comptes d'entreprise sont nécessaires pour gérer vos utilisateurs via une intégration d'annuaire prise en charge. Pour plus d'informations, consultez Revendication d'un domaine et Connexion à Active Directory.

Vous pouvez également gérer l'activation et la suspension des utilisateurs depuis votre compte Enterprise. Pour plus d'informations, consultez Gestion des autorisations et des accès des utilisateurs.

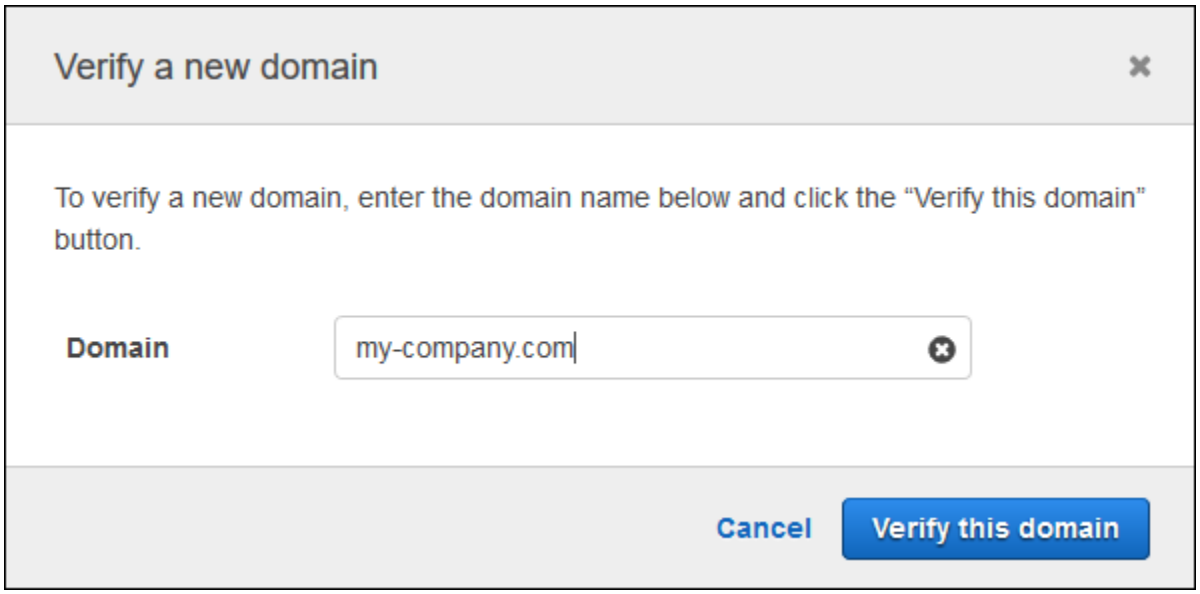
Revendication d'un domaine

Pour créer un compte d'entreprise et bénéficier d'un plus grand contrôle sur votre compte et sur les utilisateurs, vous devez revendiquer au moins un domaine de messagerie.

Pour demander un domaine

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

2. Sur la page Comptes , sélectionnez le nom d'un compte d'équipe.
3. Dans le panneau de navigation, choisissez Identity (Identité), Domains (Domaines).
4. Sur la page Domains (Domaines), choisissez Claim a new domain (Demander un nouveau domaine).
5. En regard de Domain (Domaine), saisissez le domaine que votre organisation utilise pour les adresses e-mail. Choisissez Verify this domain (Vérifier ce domaine).



6. Suivez les instructions à l'écran pour ajouter un enregistrement TXT au serveur DNS de votre domaine. En général, le processus implique de vous connecter au compte de votre domaine, de rechercher les enregistrements DNS de votre domaine et d'ajouter un enregistrement TXT avec le nom et la valeur fournis par Amazon Chime. Pour plus d'informations sur la mise à jour des enregistrements DNS de votre domaine, consultez la documentation relative à votre fournisseur DNS ou au serveur d'inscriptions de nom de domaine.

   Amazon Chime vérifie l'existence de cet enregistrement pour vérifier que vous êtes le propriétaire du domaine. Une fois le domaine vérifié, son état passe de Pending verification (Vérification en attente) à Verified (Vérifié).

   > **Note**
   >
   > La propagation de la modification et de la vérification du DNS par Amazon Chime peut prendre jusqu'à 24 heures.

7. Si votre organisation utilise des domaines supplémentaires ou des sous-domaines pour les adresses e-mail, répétez cette procédure pour chaque domaine.

Pour plus d'informations sur le dépannage des demandes de domaine, consultez Pourquoi ma demande de réclamation de domaine n'est elle pas en cours de vérification ?

Conversion d'un compte d'équipe en compte d'entreprise

Pour convertir un compte d'équipe existant en compte d'entreprise, revendiquez un ou plusieurs domaines de messagerie dans la console Amazon Chime. Pour plus d'informations sur les différences entre les comptes Team et Enterprise, consultezChoisir entre un compte Amazon Chime Team ou un compte Enterprise. Pour plus d'informations sur la réclamation d'un domaine, consultezRevendication d'un domaine.

Pour convertir un compte Team en compte Enterprise

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour Comptes, choisissez le nom du compte.
3. Pour Identité, choisissez Mise en route.
4. Suivez les étapes de la console pour demander votre domaine.
5. (Facultatif) Suivez les étapes de la console pour configurer votre fournisseur d'identité et votre groupe d'annuaires.

Une fois votre compte converti en compte Enterprise, vous pouvez décider de connecter ou non une instance Active Directory par le biais de ce compte AWS Directory Service. La connexion à une instance Active Directory permet à vos utilisateurs de se connecter à Amazon Chime à l'aide de leurs informations d'identification Active Directory. Pour plus d'informations, consultez Connexion à Active Directory.

Si vous ne vous connectez pas à une instance Active Directory, vos utilisateurs peuvent continuer à se connecter à Amazon Chime à l'aide de Login with Amazon (LWA) ou des informations d'identification de leur compte Amazon.com.

Attribution d'un nouveau nom à votre compte

Les étapes suivantes expliquent comment renommer l'équipe Amazon Chime et les comptes d'entreprise que vous administrez. Le nom que vous choisissez apparaît dans les e-mails qui invitent les utilisateurs à rejoindre Amazon Chime.

Pour renommer votre compte

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

   La page Comptes apparaît par défaut.
2. Dans la colonne Nom du compte, sélectionnez le compte que vous souhaitez renommer.
3. Dans le volet de gauche, sous Paramètres, sélectionnez Compte.

   La page récapitulative du compte apparaît.
4. Ouvrez la liste des actions du compte et choisissez Renommer le compte.

   La boîte de dialogue Renommer le compte apparaît.
5. Entrez le nouveau nom du compte et choisissez Enregistrer.

Suppression de votre compte

Si vous supprimez votre AWS compte dans le AWS Management Console, vos comptes Amazon Chime sont automatiquement supprimés. Vous pouvez également utiliser la console Amazon Chime pour supprimer un compte Amazon Chime Team ou Enterprise.

> **Note**
>
> Les utilisateurs qui ne sont pas gérés sur un compte Team ou Enterprise peuvent demander à être supprimés à l'aide de la commande « Deleme » d'Amazon Chime Assistant. Pour plus d'informations, consultez la section Utilisation de l'assistant Amazon Chime.

Pour supprimer un compte d'équipe

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sélectionnez le compte dans la colonne Account name (Nom de compte) et sélectionnez Account (Compte) sous Settings (Paramètres).
3. Dans le panneau de navigation, la page Users (Utilisateurs) s'affiche.
4. Sélectionnez les utilisateurs et choisissez User actions (Actions utilisateur), Remove user (Supprimer un utilisateur).
5. Dans le panneau de navigation, choisissez Accounts (Compte), Account actions (Actions de compte), puis Delete account (Supprimer le compte).

6. Confirmer que vous voulez supprimer votre compte.

Amazon Chime supprime toutes les données utilisateur lorsque vous supprimez votre compte. Cela inclut la résiliation d'un AWS compte, de comptes Amazon Chime individuels ou d'utilisateurs Amazon Chime non gérés. Cela exclut les données autres que le contenu liées aux comptes utilisateurs et à l'utilisation d'Amazon Chime (attributs de service couverts par le contrat client) qui sont générées par Amazon Chime.

Pour supprimer un compte d'entreprise

1. Supprimez les domaines.

> **Note**
>
> Lorsque vous supprimez un domaine, cela entraîne les actions suivantes :
>
> - Les utilisateurs associés au domaine sont immédiatement déconnectés de tous les appareils et perdent accès à tous les contacts, conversations instantanées et salles de conversation.
> - Les réunions planifiées par des utilisateurs de ce domaine ne sont plus lancées.
> - Les utilisateurs qui ont été interrompus continuent de s'afficher avec le statut Suspended (Interrompu) sur les pages Users (Utilisateurs) et User detail (Informations utilisateur) et ne peuvent pas accéder à leurs données. Ils ne peuvent pas créer de nouveaux comptes Amazon Chime avec leur adresse e-mail.
> - Les utilisateurs enregistrés continuent de s'afficher avec le statut Released (Enregistré) sur les pages Users (Utilisateurs) et User detail (Informations utilisateur) et ne peuvent pas accéder à leurs données. Ils peuvent créer un nouveau compte Amazon Chime avec leur adresse e-mail.
> - Si vous avez un compte Active Directory et que vous supprimez un domaine associé à l'adresse e-mail principale d'un utilisateur, celui-ci ne peut pas accéder à Amazon Chime et son profil est supprimé. Si vous supprimez un domaine associé à l'adresse e-mail secondaire d'un utilisateur, celui-ci ne peut pas se connecter avec cette adresse e-mail, mais il conserve l'accès à ses contacts et à ses données Amazon Chime.
> - Si vous possédez un compte Enterprise OpenID Connect (OIDC) et que vous supprimez un domaine associé à l'adresse e-mail principale d'un utilisateur, celui-ci ne peut plus accéder à Amazon Chime et son profil est supprimé.

2. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
3. Sur la page Comptes , sélectionnez le nom d'un compte d'équipe.
4. Dans le panneau de navigation, choisissez Settings (Paramètres), Domains (Domaines).
5. Sur la page Domains (Domaines), choisissez Remove domain (Supprimer un nouveau domaine).
6. Dans le panneau de navigation, choisissez Accounts (Compte), Account actions (Actions de compte), puis Delete account (Supprimer le compte).
7. Confirmer que vous voulez supprimer votre compte.

Amazon Chime supprime toutes les données utilisateur lorsque vous supprimez votre compte. Cela inclut la résiliation d'un AWS compte, de comptes Amazon Chime individuels ou d'utilisateurs Amazon Chime non gérés. Cela exclut les données autres que le contenu liées aux comptes utilisateurs et à l'utilisation d'Amazon Chime (attributs de service couverts par le contrat client) qui sont générées par Amazon Chime.

Gestion des paramètres de réunion

Gérez vos paramètres de réunion depuis la console Amazon Chime.

Paramètres de stratégie de réunion

Gérez les politiques de compte dans la console Amazon Chime sous Paramètres, Réunions. Choisissez l'une des options de stratégie suivantes.

Activer le contrôle partagé dans le partage d'écran

Indiquez si les utilisateurs de votre organisation peuvent accorder le contrôle partagé de leurs ordinateurs lors de réunions. Les participants qui demandent un contrôle partagé des ordinateurs de vos utilisateurs reçoivent un message d'erreur indiquant que le contrôle à distance n'est pas disponible.

Activer les appels sortants pour participer à des réunions

Active la fonction « Call me call me » d'Amazon Chime. Permet aux participants de rejoindre les réunions en recevant un appel téléphonique d'Amazon Chime.

Paramètres de l'application de réunion

Gérez l'accès aux applications de réunion sous Paramètres, Réunions dans la console Amazon Chime. Vous pouvez choisir les options suivantes :

Autoriser les utilisateurs à se connecter à Amazon Chime à l'aide de l'application Amazon Chime Meetings pour Slack

> Cette option permet aux utilisateurs de votre organisation de se connecter à Amazon Chime depuis l'application Amazon Chime Meetings pour Slack. Pour plus d'informations, consultez Configuration de l'application Amazon Chime Meetings pour Slack.

Paramètres de région des réunions

Pour améliorer la qualité des réunions et réduire le temps de latence, Amazon Chime traite les réunions dans la AWS région optimale pour tous les participants. Vous pouvez choisir de laisser Amazon Chime sélectionner la région optimale pour une réunion parmi toutes les régions disponibles ou d'utiliser uniquement les régions que vous sélectionnez.

Vous pouvez mettre à jour ce paramètre au moyen des paramètres de votre compte Meetings (Réunions) à tout moment. Dans les paramètres de vos réunions, vous pouvez également consulter le pourcentage de réunions Amazon Chime traitées dans chaque région.

Pour mettre à jour les paramètres de région de réunion

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Accounts (Comptes), sélectionnez le nom de votre compte.
3. Dans le panneau de navigation, choisissez Paramètres (Settings), Meetings (Réunions).
4. Pour Regions (Régions), choisissez l'une des options suivantes :
   - Utilisez toutes les régions disponibles pour garantir la qualité des réunions : permet à Amazon Chime d'optimiser le traitement des réunions pour vous.
   - Utiliser uniquement les régions que je sélectionne : vous permet de sélectionner des régions dans le menu déroulant.
5. Choisissez Enregistrer.

Gestion des stratégies de rétention des conversations instantanées

Si vous administrez un ou plusieurs comptes Amazon Chime Enterprise, vous pouvez définir des politiques de rétention des discussions pour les éléments suivants :

- Conversations par chat qui incluent uniquement les membres de votre compte Enterprise.
- Salons de discussion créés par les membres de votre compte Enterprise.

Une politique de rétention supprime automatiquement les messages en fonction de la période que vous avez définie. Vous pouvez définir des périodes allant d'un jour à 15 ans.

> **Note**
>
> Les comptes Amazon Chime Enterprise ont une période de conservation de 90 jours. La politique s'applique aux conversations impliquant des utilisateurs appartenant au compte et des utilisateurs n'appartenant pas au compte.
> Les stratégies de rétention ne s'appliquent pas aux éléments suivants :
>
> - Conversations par chat qui n'incluent pas les membres des comptes Amazon Chime Enterprise
> - Salons de discussion créés par des utilisateurs n'appartenant pas à un compte Amazon Chime Enterprise

Comment les politiques de rétention affectent les utilisateurs d'Amazon Chime

Les politiques de rétention définies par les administrateurs de comptes d'entreprise affectent différemment les utilisateurs d'Amazon Chime, selon qu'ils font partie du même compte d'entreprise, d'un autre compte d'entreprise, d'un compte d'équipe ou qu'ils ne sont membres d'aucun compte.

Conversations instantanées pour les membres d'un compte d'entreprise

Le tableau suivant montre comment les stratégies de rétention affectent les conversations instantanées pour les membres d'un compte d'entreprise.

Si la conversation instantanée inclut...	La stratégie de rétention est...
Uniquement les autres membres du compte d'entreprise de l'utilisateur	Définie par l'administrateur de l'utilisateur
Toute personne en dehors du compte d'entreprise de l'utilisateur	Définie automatiquement sur 90 jours

Salles de conversation pour les membres d'un compte d'entreprise

Le tableau suivant montre comment les stratégies de rétention affectent les salles de conversation pour les membres d'un compte d'entreprise.

Si la salle de conversation est créée par...	La stratégie de rétention est...
Membre du compte Entreprise de l'utilisateur	Définie par l'administrateur de l'utilisateur
Un autre membre du compte d'entreprise	Définie par l'administrateur de l'autre compte
Un membre d'un compte hors Entreprise	Ne s’applique pas

Conversations instantanées pour les membres d'un compte d'équipe

Le tableau suivant montre comment les stratégies de rétention affectent les conversations instantanées pour les membres d'un compte d'équipe.

Si la conversation instantanée inclut...	La stratégie de rétention est...
Uniquement les utilisateurs qui ne sont pas membres d'un compte d'entreprise	Ne s’applique pas
Au moins un membre d'un compte d'entreprise	Définie automatiquement sur 90 jours

Salles de conversation pour les membres d'un compte d'équipe

Le tableau suivant montre comment les stratégies de rétention affectent les salles de conversation pour les membres d'un compte d'équipe.

Si la salle de conversation est créée par...	La stratégie de rétention est...
Un utilisateur de compte d'équipe	Ne s’applique pas
Toute personne qui n'est pas membre d'un compte d'entreprise	Ne s’applique pas
Un membre d'un compte d'entreprise	Définie par l'administrateur du compte d'entreprise

Les utilisateurs d'Amazon Chime qui ne sont pas membres d'un compte Enterprise ou Team sont uniquement soumis aux politiques de rétention des forums de discussion créés par un membre d'un compte Enterprise.

Conversations instantanées avec des destinataires qui n'appartiennent pas à un compte d'entreprise ou d'équipe

Le tableau suivant montre comment les politiques de rétention affectent les conversations par chat pour les utilisateurs qui ne sont pas membres d'un compte Amazon Chime Enterprise ou Team.

Si la conversation instantanée inclut...	La stratégie de rétention est...
Uniquement les utilisateurs qui ne sont pas membres d'un compte d'entreprise	Ne s’applique pas
Au moins un membre d'un compte d'entreprise	Définie automatiquement sur 90 jours

Salles de conversation créées par des utilisateurs qui n'appartiennent pas à un compte d'entreprise ou d'équipe

Le tableau suivant montre comment les politiques de rétention affectent les forums de discussion pour les utilisateurs qui ne sont pas membres d'un compte Amazon Chime Enterprise ou Team.

Si la salle de conversation est créée par...	La stratégie de rétention est...
Un utilisateur qui n'est pas membre d'un compte d'entreprise ou d'équipe	Ne s’applique pas

Si la salle de conversation est créée par...	La stratégie de rétention est...
Un utilisateur de compte d'équipe	Ne s'applique pas
Un membre d'un compte d'entreprise	Définie par l'administrateur du compte d'entreprise

Activation de la rétention des conversations

Les administrateurs de comptes Amazon Chime Enterprise peuvent utiliser la console Amazon Chime pour activer la rétention des discussions pour les conversations et les forums de discussion sur leur compte. Vous pouvez également utiliser la console pour mettre à jour les périodes de rétention ou désactiver la rétention à tout moment.

Pour activer la rétention des conversations

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, sélectionnez le nom d'un compte.
3. Dans le volet de navigation, sous Paramètres, choisissez Rétention.
4. Sur la page Conservation, sous Conservation des conversations dans le chat, déplacez le curseur sur Activé.
5. Sous Période de conservation, entrez un nombre dans la première case, puis ouvrez la liste à côté de la case et choisissez Jours, semaines ou années.
6. Dans la section Rétention du salon de discussion, répétez les étapes 4 et 5. Lorsque vous avez terminé, choisissez Save (Sauvegarder).

Dans la journée qui suit la définition d'une période de rétention, les utilisateurs de votre compte perdent l'accès aux messages envoyés en dehors de la période de rétention.

Restaurer les messages de chat

> **Note**
>
> Vous devez être un administrateur de compte Amazon Chime Enterprise pour effectuer ces étapes.

Vous pouvez restaurer les messages de chat dans les 30 jours suivant la définition d'une période de rétention du chat. Lorsque vous restaurez les messages de chat, vous restaurez tous les messages envoyés par tous les utilisateurs de votre compte Amazon Chime.

Au cours de cette période de 30 jours, vous pouvez effectuer l'une des opérations suivantes pour restaurer les messages :

- Utilisez la console Amazon Chime pour désactiver la conservation des données.

  —OU—

- Prolongez la période de conservation.

Après la période de grâce de 30 jours, tous les messages de chat soumis à la période de conservation sont définitivement supprimés. Les nouveaux messages de chat sont définitivement supprimés dès qu'ils ont dépassé la période de conservation.

Pour plus d'informations sur la définition ou la modification d'une période de conservationActivation de la rétention des conversations, voir plus haut dans cette section.

Les messages de chat sont également définitivement supprimés d'Amazon Chime lorsque vous ou un membre du compte effectuez l'une des actions suivantes :

- Supprimer un salon de discussion Amazon Chime. Pour plus d'informations sur la suppression de salons de discussion, consultez la section Suppression de salons de discussion dans le guide de l'utilisateur d'Amazon Chime.
- Mettez fin à une réunion Amazon Chime dans laquelle des messages de chat sont présents.

> **Note**
>
> Si nécessaire, vous pouvez copier et enregistrer manuellement les messages de chat d'une réunion, mais vous devez le faire avant la fin de la réunion. Pour plus d'informations, consultez la section Utilisation du chat en réunion dans le guide de l'utilisateur d'Amazon Chime.

Supprimer des messages de chat

Conformément aux politiques de conservation des données, Amazon Chime conserve tous les messages de chat et empêche les utilisateurs finaux de supprimer les messages qu'ils envoient. Cependant, les administrateurs système Amazon Chime peuvent utiliser deux API pour supprimer des messages individuels des conversations et des forums de discussion. Les messages doivent se trouver sur le compte Amazon Chime de l'administrateur.

Les utilisateurs peuvent demander la suppression d'un message en vous envoyant un identifiant de message et un identifiant de conversation ou de salon de discussion correspondant. La rubrique Utilisation des fonctionnalités de chat, dans le guide de l'utilisateur d'Amazon Chime, explique comment procéder.

Lorsque vous recevez une demande de suppression, vous pouvez écrire du code ou utiliser la AWS CLI pour appeler les API suivantes.

Pour supprimer un message

- Effectuez l'une des actions suivantes :
  - Pour les messages de conversation : utilisez l'RedactConversationMessageAPI.

    Dans la CLI, exécutez la commande suivante :

    ```
    aws chime redact-conversation-message --conversation-id id_string --message-id id_string
    ```
  - Pour les messages du salon de discussion, utilisez l'RedactRoomMessageAPI.

    Dans la CLI, exécutez la commande suivante :

    ```
    aws chime redact-room-message --room-id id_string --message-id id_string
    ```

Connexion à Active Directory

Lorsque vous connectez votre compte administratif Amazon Chime à un Active Directory, vous pouvez bénéficier des fonctionnalités suivantes :

- Vos utilisateurs d'Amazon Chime peuvent se connecter à l'aide de leurs informations d'identification Active Directory.
- En tant qu'administrateur Amazon Chime, vous choisissez les fonctionnalités de sécurité des informations d'identification à ajouter, notamment la rotation des mots de passe, les règles de complexité des mots de passe et l'authentification multifactorielle.
- Lorsque vous supprimez des comptes utilisateurs de votre Active Directory, leurs comptes Amazon Chime sont également supprimés.
- Vous pouvez spécifier les groupes Active Directory qui reçoivent des autorisations Amazon Chime Pro.
  - Plusieurs groupes peuvent être configurés de façon à recevoir des autorisations Basic ou Pro.
  - Les utilisateurs doivent être membres de l'un ou l'autre des groupes pour se connecter à Amazon Chime.
  - Les utilisateurs des deux groupes reçoivent une licence Pro.

Pour plus d'informations sur la gestion des autorisations des utilisateurs, consultezGestion des autorisations et des accès des utilisateurs.

Prérequis

Avant de pouvoir vous connecter à votre Active Directory dans Amazon Chime, vous devez remplir les conditions préalables suivantes :

- Assurez-vous que vous disposez des AWS Identity and Access Management autorisations appropriées pour configurer les domaines, les annuaires actifs et les groupes d'annuaires. Pour plus d'informations, consultez Gestion des identités et des accès pour Amazon Chime.
- Créez un répertoire configuré dans la région USA Est (Virginie du Nord). AWS Directory Service Pour plus d'informations, consultez le Guide d'administration AWS Directory Service. Amazon Chime peut se connecter à l'aide d'AD Connector, de Microsoft AD ou de Simple AD.
- Réclamez un domaine afin de créer un compte Amazon Chime Enterprise ou de convertir votre compte Team existant en compte Enterprise. Si vos utilisateurs possèdent des adresses e-mail professionnelles provenant de plusieurs domaines, assurez-vous de revendiquer tous ces domaines. Pour plus d'informations, consultez Revendication d'un domaine et Conversion d'un compte d'équipe en compte d'entreprise.

Connexion à votre Active Directory dans Amazon Chime

Une fois que vous avez connecté votre Active Directory à Amazon Chime, vos utilisateurs sont invités à se connecter avec leurs informations d'identification d'annuaire lorsqu'ils utilisent une adresse e-mail provenant de l'un des domaines que vous avez revendiqués dans votre compte Amazon Chime Enterprise.

Pour vous connecter à votre Active Directory dans Amazon Chime

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, pour Identity, choisissez Active Directory.
3. Pour l'ID du répertoire Cloud, sélectionnez le AWS Directory Service répertoire à utiliser pour Amazon Chime, puis choisissez Connect.

   > **Note**
   >
   > Vous trouverez votre ID d'annuaire à l'aide de la console AWS Directory Service.

4. Une fois votre annuaire connecté, choisissez Ajouter un nouveau groupe.
5. Pour Groupe, entrez le nom du groupe. Le nom doit correspondre exactement à un groupe Active Directory dans l'annuaire cible. Les unités d'organisation Active Directory ne sont pas prises en charge.
6. Pour les autorisations, choisissez Basic ou Pro.
7. Choisissez Add Group (Ajouter un groupe).
8. (Facultatif) Répétez cette procédure pour créer des groupes de répertoires supplémentaires.

Configuration de plusieurs adresses e-mail

Une fois connectés à votre Active Directory dans Amazon Chime, les utilisateurs peuvent se connecter à Amazon Chime à l'aide de leurs informations d'identification Active Directory. Plusieurs adresses e-mail peuvent être attribuées à vos utilisateurs dans votre Active Directory. Pour permettre à vos utilisateurs de se connecter à Amazon Chime à l'aide de leurs informations d'identification Active Directory, vous devez revendiquer chaque domaine de messagerie applicable dans votre compte administratif Amazon Chime. Pour plus d'informations, consultez Revendication d'un domaine.

> **Note**
>
> Si vos utilisateurs tentent de se connecter à l'aide d'une adresse e-mail provenant d'un domaine non réclamé, ils sont invités à se connecter en utilisant Log in with Amazon. Ils ne sont pas en mesure de se connecter à votre compte administratif lorsqu'ils utilisent une adresse e-mail provenant d'un domaine non réclamé.

Lorsque vous consultez les détails de l'utilisateur dans la console Amazon Chime, Amazon Chime utilise l'adresse e-mail unique figurant dans `EmailAddress` l'attribut de votre Active Directory comme adresse e-mail principale de chaque utilisateur. Il s'agit de la seule adresse e-mail que vous pouvez voir pour l'utilisateur dans la console Amazon Chime. Toutefois, les utilisateurs peuvent se connecter avec toutes les adresses supplémentaires répertoriées dans l'`ProxyAddress`attribut, à condition que vous revendiquiez ces domaines dans votre compte Amazon Chime.

Exemple de configuration incorrecte

Un utilisateur dont le nom d'utilisateur est shirley.rodriguez est membre d'un compte Amazon Chime qui a revendiqué deux domaines : example.com et example.org. Dans Active Directory, cet utilisateur possède les trois adresses e-mail suivantes :

- Adresse e-mail principale : shirley.rodriguez@example.com
- Adresse e-mail déléguée 1 : shirley.rodriguez@example2.com
- Adresse e-mail du proxy 2 : srodriguez@example.org

Cet utilisateur peut se connecter à Amazon Chime en utilisant shirley.rodriguez@example.com ou srodriguez@example.org et shirley.rodriguez. S'ils tentent de se connecter en utilisant shirley.rodriguez@example2.com, ils sont invités à se connecter avec Amazon, et ils ne font pas partie de votre compte géré. C'est pourquoi il est important de revendiquer tous les domaines de messagerie de vos utilisateurs.

Les autres utilisateurs d'Amazon Chime peuvent ajouter cet utilisateur en tant que contact, l'inviter à des réunions ou l'ajouter en tant que délégué en utilisant l'adresse e-mail shirley.rodriguez@example.com ou srodriguez@example.org.

Exemple de configuration correcte

Un utilisateur dont le nom d'utilisateur est shirley.rodriguez est membre d'un compte Amazon Chime qui a revendiqué trois domaines : exemple.com, exemple2.com et exemple.org. Dans Active Directory, cet utilisateur possède les trois adresses e-mail suivantes :

- Adresse e-mail principale : shirley.rodriguez@example.com
- Adresse e-mail déléguée 1 : shirley.rodriguez@example2.com
- Adresse e-mail du proxy 2 : srodriguez@example.org

Cet utilisateur peut se connecter à Amazon Chime à l'aide de n'importe laquelle de ses adresses e-mail professionnelles. Les autres utilisateurs peuvent également les ajouter en tant que contact, les inviter à des réunions ou les ajouter en tant que délégués en utilisant l'une de leurs adresses e-mail professionnelles.

Connexion à Okta SSO

Si vous disposez d'un compte d'entreprise, vous pouvez vous connecter à Okta SSO pour vous authentifier et attribuer des autorisations utilisateur.

> **Note**
>
> Si vous devez créer un compte d'entreprise, qui vous permet de gérer tous les utilisateurs d'un ensemble donné de domaines d'adresses e-mail, consultez Revendication d'un domaine.

La connexion d'Amazon Chime à Okta nécessite la configuration de deux applications dans la console d'administration Okta. La première application est configurée manuellement et utilise OpenID Connect pour authentifier les utilisateurs auprès du service Amazon Chime. La deuxième application est disponible sous le nom d'Amazon Chime SCIM Provisioning dans le réseau d'intégration Okta (OIN). Il est configuré pour envoyer des mises à jour à Amazon Chime concernant les modifications apportées aux utilisateurs et aux groupes.

Pour vous connecter à Okta SSO

1. Créez l'application Amazon Chime (OpenID Connect) dans la console d'administration Okta :

1. Connectez-vous au tableau de bord d'administration d'Okta, puis choisissez Add Application (Ajouter une application). Dans la boîte de dialogue Create New Application (Créer une nouvelle application), choisissez Web, Next (Suivant).
2. Configurez les paramètres de l'application :
   a. Nom de l'application **`Amazon Chime`**.
   b. Pour Login Redirect URI (URI de redirection de connexion), entrez la valeur suivante : **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
   c. Dans la section Allowed Grant Types (Types d'autorisations admises), sélectionnez toutes les options pour les activer.
   d. Dans le menu déroulant Connexion initiée par, choisissez L'un ou l'autre (Okta ou application), puis sélectionnez toutes les options associées.
   e. Pour Initiate Login URI (URI de lancement de connexion), entrez la valeur suivante : **`https://signin.id.ue1.app.chime.aws/auth/okta`**
   f. Choisissez Enregistrer.
   g. Ne fermez pas cette page car vous aurez besoin, à l'étape 2, des informations relatives aux éléments suivants : Client ID (ID client), Client secret (Clé secrète du client) et Issuer URI (URI de l'émetteur).

2. Dans la console Amazon Chime, procédez comme suit :
   1. En haut de la page de configuration Okta Single-Sign On, choisissez Set up incoming keys (Configurer les clés entrantes).
   2. Dans la boîte de dialogue Setup incoming Okta keys (Configurer les clés entrantes Okta) :
      a. Collez les informations relatives au Client ID (ID client) et au Client secret (Clé secrète du client) depuis la page Okta Application Settings (Paramètres de l'application Okta).
      b. Collez l'Issuer URI (URI de l'émetteur) approprié depuis la page Okta API (API Okta). L'URI de l'émetteur doit être un domaine Okta, comme `https://example.okta.com`.
3. Configurez l'application Amazon Chime SCIM Provisioning dans la console d'administration Okta pour échanger certaines informations d'identité et d'appartenance à un groupe avec Amazon Chime :
   1. Dans la console d'administration Okta, choisissez Applications, Ajouter une application, recherchez Amazon Chime SCIM Provisioning et ajoutez l'application.

> **Important**
>
> Pendant la configuration initiale, choisissez les deux options Do not display application to users (Ne pas afficher l'application pour les utilisateurs) et Do not display application icon in the Okta Mobile App (Ne pas afficher l'icône de l'application dans l'application mobile Okta), puis choisissez Done (Terminé).

2. Dans l'onglet Provisioning (Mise en service), choisissez Configure API Integration (Configurer l'intégration d'API) et sélectionnez Enable API Integration (Activer l'intégration d'API). Ne fermez pas cette page car vous aurez besoin d'y copier une clé d'accès API à la prochaine étape.
3. Dans la console Amazon Chime, choisissez Create access key pour créer une clé d'accès API. Copiez-la dans le champ Okta API Token (Jeton d'API Okta) de la boîte de dialogue Configure API Integration (Configurer l'intégration d'API), et choisissez Test the Integration (Test de l'intégration), puis Save (Enregistrer).
4. Configurez les actions et les attributs qu'Okta utilisera pour mettre à jour Amazon Chime. Dans l'onglet Provisioning (Mise en service), dans la section To App (Dans l'application), choisissez Edit (Modifier), puis faites votre choix entre Enable Users (Autoriser les utilisateurs), Update User Attributes (Mettre à jour les attributs utilisateur) ou Deactivate Users (Désactiver les utilisateurs). Choisissez ensuite Save (Enregistrer).
5. Dans l'onglet Assignments (Affectations), accordez aux utilisateurs des autorisations dans la nouvelle application SCIM.

> **Important**
>
> Nous vous recommandons d'accorder des autorisations via un groupe contenant tous les utilisateurs qui devraient avoir accès à Amazon Chime, quelle que soit leur licence. Le groupe doit être identique à celui utilisé précédemment à l'étape 1 pour attribuer l'application OIDC présentée à l'utilisateur. Sinon, les utilisateurs finaux ne seront pas en mesure de se connecter.

6. Dans l'onglet Push Groups, configurez les groupes et les adhésions qui sont synchronisés avec Amazon Chime. Ces groupes permettent de faire la différence entre les utilisateurs Basic et les utilisateurs Pro.

4. Configurez les groupes de répertoires dans Amazon Chime :

1. Dans la console Amazon Chime, accédez à la page de configuration de l'authentification unique Okta.
2. Sous Directory groups (Groupes d'annuaires), choisissez Add new groups (Ajouter des groupes).
3. Entrez le nom d'un groupe de répertoires à ajouter à Amazon Chime. Le nom doit correspondre précisément à celui de l'un des Push Groups (Groupes Push) précédemment configurés à l'étape 3-f.
4. Choisissez si les utilisateurs de ce groupe doivent ou non bénéficier de capacités Basic ou Pro, puis sélectionnez Save (Enregistrer). Répétez cette procédure pour configurer d'autres groupes.

> **Note**
>
> Si vous recevez un message d'erreur indiquant que le groupe est introuvable, c'est peut-être parce que les deux systèmes n'ont pas terminé la synchronisation. Patientez quelques minutes, puis choisissez à nouveau Add new groups (Ajouter des groupes).

Le choix des fonctionnalités Basic ou Pro pour les utilisateurs de votre groupe d'annuaires a une incidence sur la licence, les fonctionnalités et le coût de ces utilisateurs dans votre compte Amazon Chime Enterprise. Pour plus d'informations, consultez Tarification d'.

Déploiement du complément Amazon Chime pour Outlook

Amazon Chime fournit deux compléments pour Microsoft Outlook : le complément Amazon Chime pour Outlook sous Windows et le complément Amazon Chime pour Outlook. Ces modules complémentaires offrent les mêmes fonctionnalités de planification, mais prennent en charge différents types d'utilisateurs. Les abonnés Microsoft Office 365 et les organisations utilisant Microsoft Exchange 2013 ou version ultérieure sur site peuvent utiliser le complément Amazon Chime pour Outlook. Les utilisateurs Windows disposant d'un serveur Exchange local exécutant Exchange Server 2010 ou une version antérieure et les utilisateurs d'Outlook 2010 doivent utiliser le complément Amazon Chime pour Outlook sous Windows.

Les utilisateurs de Windows qui ne sont pas autorisés à installer le complément Amazon Chime pour Outlook doivent opter pour le complément Amazon Chime pour Outlook sous Windows.

Pour en savoir plus sur quel module complémentaire est le mieux adapté pour vous et votre organisation, consultez Choisir le bon module complémentaire Outlook.

Si vous choisissez le complément Amazon Chime pour Outlook pour votre organisation, vous pouvez le déployer auprès de vos utilisateurs grâce à un déploiement centralisé. Pour plus d'informations, consultez le guide d'installation du complément Amazon Chime pour Outlook destiné aux administrateurs.

Configuration de l'application Amazon Chime Meetings pour Slack

Si vous utilisez Slack Enterprise Grid Organizations et que vous possédez ou administrez une organisation Slack, vous pouvez configurer l'application Amazon Chime Meetings pour Slack pour vos organisations. Si vous êtes administrateur d'un espace de travail Slack, vous pouvez configurer l'application Amazon Chime Meetings pour Slack pour vos espaces de travail.

Les étapes décrites dans les sections suivantes expliquent comment effectuer les deux types de configuration et comment effectuer des tâches supplémentaires telles que la migration d'un espace de travail vers une organisation.

Rubriques

Installation de l'application Amazon Chime Meetings pour Slack dans une organisation

L'installation de l'application Amazon Chime Meetings pour Slack dans une organisation Slack permet aux utilisateurs de démarrer des réunions et des appels instantanés avec d'autres utilisateurs dans les différents espaces de travail de cette organisation. Il permet également aux administrateurs d'espaces de travail d'installer automatiquement l'application Amazon Chime Meetings pour Slack Meetings sur tout nouvel espace de travail. Les étapes suivantes expliquent comment procéder.

> **Note**
>
> Les étapes suivantes supposent que vous êtes propriétaire ou administrateur d'une organisation et que vous pouvez vous connecter à la console de gestion Slack.

Pour configurer l'application Amazon Chime Meetings pour Slack dans une organisation

1. Dans le volet gauche de la console de gestion Slack, sélectionnez Apps.

   La page Applications apparaît et répertorie les applications installées par l'organisation, le cas échéant.
2. Choisissez Gérer les applications, situé dans le coin supérieur droit de la page, puis choisissez Installer une application.

   La boîte de dialogue Rechercher une application à installer apparaît.
3. Effectuez une recherche**`Amazon Chime Meetings`**, puis sélectionnez-la dans les résultats de recherche.

   La boîte de dialogue Ajouter des réunions Amazon Chime aux espaces de travail apparaît et répertorie les espaces de travail de l'organisation.
4. Choisissez le ou les espaces de travail sur lesquels vous souhaitez installer l'application Amazon Chime Meetings pour Slack.
5. Vous pouvez également choisir Par défaut pour le futur espace de travail si vous souhaitez installer automatiquement l'application Amazon Chime Meetings pour Slack dans tous les nouveaux espaces de travail, puis choisissez Next.

   La boîte de dialogue Vérifier les autorisations demandées par cette application apparaît et affiche les autorisations et les actions relatives à l'application Amazon Chime Meetings pour Slack.
6. Choisissez Suivant.
7. Si vous avez choisi d'installer l'application Amazon Chime Meetings pour Slack sur les nouveaux espaces de travail par défaut, choisissez Je suis prêt à définir cette application par défaut pour les futurs espaces de travail, puis cliquez sur Enregistrer. Dans le cas contraire, il vous suffit de sélectionner Enregistrer.

> **Note**
>
> Vous pouvez également utiliser OAuth pour installer des applications dans vos organisations. Pour plus d'informations, consultez la section Installation avec OAuth dans l'aide de Slack.

Installation de l'application Amazon Chime Meetings pour Slack sur les espaces de travail

L'installation de l'application Amazon Chime Meetings pour Slack sur un espace de travail permet aux utilisateurs de démarrer des réunions et des appels instantanés avec d'autres utilisateurs de cet espace de travail. Les utilisateurs n'ont pas besoin d'un profil utilisateur Amazon Chime pour utiliser l'application Amazon Chime Meetings pour Slack. Ils peuvent se connecter à l'aide de leur profil utilisateur Slack et lancer des appels ou des réunions à tout moment. Si les utilisateurs doivent organiser des réunions avec plusieurs autres personnes, vous devez configurer un compte Amazon Chime Team et accorder à ces utilisateurs supplémentaires des autorisations Pro. Pour plus d'informations sur le lancement d'appels et de réunions Amazon Chime, consultez la section Utilisation de l'application Amazon Chime Meetings pour Slack dans le guide de l'utilisateur Amazon Chime. Pour plus d'informations sur la configuration d'un compte Amazon Chime Team, consultez ce Associer des espaces de travail à des comptes Amazon Chime Team guide.

Pour installer l'application Amazon Chime Meetings pour Slack pour les espaces de travail Slack

1. Accédez à la liste des applications Slack et recherchez l'application Amazon Chime Meetings.
2. Choisissez Ajouter à Slack pour installer l'application Amazon Chime Meetings pour Slack depuis la liste des applications Slack.
3. Configurez le paramètre Appels de votre espace de travail Slack pour activer les appels dans Slack à l'aide d'Amazon Chime.

Migration des espaces de travail vers les organisations

Si vous possédez une organisation Slack, vous pouvez migrer des espaces de travail vers cette organisation. Pour plus d'informations sur la migration des espaces de travail, voir Migrer les espaces de travail vers Enterprise Grid dans l'aide de Slack.

Associer des espaces de travail à des comptes Amazon Chime Team

Associez votre espace de travail à un compte Amazon Chime Team pour gérer les autorisations de vos utilisateurs. Vous pouvez faire passer les organisateurs de réunions à Amazon Chime Pro afin qu'ils puissent démarrer des réunions avec un maximum de 250 participants et 25 vignettes vidéo, et inclure les numéros de téléphone à appeler pour l'audio. Attribuez aux utilisateurs des autorisations Amazon Chime Basic afin qu'ils puissent démarrer one-on-one des réunions ou participer à des réunions Amazon Chime. Pour plus d'informations, consultez la section Tarification d'Amazon Chime.

> **Note**
>
> Si vous associez un compte Amazon Chime Team à votre espace de travail Slack, les utilisateurs peuvent se connecter à Amazon Chime depuis l'application Amazon Chime Meetings pour Slack. Vous pouvez modifier ce paramètre à tout moment. Pour plus d'informations, consultez Gestion des paramètres de réunion.

Avant de pouvoir associer votre espace de travail Slack à un compte Amazon Chime Team, vous devez créer un AWS compte. Pour plus d'informations sur la création d'un AWS compte, consultezConditions requises pour les administrateurs système Amazon Chime.

Pour associer votre espace de travail Slack à un compte Amazon Chime Team lors de l'installation de l'application Amazon Chime Meetings pour Slack

1. Immédiatement après avoir installé l'application Amazon Chime Meetings pour Slack dans votre espace de travail Slack, choisissez Mettre à niveau maintenant.
2. Suivez les instructions pour vous connecter à la console Amazon Chime à l'aide des informations d'identification de AWS votre compte.
3. Suivez les instructions pour créer un nouveau compte d'équipe dans Amazon Chime ou choisissez-en un existant.

   - Créer un nouveau compte — Créez un nouveau compte Amazon Chime sur lequel vous pourrez inviter vos utilisateurs de Slack. Saisissez un nom de compte, indiquez si vous voulez inviter vos utilisateurs Slack, puis choisissez Create (Créer).
   - Choisissez un compte existant : sélectionnez un compte Amazon Chime existant pour y inviter les utilisateurs de Slack. Sélectionnez le compte, puis choisissez Invite (Inviter).

Lorsque vous invitez vos utilisateurs de Slack à rejoindre Amazon Chime, ils reçoivent une invitation par e-mail. Lorsqu'ils acceptent l'invitation, ils sont automatiquement mis à niveau vers Amazon Chime Pro.

Si vous n'avez pas associé votre espace de travail Slack à un compte Amazon Chime Team lorsque vous avez installé l'application Amazon Chime Meetings pour Slack, vous pouvez le faire après coup en suivant les étapes suivantes.

Pour associer votre espace de travail Slack à un compte Amazon Chime Team après avoir installé l'application Amazon Chime Meetings pour Slack

1. Connectez-vous à votre AWS compte.
2. Connectez-vous à votre espace de travail Slack en tant qu'administrateur.
3. Accédez à https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Suivez les instructions pour créer un nouveau compte d'équipe dans Amazon Chime ou choisissez un compte existant.

    - Créer un nouveau compte — Créez un nouveau compte Amazon Chime sur lequel vous pourrez inviter vos utilisateurs de Slack. Saisissez un nom de compte, indiquez si vous voulez inviter vos utilisateurs Slack, puis choisissez Create (Créer).
    - Choisissez un compte existant : sélectionnez un compte Amazon Chime existant pour y inviter les utilisateurs de Slack. Sélectionnez le compte, puis choisissez Invite (Inviter).

Gestion des utilisateurs

> **Note**
>
> Les étapes décrites dans cette section supposent que vous disposez d'un ensemble d'adresses e-mail d'utilisateurs ou que vous avez connecté votre compte administrateur à Active Directory. Pour plus d'informations, reportez-vous à Connexion à Active Directory ce guide.

Vous utilisez la console Amazon Chime pour ajouter et gérer des utilisateurs. Vous ajoutez des utilisateurs en les invitant. Lorsqu'ils acceptent vos invitations, ils apparaissent sous Utilisateurs, qui répertorie tous les utilisateurs de votre compte et leurs informations d'utilisateur. Pour plus d'informations, consultez Affichage des informations utilisateur.

Les administrateurs de comptes utilisant Login with Amazon (LWA) disposent également d'options permettant de gérer les niveaux d'autorisation et de supprimer des utilisateurs d'un compte. Ces actions sont gérées via Active Directory ou Okta, en fonction de celle que vous configurez pour le compte à utiliser. Pour plus d'informations, consultez Gestion des autorisations et des accès des utilisateurs.

Table des matières

Ajout d'utilisateurs

Vous ajoutez des utilisateurs à un compte Amazon Chime en les invitant à rejoindre le compte. Vous envoyez des invitations à des utilisateurs potentiels depuis la console Amazon Chime, et ces étapes expliquent comment procéder.

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

   La liste des comptes que vous gérez apparaît.
2. Choisissez le compte auquel vous souhaitez ajouter des membres, puis choisissez Inviter des utilisateurs.

   La boîte de dialogue Inviter de nouveaux utilisateurs apparaît.
3. Entrez les adresses e-mail des utilisateurs que vous souhaitez inviter. Séparez chaque adresse par un point-virgule (;).
4. Choisissez Invite users (Inviter des utilisateurs).

Les nouveaux utilisateurs apparaissent dans la liste. Lorsque vous invitez des utilisateurs à rejoindre un compte d'équipe, leurs coordonnées n'apparaissent pas tant qu'ils n'ont pas accepté votre invitation.

Affichage des informations utilisateur

Dans la console Amazon Chime, sous Utilisateurs, vous pouvez consulter la liste de tous les utilisateurs de votre compte et leurs informations d'utilisateur. Recherchez un utilisateur spécifique à l'aide de son adresse e-mail et choisissez son nom pour voir ses informations d'utilisateur. Sous Détails de l'utilisateur, vous pouvez consulter des informations détaillées sur l'utilisateur et mettre à jour son compte utilisateur.

Le tableau suivant répertorie les informations utilisateur qui apparaissent dans la console.

> **Note**
>
> Les informations complètes de l'utilisateur n'apparaissent pas pour les utilisateurs du compte Team tant qu'ils n'ont pas accepté leurs invitations.

Champ	Description	Exemple
Display name (Nom d'affichage)	Le nom de l'utilisateur qui apparaît dans Amazon Chime. Pour les utilisateurs de Login with Amazon (LWA), il s'agit du nom complet. Pour les utilisateurs Active Directory, le DISPLAY_NAME_ATTRIBUTE est utilisé.	Major, Mary
Email address (Adresse e-mail)	Pour les utilisateurs LWA, adresse e-mail utilisée pour l'inscription. Pour les utilisateurs Active Directory, l'adresse e-mail principale à partir de Active Directory s'affiche.	mary.major@example.com
Inscription	État d'enregistrement actuel de l'utilisateur. Les valeurs possibles diffèrent entre les comptes d'entreprise, où les invitations ne sont pas envoyées, et les comptes d'équipe, où les invitations sont envoyées.	Inscrit, Non inscrit ou Suspendu (pour un compte d'entreprise)
Niveau d'autorisation	Réglé sur Pro par défaut, pour permettre aux utilisateurs d'organiser des réunions. Peut être défini sur Basic (Basique).	Pro (Professionnel), Basic (Basique)
Invité	Pour les comptes d'équipe, date à laquelle l'utilisateur a été invité à faire partie du compte.	01/05/2020

Champ	Description	Exemple
A rejoint	Date à laquelle l'utilisateur s'est connecté pour la première fois à Amazon Chime. Pour les utilisateurs de la version d'essai Pro, il s'agit également de la date de début de leur période d'essai Pro.	01/10/2020
Personal PIN (Code PIN personnel)	Code PIN personnel de réunion que l'utilisateur peut utiliser pour planifier des réunions.	0123456789
Privacy setting (Paramètre de confidentialité)	Paramètre de présence sélectionné par l'utilisateur.	Public (Public) ou Private (Privé)
Meetings attended (Participation aux réunions)	Nombre de réunions auxquelles un utilisateur a participé.	87
Meetings organized (Organisation de réunions)	Nombre de réunions qu'un utilisateur a organisées.	12
Meeting satisfaction (Niveau de satisfaction de réunion)	Le pourcentage de réponses positives données à l' end-of-meetingenquête.	92 %
Utilisateur dernièrement actif	Dernière date à laquelle l'utilisateur a été actif.	06/12/2020
Messages de conversation envoyés	Le nombre de messages de chat envoyés par l'utilisateur.	1025
Numéro de téléphone	Le numéro de téléphone affecté à un utilisateur, le cas échéant.	+12065550100

Gestion des autorisations et des accès des utilisateurs

Gérez les fonctionnalités auxquelles vos utilisateurs d'Amazon Chime peuvent accéder en leur attribuant des autorisations Pro ou Basic. Les utilisateurs disposant d'autorisations de base ne peuvent pas organiser de réunions, mais ils peuvent y assister et utiliser le chat. Pour plus d'informations sur les fonctionnalités auxquelles les utilisateurs disposant d'autorisations Pro et Basic peuvent accéder, consultez la section Forfaits et tarifs.

Gérez qui peut se connecter à votre compte administratif Amazon Chime en invitant ou en suspendant des utilisateurs. Seuls les administrateurs de comptes Enterprise peuvent suspendre des utilisateurs. Les administrateurs de comptes d'équipe peuvent supprimer des utilisateurs de leurs comptes afin qu'ils ne payent plus pour les autorisations des utilisateurs. Toutefois, ils ne peuvent pas suspendre l'utilisateur pour l'empêcher de se connecter. Pour plus d'informations sur les différences entre les comptes Enterprise et Team, consultezGestion de vos comptes Amazon Chime.

Gestion des autorisations utilisateur

En tant qu'administrateur Amazon Chime, vous pouvez gérer les autorisations Pro et Basic pour les utilisateurs de votre compte Amazon Chime.

Si Active Directory ou Okta est configuré pour votre compte Amazon Chime, gérez les autorisations des utilisateurs via leur appartenance à un groupe d'annuaires. Si Active Directory ou Okta ne sont pas configurés, gérez les autorisations des utilisateurs depuis la console Amazon Chime.

Comptes Login with Amazon d'équipe et d'entreprise

Si vous administrez un compte Amazon Chime Team ou un compte Enterprise LWA, où les utilisateurs se connectent avec leur compte Login with Amazon (LWA), vous pouvez gérer les autorisations Pro et Basic dans la console Amazon Chime.

Pour gérer les autorisations des utilisateurs pour les comptes Team et Enterprise LWA

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour les comptes, choisissez le nom du compte Amazon Chime.
3. Choisissez Utilisateurs.
4. Sélectionnez les utilisateurs et choisissez Actions, Attribuer des autorisations.
5. Choisissez l'une des autorisations suivantes :

- Pro
- Base

6. Choisissez Attribuer.

Comptes Enterprise Active Directory ou Enterprise OpenID Connect (Okta)

Si vos utilisateurs se connectent avec des informations d'identification Active Directory ou Okta, gérez leurs autorisations en les rendant membres d'un groupe d'annuaires auquel des autorisations Pro ou Basic sont attribuées.

Pour attribuer des autorisations Pro à un utilisateur, faites-en un membre d'un groupe Active Directory ou Okta auquel vous avez attribué des autorisations Pro. Pour attribuer des autorisations de base à un utilisateur, faites-en un membre d'un groupe auquel vous avez attribué des autorisations de base. Les utilisateurs qui ne disposent pas des autorisations Pro ou Basic ne peuvent pas se connecter à Amazon Chime.

Gestion de l'accès des utilisateurs

Si vous gérez un compte Amazon Chime, vous pouvez inviter des utilisateurs pour les autoriser à se connecter à votre compte. Les administrateurs de comptes d'entreprise peuvent suspendre l'accès des utilisateurs pour les empêcher de se connecter au compte.

Inviter et supprimer des utilisateurs d'un compte Team

Si vous gérez un compte Team, utilisez la console Amazon Chime pour inviter des utilisateurs depuis n'importe quel domaine de messagerie.

> **Note**
>
> L'essai Pro gratuit de 30 jours d'un utilisateur prend fin lorsqu'il accepte votre invitation.

Pour inviter des utilisateurs à faire partie d'un compte d'équipe

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour Comptes, choisissez le nom du compte d'équipe.
3. Choisissez Utilisateurs, puis Invitez des utilisateurs.

4. Entrez les adresses e-mail des utilisateurs à inviter, en séparant les adresses e-mail multiples par un point-virgule (). **;**
5. Choisissez Invite users (Inviter des utilisateurs).

La procédure suivante dissocie les utilisateurs de votre compte d'équipe en supprimant les autorisations Pro ou Basic qui leur ont été attribuées. Les utilisateurs supprimés peuvent toujours se connecter à Amazon Chime, mais ils ne sont plus des membres payants de votre compte Amazon Chime.

Pour supprimer des utilisateurs d'un compte d'équipe

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour Comptes, choisissez le nom du compte d'équipe.
3. Choisissez Utilisateurs.
4. Sélectionnez les utilisateurs à supprimer, puis choisissez Actions, Supprimer l'utilisateur.

Toutes les autorisations Pro ou Basic attribuées aux utilisateurs sont supprimées. Les utilisateurs ne peuvent plus utiliser la saisie semi-automatique pour trouver de nouveaux utilisateurs de l'équipe dans leurs contacts.

Inviter et suspendre les utilisateurs d'un compte Enterprise

Si vous gérez un compte d'entreprise, tous les utilisateurs qui s'inscrivent à Amazon Chime avec une adresse e-mail associée aux domaines que vous avez revendiqués sont automatiquement ajoutés à votre compte. Si vous avez configuré Active Directory ou Okta, les utilisateurs doivent également être membres du groupe d'annuaires que vous avez configuré pour Amazon Chime.

Pour inviter des utilisateurs à faire partie d'un compte d'entreprise

- Envoyez un e-mail d'invitation aux utilisateurs de votre organisation et demandez-leur de suivre les étapes décrites dans la section Création d'un compte Amazon Chime dans le guide de l'utilisateur Amazon Chime.

Les utilisateurs se connectent avec une adresse e-mail provenant de l'un des domaines que vous avez réclamés pour votre compte. Une fois qu'ils ont terminé les étapes de création de leurs comptes utilisateur Amazon Chime, ils apparaissent automatiquement dans la section Utilisateurs de votre compte d'entreprise dans la console Amazon Chime.

La procédure suivante suspend l'accès des utilisateurs à un compte d'entreprise sur lequel Active Directory ou Okta n'est pas configuré. Cela empêche les utilisateurs de se connecter à Amazon Chime.

Pour suspendre des utilisateurs d'un compte d'entreprise

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Pour Comptes, choisissez le nom du compte d'entreprise.
3. Choisissez Utilisateurs.
4. Sélectionnez les utilisateurs à suspendre, puis choisissez Actions, Suspendre l'utilisateur.
5. Cochez la case et choisissez Suspendre.

Si Active Directory ou Okta sont configurés pour votre compte Enterprise, suivez la procédure suivante pour suspendre des utilisateurs.

Pour suspendre les utilisateurs d'un compte d'entreprise Active Directory ou OpenID Connect (Okta)

- Effectuez l'une des actions suivantes :
  - Depuis votre tableau de bord d'administrateur Active Directory ou Okta, suspendez l'utilisateur ou marquez-le comme inactif.
  - Supprimez l'utilisateur de tout groupe Active Directory auquel des autorisations Basic ou Pro lui ont été attribuées.

Modification des codes PIN personnels de réunion

Un code PIN personnel de réunion est un ID statique généré lorsque l'utilisateur s'inscrit. Le code PIN permet à un utilisateur d'Amazon Chime de planifier facilement des réunions avec d'autres utilisateurs d'Amazon Chime. L'utilisation d'un code PIN personnel de réunion signifie que les organisateurs d'une réunion ne sont pas obligés de mémoriser les détails pour chaque nouvelle réunion qu'ils planifient.

Si un utilisateur a l'impression que son code PIN personnel de réunion a été usurpé, il peut le réinitialiser et générer un nouvel ID. Lorsqu'un code PIN personnel de réunion est mis à jour, l'utilisateur doit mettre à jour toutes les réunions qui ont été planifiées à l'aide de l'ancien code PIN personnel de réunion.

Pour modifier un code PIN personnel de réunion

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, sélectionnez le nom du compte Amazon Chime.
3. Dans le panneau de navigation, choisissez utilisateurs.
4. Recherchez l'utilisateur dont le code PIN doit être modifié.
5. Pour ouvrir la page User detail (Informations utilisateur), choisissez le nom de l'utilisateur.
6. Choisissez User Actions (Actions utilisateur), Reset personal PIN (Réinitialiser le code personnel PIN), Confirm (Confirmer).

Gestion des versions d'évaluation Pro

Lorsqu'un utilisateur accepte une invitation de l'équipe Amazon Chime ou qu'il est ajouté à un compte Enterprise, son essai gratuit prend fin et il dispose des autorisations Pro. Cela lui permet de continuer à héberger des réunions planifiées. Le remplacement du niveau d'autorisation d'un utilisateur par Basic (De base) l'empêche d'agir en comme hôte de réunion.

Avec la tarification basée sur l'utilisation d'Amazon Chime, vous ne payez que pour les utilisateurs qui organisent des réunions les jours où ils les organisent. Les participants de la réunion et les utilisateurs de la messagerie instantanée ne sont pas facturés.

Les utilisateurs Pro sont considérés comme Active Pro s'ils ont hébergé une réunion qui s'est terminée un jour calendaire et si au moins l'une des conditions suivantes est remplie :

- La réunion a été programmée.
- La réunion a compté plus de deux participants.
- La réunion a au moins un enregistrement d'événement.
- La réunion a inclus un participant ayant appelé.
- La réunion a inclus un participant qui s'est joint avec H.323 ou SIP.

Pour plus d'informations, consultez Forfaits et tarification.

Demande de pièces jointes utilisateur

Si vous gérez un compte Enterprise et que vous disposez des autorisations appropriées, vous pouvez demander et recevoir les pièces jointes que vos utilisateurs téléchargent dans Amazon

Chime. Vous pouvez obtenir des pièces jointes que les utilisateurs ont téléchargées dans des conversations individuelles et de groupe, ou dans des salons de discussion qu'ils ont créés.

> **Note**
>
> Si vous gérez un compte Amazon Chime Team, vous pouvez passer à un compte Enterprise en revendiquant un ou plusieurs domaines. Vous pouvez également supprimer des utilisateurs du compte d'équipe, ce qui permet aux utilisateurs non gérés d'obtenir leurs pièces jointes à l'aide de l'Amazon Chime Assistant.

Pour demander de pièces jointes provenant d'utilisateurs

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Sur la page Comptes, sélectionnez le nom du compte Amazon Chime.
3. Dans Settings (Paramètres), choisissez Account (Compte), Account actions (Actions de compte), Request attachments (Demander des pièces jointes).
4. Dans un délai d'environ 24 heures, la page de résumé du compte fournit un lien vers un fichier contenant une liste d'URL présignées que vous utilisez pour accéder à chaque pièce jointe.
5. Téléchargez le fichier.

> **Note**
>
> Veillez à préserver un niveau de contrôle d'accès approprié pour le fichier. En effet, un utilisateur qui accède au fichier peut utiliser la liste des URL pour télécharger les pièces jointes associées.
> Les URL présignées expirent au bout de 6 jours. Vous pouvez envoyer une seule demande tous les 7 jours.

Pour utiliser des politiques AWS Identity and Access Management (IAM) afin de gérer l'accès à la console d'administration Amazon Chime et à l'action Request attachments, utilisez l'une des politiques gérées par Amazon Chime FullAccess (UserManagement,, ou). ReadOnly Vous pouvez également mettre à jour les stratégies personnalisées afin d'inclure l'action `StartDataExport` et l'action `RetrieveDataExport`. Pour plus d'informations sur ces actions, consultez la section Actions définies par Amazon Chime dans le guide de l'utilisateur IAM.

Comment Amazon Chime gère les mises à jour automatiques

Amazon Chime propose différentes méthodes pour mettre à jour ses clients. La méthode varie selon que vous exécutez Amazon Chime dans un navigateur, sur votre ordinateur de bureau ou sur un appareil mobile.

L'application Web Amazon Chime (https://app.chime.aws) intègre toujours les dernières fonctionnalités et correctifs de sécurité.

Le client de bureau Amazon Chime vérifie les mises à jour chaque fois que vous choisissez Quitter ou Sign Out. Cela s'applique aux machines Windows et macOS. Lorsque vous exécutez le client, celui-ci vérifie les mises à jour toutes les trois heures. Vous pouvez également vérifier les mises à jour en choisissant Vérifier les mises à jour dans le menu Aide de Windows ou dans le menu Amazon Chime de macOS.

Lorsque le client de bureau détecte une mise à jour, Amazon Chime invite l'utilisateur à l'installer, sauf s'il participe à une réunion en cours. Ils sont en réunion permanente lorsque :

- Ils assistent à une réunion.
- Ils ont été invités à une réunion qui est toujours en cours.

Amazon Chime les invite à installer la dernière version et leur fournit un compte à rebours de 15 secondes pour qu'ils puissent reporter l'installation. Les utilisateurs choisissent Essayer plus tard pour reporter la mise à jour.

Si les utilisateurs reportent une mise à jour et qu'ils ne participent pas à une réunion en cours, le client vérifie l'existence de la mise à jour au bout de trois heures et les invite à nouveau à l'installer. L'installation commence à la fin du compte à rebours.

> **Note**
>
> Sur un ordinateur macOS, les utilisateurs doivent choisir Redémarrer maintenant pour commencer la mise à jour.

Sur les appareils mobiles : les applications mobiles Amazon Chime utilisent les options de mise à jour proposées par l'App Store et Google Play pour fournir la dernière version du client Amazon Chime. Vous pouvez également utiliser le système de gestion des appareils mobiles pour déployer les mises à jour.

Migration des utilisateurs vers un autre compte Team

Vous migrez des utilisateurs vers d'autres comptes Team en créant et en configurant un compte de destination, s'il n'en existe pas déjà un. Vous ajoutez ensuite des utilisateurs au compte de destination. Les étapes suivantes vous permettent d'accéder aux informations relatives à la réalisation de chaque étape d'une migration.

Pour migrer les utilisateurs

1. Si vous n'avez pas de compte d'équipe de destination, créez-en un. Pour plus d'informations, consultez Étape 1 : Création d'un compte administrateur Amazon Chime.
2. Le cas échéant, configurez le compte. Pour plus d'informations, consultez Étape 2 (facultative) : Configuration des paramètres du compte.
3. Ajoutez des utilisateurs au compte. Pour plus d'informations, voir Étape 3 : Ajout des utilisateurs à votre compte.

Gestion des numéros de téléphone dans Amazon Chime

Vous utilisez la console Amazon Chime pour fournir des numéros de téléphone. Lorsque vous fournissez des numéros, vous les demandez à partir d'un pool de numéros géré par Amazon Chime. Lorsque vous annulez l'attribution puis que vous supprimez des numéros, ils retournent dans le pool. Lorsque vous transférez des numéros, vous les transférez vers et depuis Amazon Chime.

> **Note**
>
> Lorsque vous utilisez la console Amazon Chime, vous ne pouvez fournir que des numéros Amazon Chime Business Calling. Si vous avez besoin de numéros internationaux, vous pouvez utiliser les connecteurs vocaux Amazon Chime et les applications multimédia SIP. Pour ce faire, vous devez d'abord créer un compte administratif du SDK Amazon Chime. Pour plus d'informations, consultez les rubriques suivantes du guide de l'administrateur du SDK Amazon Chime :
>
> - Prérequis
> - Gestion de l'inventaire des numéros de téléphone
> - Gestion des connecteurs vocaux
> - Gestion des applications multimédia SIP

Les rubriques des sections suivantes expliquent comment configurer et gérer les numéros de téléphone Amazon Chime.

Table des matières

Mise en service de numéros de téléphone

Utilisez la console Amazon Chime pour fournir des numéros de téléphone pour votre compte Amazon Chime. Les chiffres proviennent d'un pool géré par Amazon Chime. Choisissez Amazon Chime Business Calling pour fournir et attribuer des numéros de téléphone à vos utilisateurs Amazon Chime existants.

Lorsque le provisionnement est terminé, les numéros de téléphone apparaissent dans votre inventaire. Vous les attribuez ensuite à des utilisateurs individuels.

Pour mettre en service des numéros de téléphone

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Choisissez Orders (Commandes), Provision phone numbers (Mise en service des numéros de téléphone).
4. Sélectionnez Business Calling, puis choisissez Next.
5. Recherchez les numéros de téléphone disponibles. Sélectionnez les numéros de téléphone de votre choix, puis choisissez Provision (Mettre en service).

Les numéros de téléphone apparaissent dans vos listes de commandes et de commandes en attente pendant le provisionnement.

Transfert de numéros de téléphone existants

En plus de fournir des numéros de téléphone, vous pouvez également transférer les numéros de votre opérateur téléphonique vers votre inventaire. Cela inclut les numéros gratuits.

> **Note**
>
> Si vous devez transférer des numéros internationaux, utiliser le connecteur vocal Amazon Chime ou utiliser des applications multimédia SIP, vous devez créer un compte administrateur du SDK Amazon Chime et utiliser la console Amazon Chime SDK. Pour plus d'informations à ce sujet, reportez-vous à la section Conditions préalables du Guide de l'administrateur du SDK Amazon Chime.

Les sections suivantes expliquent comment transférer des numéros de téléphone.

Rubriques

Conditions requises pour le portage des numéros

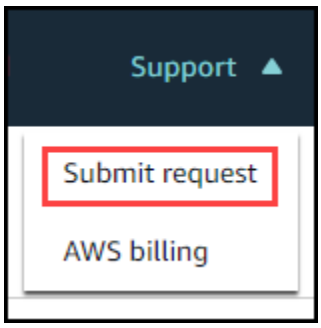
Pour transférer les numéros, vous devez avoir une lettre d'agence (LOA). Vous devez avoir une LOA pour les numéros de téléphone nationaux. Téléchargez le formulaire de lettre d'agence (LOA) et remplissez-le. Si vous devez transférer des numéros de téléphone de différents opérateurs, remplissez une LOA distincte pour chaque opérateur.

Portage de numéros de téléphone dans

Vous créez une demande d'assistance pour transférer les numéros de téléphone existants.

Pour porter les numéros de téléphone existants

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans la barre de commandes en haut de la page, choisissez Support, puis Soumettre la demande.



   Cela vous amène à la console AWS Support.

> **Note**
>
> Vous pouvez également accéder directement à la page AWS Support centrale. Si c'est le cas, choisissez Créer un dossier, puis suivez les étapes ci-dessous.

3. Dans la section Comment pouvons-nous vous aider, procédez comme suit :

   a. Choisissez Compte et facturation.

   b. Dans la liste des services, choisissez Chime SDK (Number Management).

   c. Dans la liste des catégories, choisissez Phone Number Port In.

   d. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).

4. Sous Informations supplémentaires, procédez comme suit

   a. Sous Objet, entrez**`Porting phone numbers in`**.

   b. Dans Description, entrez les informations suivantes :

      Pour le portage de numéros américains :

      - Numéro de téléphone de facturation (BTN) du compte.
      - Autorisation du nom de la personne. Il s'agit de la personne en charge de la facturation du compte auprès du transporteur actuel.
      - Transporteur actuel, s'il est connu.
      - Numéro de compte de service, si ces informations sont présentes avec le transporteur actuel.
      - Code PIN du service, le cas échéant.
      - Adresse du service et nom du client, tels qu'ils apparaissent dans votre contrat transporteur actuel.
      - Date et heure demandées pour le port.
      - (Facultatif) Si vous souhaitez transférer votre numéro de téléphone de facturation (BTN), sélectionnez l'une des options suivantes :
        - Je suis en train de porter mon BTN et je souhaite le remplacer par un nouveau BTN que je fournis. Je peux confirmer que ce nouveau BTN est sur le même compte auprès de l'opérateur actuel.

- Je transfère mon BTN et je souhaite fermer mon compte auprès de mon opérateur actuel.
- Je transfère mon BTN parce que mon compte est actuellement configuré de sorte que chaque numéro de téléphone corresponde à son propre BTN. (Sélectionnez cette option uniquement lorsque votre compte auprès de l'opérateur actuel est configuré de cette façon.)
- Après avoir choisi une option, joignez votre lettre d'agence (LOA) à la demande.

Pour le portage de numéros internationaux :

- Vous devez utiliser le type de produit SIP Media Application Dial-In pour les numéros de téléphone non américains.
- Type de numéro (local ou gratuit)
- Pour porter les numéros de téléphone existants
- Estimation du volume d'utilisation
- Pays

c. Dans la liste des types de numéros de téléphone, sélectionnez Business Calling, SIP Media Application Dial-In ou Voice Connector.

d. Dans Numéro de téléphone, entrez au moins un numéro de téléphone, même si vous transférez plusieurs numéros.

e. Sous Date de portage, entrez la date de portage souhaitée.

f. Sous Heure de portage, entrez l'heure souhaitée.

g. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

5. Dans la section Résoudre maintenant ou contactez-nous, choisissez Contactez-nous.
6. Dans la liste des langues de contact préférées, choisissez une langue
7. Choisissez Web ou Téléphone. Si vous choisissez Téléphone, entrez votre numéro de téléphone. Lorsque vous avez terminé, choisissez Soumettre.

AWS Support vous permet de savoir si vos numéros de téléphone peuvent être transférés depuis votre opérateur téléphonique actuel. Dans la mesure du possible, vous devez soumettre tous les documents requis. Les étapes décrites dans la section suivante expliquent comment soumettre ces documents.

Soumission des documents requis

Une fois que le AWS Support vous a indiqué que vous pouvez transférer des numéros de téléphone, vous devez soumettre tous les documents requis. Les étapes suivantes expliquent comment procéder.

> **Note**
>
> AWS Support fournit un lien Amazon S3 sécurisé pour le téléchargement de tous les documents demandés. Ne poursuivez pas tant que vous n'avez pas reçu le lien.

Pour soumettre des documents

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Connectez-vous à votre AWS compte, puis ouvrez le lien de téléchargement Amazon S3 généré spécifiquement pour votre compte.

   > **Note**
   >
   > Le lien expire au bout de dix jours. Il est généré spécifiquement pour le compte qui a créé le dossier. Le lien nécessite un utilisateur autorisé du compte pour effectuer le téléchargement.

3. Choisissez Ajouter des fichiers, puis sélectionnez les documents d'identité liés à votre demande.
4. Développez la section Autorisations et choisissez Spécifier les autorisations ACL individuelles.
5. À la fin de la section Liste de contrôle d'accès (ACL), choisissez Ajouter un bénéficiaire, puis collez la clé fournie par le AWS Support dans le champ Bénéficiaire.
6. Sous Objets, cochez la case Lire, puis choisissez Télécharger.

Après avoir fourni la lettre d'agence (LOA), AWS Support confirmez auprès de votre opérateur téléphonique actuel que les informations figurant sur la LOA sont correctes. Si les renseignements fournis dans la LOA ne correspondent pas à ceux que votre opérateur téléphonique a dans ses dossiers, AWS Support vous demandera de mettre à jour les informations fournies dans la LOA.

Afficher le statut de la demande

Les étapes suivantes expliquent comment utiliser la console Amazon Chime pour consulter le statut de vos demandes de portage.

Pour consulter le statut

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, choisissez Gestion des numéros de téléphone.
3. Choisissez l'onglet Commandes.

La colonne État indique le statut de votre demande. AWS Support vous contacte également pour vous faire part de mises à jour et de demandes d'informations supplémentaires, le cas échéant. Pour plus d'informations, consultez Définitions des différents états du transfert de numéros de téléphone, plus loin dans cette section.

Attribution de numéros portés

Une fois que votre opérateur téléphonique a confirmé que la LOA est correcte, il examine et approuve le port demandé. Ils fournissent ensuite AWS Support une date et une heure de validation des commandes fermes (FOC) pour que le port ait lieu.

À la date FOC, les numéros de téléphone portés sont activés pour être utilisés. Vous devez ensuite attribuer les numéros aux utilisateurs du compte souhaité.

Pour attribuer des numéros de téléphone

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, choisissez Gestion des numéros de téléphone.
3. Dans l'onglet Inventaire, cochez la case à côté du numéro que vous souhaitez attribuer, puis choisissez Attribuer.

   > **Note**
   >
   > Vous ne pouvez choisir qu'un seul numéro à la fois.

4. Sur la page Attribuer +1 numéro de téléphone à un profil utilisateur, sélectionnez le compte associé au numéro, puis cliquez sur Suivant.

5. Sélectionnez l'utilisateur auquel vous souhaitez attribuer le numéro, puis choisissez Attribuer.

Portage de numéros de téléphone vers l'extérieur

Vous transférez des numéros depuis Amazon Chime en initiant une demande de portage auprès de votre opérateur gagnant. Lorsque vous soumettez des informations à votre opérateur gagnant, incluez votre AWS numéro de compte en tant qu'identifiant de compte associé au numéro de téléphone transféré.

Lorsque le processus de portage est terminé et que le transporteur gagnant dispose des numéros, vous devez annuler l'attribution de ces numéros et les supprimer de votre stock. Pour plus d'informations, consultez Annulation de l'attribution des numéros de téléphone Amazon Chime Business Calling et Suppression de numéros de téléphone dans ce guide.

⚠ Important

- La capacité de transférer des numéros dépend de la capacité du transporteur gagnant à accepter ces numéros.
- La vérification de l'authenticité de la demande de transfert de l'opérateur cible est essentielle pour la sécurité de votre numéro de téléphone. Si les informations du compte ne sont pas correctes (par exemple, l'identifiant du compte ne correspond pas), votre demande de transfert peut être rejetée, ce qui entraînera des retards et vous obligera à soumettre à nouveau votre demande.

(Facultatif) Comment demander un code PIN pour protéger votre numéro

Pour plus de sécurité, vous pouvez nous contacter pour appliquer un code PIN à votre numéro. Le transporteur gagnant utilise ensuite ce code PIN. Procédez comme suit :

Pour demander un code PIN

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Contactez-nous, sélectionnez Support.

   Cela vous amène à la console AWS Support.

> **Note**
>
> Vous pouvez également accéder directement à la page AWS Support centrale. Si c'est le cas, choisissez Créer un dossier, puis suivez les étapes ci-dessous.

3. Dans la section Comment pouvons-nous vous aider, procédez comme suit :
   a. Choisissez Compte et facturation.
   b. Dans la liste des services, choisissez Chime SDK (Number Management).
   c. Dans la liste des catégories, choisissez Phone Number Port Out.
   d. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).
4. Sous Informations supplémentaires, procédez comme suit
   a. Sous Objet, entrez**`Porting phone numbers out`**.
   b. Sous Description, entrez ce qui suit.

      ```
      I would like to assign a pin to my phone number: Pin: ABCD123 Phone Number: 1234567890
      ```

      > **Note**
      >
      > Vous devez fournir un code PIN alphanumérique de 4 à 10 caractères.

AWS Support associe un code PIN au numéro de téléphone. Lorsque vous demandez le port auprès de votre opérateur gagnant, fournissez votre numéro de AWS compte et votre code PIN. Nous utiliserons ces informations pour valider toutes les demandes de port reçues pour votre numéro.

Définitions des différents états du transfert de numéros de téléphone

Après avoir soumis une demande de portage de numéros de téléphone existants vers Amazon Chime, vous pouvez consulter le statut de votre demande de portage dans la console Amazon Chime sous Appels, Gestion des numéros de téléphone, En attente.

Les états et définitions de portage sont les suivants :

CANCELLED

AWS Support a annulé l'ordre de portage en raison d'un problème avec le port, tel qu'une demande d'annulation émanant du transporteur ou de votre part. AWS Support vous contacte pour vous fournir des informations.

CANCEL_REQUESTED

AWS Support est en train de traiter une annulation de l'ordre de portage en raison d'un problème avec le port, tel qu'une demande d'annulation émanant du transporteur ou de votre part. AWS Support vous contacte pour vous fournir des informations.

CHANGE_REQUESTED

AWS Support traite votre demande de modification et la réponse du transporteur est en attente. Prévoyez un délai de traitement supplémentaire.

TERMINÉ

Votre ordre de portage est terminé et vos numéros de téléphone sont activés.

EXCEPTION

AWS Support vous contacte pour obtenir les informations supplémentaires nécessaires pour compléter la demande de port. Prévoyez un délai de traitement supplémentaire.

FOC

La date FOC est confirmée auprès du transporteur. AWS Support vous contacte pour confirmer la date.

PENDING DOCUMENTS

AWS Support vous contacte pour obtenir les documents supplémentaires nécessaires pour compléter la demande de port. Prévoyez un délai de traitement supplémentaire.

SUBMITTED

Votre ordre de portage est soumis et la réponse du transporteur est en attente.

Attribution de numéros de téléphone Amazon Chime Business Calling

Utilisez la page d'inventaire de gestion des numéros de téléphone pour attribuer des numéros de téléphone Amazon Chime Business Calling à des utilisateurs individuels.

Pour attribuer des numéros de téléphone Amazon Chime Business Calling

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Dans l'onglet Inventaire, sélectionnez le numéro de téléphone que vous souhaitez attribuer.
4. Choisissez Attribuer.
5. Sélectionnez le compte auquel appartient l'utilisateur, puis cliquez sur Suivant.
6. Sélectionnez l'utilisateur, puis choisissez Attribuer.

Lorsque vous modifiez un numéro de téléphone ou des autorisations relatives à un numéro de téléphone, nous vous recommandons de fournir à l'utilisateur ses nouvelles informations ou informations d'autorisation. Avant que les utilisateurs puissent accéder à leur nouveau numéro de téléphone ou aux nouvelles fonctionnalités d'autorisation, ils doivent se déconnecter de leur compte Amazon Chime, puis se reconnecter.

Annulation de l'attribution des numéros de téléphone Amazon Chime Business Calling

La procédure suivante annule l'attribution de numéros de téléphone aux utilisateurs d'Amazon Chime Business Calling.

Pour annuler l'attribution de numéros de téléphone

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Dans l'onglet Inventaire, sélectionnez le numéro de téléphone que vous souhaitez annuler.
4. Choisissez Unassign (Annuler).
5. Cochez la case, puis choisissez Unassign (Annuler).

Vous pouvez consulter le détail des numéros figurant dans votre inventaire. Par exemple, vous pouvez voir si les appels téléphoniques et les SMS sont activés.

Pour afficher les détails de numéro de téléphone de l'inventaire

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

2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Cliquez sur l'onglet Inventaire, puis sélectionnez le numéro de téléphone que vous souhaitez consulter.
4. Ouvrez la liste des actions et choisissez Afficher les détails.

Utilisation des noms d'appel sortants

Les noms d'appels sortants agissent comme des identifiants d'appelant. Vous pouvez définir un nom d'appel par défaut pour un ou plusieurs numéros de téléphone de votre inventaire. Vous pouvez également définir des noms d'appel uniques pour des numéros de téléphone individuels. Les noms apparaissent ensuite aux destinataires des appels sortants passés à l'aide de ces numéros de téléphone. Les noms d'appel s'appliquent à tous les types de produits contenant des numéros de téléphone. Vous pouvez mettre à jour les noms une fois tous les sept jours.

Par exemple, vous pouvez définir le nom d'appel par défaut du département 5 pour tous les numéros de téléphone de ce département. Vous pouvez également attribuer un nom unique à Jane Doe pour le chef de service.

Les étapes suivantes expliquent comment définir les noms d'appels sortants par défaut et individuels.

Pour définir un nom d'appel

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Dans l'onglet Inventaire, effectuez l'une des opérations suivantes : cochez les cases à côté des numéros de téléphone que vous souhaitez mettre à jour.
   - Pour définir un nom d'appel par défaut pour plusieurs numéros, cochez les cases à côté de ces numéros.
   - Pour définir un nom d'appel individuel, sélectionnez le numéro souhaité.
4. Ouvrez la liste des actions et choisissez Mettre à jour le nom d'appel par défaut.
5. Dans le champ Nom d'appel par défaut, entrez un nom de 15 caractères maximum.
6. Choisissez Enregistrer.

Attendez 72 heures pour que le système mette à jour le nom d'appel par défaut.

Suppression de numéros de téléphone

> **Important**
>
> Seuls les administrateurs système Amazon Chime peuvent effectuer ces étapes. Vous devez également annuler l'attribution des numéros de téléphone avant de pouvoir les supprimer.

Lorsque vous fournissez un numéro de téléphone, vous le commandez à partir d'un pool de numéros géré par Amazon Chime. La suppression d'un numéro le ramène dans le pool. Lorsque vous supprimez un numéro, il est d'abord envoyé dans votre file d'attente de suppression où il est conservé pendant 7 jours. Pendant ce temps, vous pouvez replacer le numéro dans votre inventaire. Après 7 jours, le système supprime automatiquement le numéro de la file d'attente et le dissocie de votre compte. Cela renvoie le numéro au pool de numéros. Si vous devez récupérer un numéro une fois que le système l'a supprimé de la file d'attente, suivez les étapes indiquéesMise en service de numéros de téléphone, mais sachez que le numéro n'est peut-être pas disponible.

Pour supprimer des numéros de téléphone non attribués

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Cliquez sur l'onglet Inventaire, puis sélectionnez le ou les numéros de téléphone que vous souhaitez supprimer.
4. Ouvrez la liste des actions et choisissez Supprimer le (s) numéro (s) de téléphone.
5. Cochez la case, puis choisissez Supprimer.

Les numéros de téléphone supprimés sont conservés dans la file d'attente de suppression pendant 7 jours avant d'être définitivement supprimés de votre inventaire.

Restauration de numéros de téléphone supprimés

Vous pouvez restaurer les numéros de téléphone supprimés de la file d'attente de suppression jusqu'à 7 jours après les avoir supprimés. La restauration d'un numéro de téléphone le renvoie dans votre inventaire.

Pour restaurer des numéros de téléphone supprimés

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Dans le volet de navigation, sous Appels, choisissez Gestion des numéros de téléphone.
3. Cliquez sur l'onglet File d'attente de suppression, puis sélectionnez le ou les numéros de téléphone que vous souhaitez restaurer.
4. Choisissez Move to inventory (Déplacer vers l'inventaire).

Gestion des paramètres globaux dans Amazon Chime

Vous utilisez la console Amazon Chime pour gérer les paramètres d'enregistrement détaillé des appels.

Configuration d'enregistrements de détails d'appels

Avant de pouvoir configurer les paramètres d'enregistrement détaillé des appels pour votre compte administratif Amazon Chime, vous devez d'abord créer un compartiment Amazon Simple Storage Service. Le compartiment Amazon S3 est utilisé comme destination de journal pour les enregistrements détaillés de vos appels. Lorsque vous configurez les paramètres de l'enregistrement détaillé de vos appels, vous accordez à Amazon Chime un accès en lecture et en écriture au compartiment Amazon S3 afin de sauvegarder et de gérer vos données. Pour plus d'informations sur la création d'un compartiment Amazon S3, veuillez consulter Mise en route sur Amazon Simple Storage Service dans le Guide de l'utilisateur Amazon Simple Storage Service.

Vous pouvez configurer les paramètres d'enregistrement détaillé des appels pour Amazon Chime Business Calling. Pour plus d'informations sur Amazon Chime Business Calling, consultezGestion des numéros de téléphone dans Amazon Chime.

Pour configurer les paramètres d'enregistrement de détails d'appels

1. Créez un compartiment Amazon S3 en suivant les étapes de démarrage sur Amazon Simple Storage Service dans le Guide de l'utilisateur Amazon Simple Storage Service.
2. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
3. Pour Global Settings (Paramètres généraux), choisissez Call detail records (Enregistrements de détails d'appels).
4. Choisissez la configuration des appels professionnels.
5. Dans Destination du journal, sélectionnez le compartiment Amazon S3.
6. Choisissez Save (Enregistrer).

Vous pouvez arrêter de consigner les enregistrements de détails d'appels à tout moment.

Pour arrêter la consignation des enregistrements de détails d'appels

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

2. Pour Global Settings (Paramètres généraux), choisissez Call detail records (Enregistrements de détails d'appels).
3. Choisissez Disable logging (Désactiver la journalisation) pour la configuration applicable.

Enregistrements détaillés des appels Amazon Chime Business Calling

Lorsque vous choisissez de recevoir les enregistrements détaillés des appels pour Amazon Chime Business Calling, ils sont envoyés vers votre compartiment Amazon S3. L'exemple suivant montre le format général du nom d'enregistrement détaillé d'un appel Amazon Chime Business Calling.

```
Amazon-Chime-Business-Calling-CDRs/json/111122223333/2019/03/01/123a4567-
b890-1234-5678-cd90efgh1234_2019-03-01-17.10.00.020_1a234567-89bc-01d2-3456-
e78f9g01234h
```

L'exemple suivant montre les données représentées dans le nom de l'enregistrement des détail d'appels.

```
Amazon-Chime-Business-Calling-CDRs/json/awsAccountID/year/month/
day/conferenceID_connectionDate-callStartTime-callDetailRecordID
```

L'exemple suivant montre le format général d'un enregistrement détaillé d'un appel Amazon Chime Business Calling.

```
{
    "SchemaVersion": "2.0",
    "CdrId": "1a234567-89bc-01d2-3456-e78f9g01234h",
    "ServiceCode": "AmazonChimeBusinessCalling",
    "ChimeAccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
    "AwsAccountId": "111122223333",
    "ConferenceId": "123a4567-b890-1234-5678-cd90efgh1234",
    "ConferencePin": "XXXXXXXXXX",
    "OrganizerUserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
    "OrganizerEmail": "jdoe@example.com",

    "CallerPhoneNumber": "+12065550100",
    "CallerCountry": "US",

    "DestinationPhoneNumber": "+12065550101",
```

```
    "DestinationCountry": "US",

    "ConferenceStartTimeEpochSeconds": "1556009595",
    "ConferenceEndTimeEpochSeconds": "1556009623",
    "StartTimeEpochSeconds": "1556009611",
    "EndTimeEpochSeconds": "1556009623",
    "BillableDurationSeconds": "24",
    "BillableDurationMinutes": ".4",
    "Direction": "Outbound"
}
```

Configuration d'une salle de conférence

Amazon Chime peut s'intégrer au matériel vidéo de votre chambre de Cisco, Tandberg, Polycom, Lifesize, Vidyo ou autres lorsque vous utilisez le protocole SIP ou H.323.

Pour vous connecter à Amazon Chime à l'aide d'un appareil VTC de salle de conférence compatible SIP, saisissez l'une des options suivantes :

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- Un ID de réunion à 10 chiffres suivi de **`@meet.chime.in`**

`meet.chime.in`connecte votre appareil SIP Room à la région Amazon Chime la plus proche. Pour vous connecter à une région spécifique, utilisez des entrées DNS spécifiques à une région pour les systèmes de salle SIP. Pour plus d'informations, veuillez consulter Systèmes de salle d'un protocole SIP (Session Initiation Protocol).

> **Note**
>
> Si votre appareil de salle SIP ne prend pas en charge TLS et nécessite une connectivité TCP, contactez le support AWS.

Si vous utilisez un appareil qui prend uniquement en charge H.323, vous devez composer l'un des numéros suivants :

- **`13.248.147.139`**
- **`76.223.18.152`**

Si un pare-feu filtre le trafic entre l'appareil VTC et Amazon Chime, ouvrez les plages des protocoles utilisés. Pour plus d'informations, veuillez consulter Configuration requise pour le réseau et la bande passante.

Sur l'écran d'accueil d'Amazon Chime, saisissez le numéro de réunion à 10 ou 13 chiffres auquel vous souhaitez participer. Vous pouvez trouver l'identifiant de réunion à 13 chiffres dans le client ou l'application Web Amazon Chime, ou choisissez l'option Dial-in.

Participation à une réunion modérée

Si la réunion est modérée et que vous êtes l'hôte ou le délégué, saisissez votre ID de réunion à 13 chiffres pour rejoindre la réunion en tant que modérateur. Si vous êtes un modérateur, entrez le code secret du modérateur dans le pavé numérique suivi du signe dièse (#) pour rejoindre et démarrer la réunion. Si vous n'êtes ni un hôte, ni un délégué ni un modérateur, vous êtes connecté à la réunion lorsqu'un modérateur rejoint et démarre la réunion.

Les modérateurs disposent de commandes d'hôte, ce qui signifie qu'ils peuvent effectuer des actions de réunion supplémentaires. Ces actions incluent le démarrage et l'arrêt de l'enregistrement, le verrouillage et le déverrouillage de la réunion, la désactivation du micro de tous les autres participants et la clôture de la réunion. Pour plus d'informations, consultez la section Actions du modérateur à l'aide du téléphone ou des systèmes vidéo de la chambre dans le guide de l'utilisateur d'Amazon Chime.

> **Note**
>
> Si vous utilisez Alexa for Business pour participer à vos réunions Amazon Chime, vous pouvez y participer en tant que modérateur uniquement si votre appareil est connecté à un système vidéo de la chambre et que vous vous connectez à l'aide du clavier numérique de l'appareil.

Appareils de téléconférence vidéo compatibles

Le tableau suivant est un sous-ensemble de la liste des appareils de téléconférence vidéo compatibles.

Device	SIP	H.323	Comment
Cisco SX20	Oui	Oui	Audio/Vidéo/Écran : OK vers et à partir de l'appareil
Cisco DX80	Oui	Oui	Audio/Vidéo/Écran : OK vers et

Device	SIP	H.323	Comment
			à partir de l'appareil
Icône Lifesize	Oui	Non	Audio/Vidéo/ Écran : OK vers et à partir de l'appareil
Polycom Debut	Oui	Oui	Audio/Vidéo/ Écran : OK vers et à partir de l'appareil
Ordinateur de RealPresence bureau Polycom	Non	Oui	Audio/Vidéo : OK, Écran : OK à partir de l'appareil
Polycom Trio	Oui	Oui	Audio/Vidéo/ Écran : OK vers et à partir de l'appareil
Tandberg C40	Oui	Oui	Audio/Vidéo/ Écran : OK vers et à partir de l'appareil

Configuration requise pour le réseau et la bande passante

Amazon Chime a besoin des destinations et des ports décrits dans cette rubrique pour prendre en charge différents services. Si le trafic entrant ou sortant est bloqué, cela peut avoir un impact sur l'utilisation des divers services, y compris les fichiers audio et vidéo, le partage d'écran ou la messagerie instantanée.

Amazon Chime utilise Amazon Elastic Compute Cloud (Amazon EC2) et d'autres services AWS sur le port TCP/443. Si votre pare-feu bloque le port TCP/443, vous devez placer `*.amazonaws.com` sur une liste d'autorisation ou placer des plages d'adresses IP AWS dans Références générales AWS pour les services suivants :

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Développez les sections suivantes pour plus d'informations sur les destinations, les ports et la bande passante.

Destinations et ports requis

Les destinations et ports suivants sont nécessaires pour exécuter Amazon Chime.

Destination	Ports
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

Port de réunion et de téléphonie

Amazon Chime utilise la destination et le port suivants pour les réunions et Amazon Chime Business Calling.

Destination	Port
99.77.128.0/18	UDP/3478

Systèmes de salle H.323

Amazon Chime utilise les destinations et les ports suivants pour les systèmes vidéo H.323 utilisés dans les chambres.

Destination	Ports
13.248.147.139	TCP/1720
76.223.18.152	TCP/1720
99.77.128.0/18	TCP/5100:6200
34.212.95.128/25	UDP/5100:6200
34.223.21.0/25	
52.55.62.128/25	
52.55.63.0/25	

Systèmes de salle d’un protocole SIP (Session Initiation Protocol)

Les destinations et ports suivants sont recommandés lors de l'exécution d'Amazon Chime pour les systèmes vidéo de chambre SIP dans votre environnement.

AWS Région	Destination	Ports
Solution internationale (Région la plus proche)	99.77.128.0/18 34.212.95.128/25 34.223.21.0/25 52.55.62.128/25 52.55.63.0/25	UDP/10000:60000
Globale	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
USA Est (Virginie du Nord)	meet.ue1.chime.in	TCP/5061
USA Ouest (Oregon)	meet.uw2.chime.in	TCP/5061
Asie-Pacifique (Singapour)	meet.as1.chime.in	TCP/5061
Asie-Pacifique (Sydney)	meet.as2.chime.in	TCP/5061
Asie-Pacifique (Tokyo)	meet.an1.chime.in	TCP/5061
Europe (Irlande)	meet.ew1.chime.in	TCP/5061
Amérique du Sud (São Paulo)	meet.se1.chime.in	TCP/5061

Exigences liées à la bande passante

Amazon Chime a les exigences de bande passante suivantes pour l'audio, la vidéo et le partage d'écran :

- Audio
  - Appel 1:1 : 54 kbps montant et descendant
  - Appel large : pas plus de 32 kbps supplémentaires descendants pour 50 appelants

- Vidéo
  - Appel 1:1 : 650 kbps montant et descendant
  - Mode HD : 1400 kbps montant et descendant
  - 3–4 personnes : 450 kbps montant et (N-1)*400 kbps descendant
  - 5–16 personnes : 184 kbps montant et (N-1)*134 kbps descendant
  - La bande passante montante et descendante s'adapte aux conditions du réseau
- Partage d'écran
  - 1,2 Mbps vers le haut (lors de la présentation) et vers le bas (lors de la visualisation) pour une qualité supérieure. L'adaptation se fait jusqu'à 320 kbps minimum en fonction des conditions du réseau.
  - Télécommande : 800 kbps fixes

Affichage des rapports

Pour permettre une prise de décisions plus avisées et augmenter la productivité de votre organisation, vous pouvez accéder à des données d'utilisation et des commentaires directement à partir de la console. Les données de rapport sont mises à jour quotidiennement, bien qu'il puisse y avoir un délai pouvant aller jusqu'à 48 heures.

Pour afficher les rapports d'utilisation et de commentaires

1. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
2. Choisissez Reports (Rapports), Dashboard (Tableau de bord).
3. Dans la page Usage and feedback dashboard report (Rapport du tableau de bord d'utilisation et de commentaire), vous pouvez consulter les données suivantes :

> **Note**
>
> Pour plus d'informations sur les données disponibles, consultez Tableau de bord des rapports Amazon Chime et informations sur l'activité utilisateur.

- Plage de dates (UTC) : plage de dates du rapport.
- Utilisateurs enregistrés : nombre d'utilisateurs qui se sont inscrits à Amazon Chime.
- Utilisateurs actifs : nombre d'utilisateurs qui ont participé à une réunion ou qui ont envoyé un message avec Amazon Chime.
- Réunions tenues : nombre total de réunions terminées. Vous pouvez sélectionner une réunion spécifique pour afficher les détails, en particulier l'ID de conférence, l'heure de début, l'organisateur, la durée et le nombre de participants. Choisissez une valeur Conference ID (ID de conférence) ou Meeting organizer (Organisateur de la réunion) spécifique pour afficher des détails supplémentaires, en particulier les participants, les événements du registre de la réunion, le type de client et les commentaires sur la réunion.
- Satisfaction à l'égard des réunions : pourcentage de réponses positives données à l' end-of-meeting enquête.
- Messages de chat envoyés : nombre de messages de chat envoyés par les utilisateurs.

Extension du client de bureau Amazon Chime

Vous pouvez étendre les fonctionnalités du client de bureau Amazon Chime en ajoutant des robots de discussion, des sessions téléphoniques par proxy et des webhooks. Les robots de discussion permettent aux utilisateurs d'effectuer des tâches telles que l'interrogation des systèmes internes pour obtenir des informations. Les sessions téléphoniques par proxy permettent aux utilisateurs d'appeler et d'envoyer des SMS sans révéler leur numéro de téléphone. Les webhooks peuvent envoyer automatiquement des messages aux forums de discussion. Par exemple, un webhook peut envoyer des rappels de réunion à une équipe, ainsi qu'un lien vers la réunion.

Rubriques

Gestion des utilisateurs

Les extraits de code suivants peuvent vous aider à gérer les utilisateurs d'Amazon Chime. Tous les exemples présentés dans cette rubrique utilisent Java.

Rubriques

Inviter plusieurs utilisateurs

L'exemple suivant montre comment inviter plusieurs utilisateurs à rejoindre un compte Amazon Chime. `Team`

```
List<String> emails = new ArrayList<>();
emails.add("janedoe@example.com");
emails.add("richardroe@example.net");
InviteUsersRequest inviteUsersRequest = new InviteUsersRequest()
```

```
    .withAccountId("chimeAccountId")
    .withUserEmailList(emails);

chime.inviteUsers(inviteUsersRequest);
```

Téléchargement de listes d'utilisateurs

L'exemple suivant montre comment télécharger au format une liste des utilisateurs associés à votre compte administratif Amazon Chime. `.csv`

```
BufferedWriter writer = Files.newBufferedWriter(Paths.get("/path/to/csv"));
CSVPrinter printer = new CSVPrinter(writer, CSVFormat.DEFAULT.withHeader("userId",
 "email"));

ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId(accountId)
    .withMaxResults(1);

boolean done = false;
while (!done) {
    ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);
    for (User user: listUsersResult.getUsers()) {
        printer.printRecord(user.getUserId(), user.getPrimaryEmail());
    }

    if (listUsersResult.getNextToken() == null) {
        done = true;
    }

    listUsersRequest = new ListUsersRequest()
        .withAccountId(accountId)
        .withNextToken(listUsersResult.getNextToken());
}

printer.close();
```

Déconnecter plusieurs utilisateurs

L'exemple suivant montre comment déconnecter plusieurs utilisateurs de votre compte administratif Amazon Chime.

```
ListUsersRequest listUsersRequest = new ListUsersRequest()
```

```
    .withAccountId("chimeAccountId");
ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);

for (User user: listUsersResult.getUsers()) {
    LogoutUserRequest logoutUserRequest = new LogoutUserRequest()
        .withAccountId(user.getAccountId())
        .withUserId(user.getUserId());

    chime.logoutUser(logoutUserRequest);
}
```

Mettre à jour les codes PIN personnels des utilisateurs

L'exemple suivant montre comment réinitialiser le code PIN de réunion personnel pour un utilisateur Amazon Chime spécifique.

```
ResetPersonalPINRequest request = new ResetPersonalPINRequest()
    .withAccountId("chimeAccountId")
    .withUserId("userId");

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

User user = result.getUser();
user.getPersonalPIN()
```

Intégration de chatbots dans le client de bureau Amazon Chime

Vous pouvez utiliser le pluginAWS Command Line Interface(AWS CLI), l'API Amazon Chime, ouAWSSDK pour intégrer les chatbots à Amazon Chime. Les chatbots vous permettent d'utiliser la puissance d'Amazon Lex,AWS Lambda, et d'autresAWSdes services destinés à rationaliser les tâches courantes grâce à des interfaces conversationnelles intelligentes accessibles aux utilisateurs dans les forums de discussion Amazon Chime.

Si vous êtes administrateur d'un compte Amazon Chime Enterprise, vous pouvez utiliser des chatbots pour permettre aux utilisateurs d'effectuer des tâches telles que :

- Interrogation de leurs systèmes internes pour obtenir des informations.
- Automatisation des tâches.
- Réception de notifications pour les problèmes critiques

- Création de tickets d'assistance.

Pour plus d'informations sur les comptes Amazon Chime Enterprise, consultezGestion de vos comptes Amazon Chime.

Si vous administrez un compte Amazon Chime Enterprise, vous pouvez créer jusqu'à 10 chatbots à intégrer à Amazon Chime. Les chatbots ne peuvent être utilisés que dans les salons de discussion créés par les membres de votre compte. Seuls les administrateurs de salons de discussion peuvent ajouter des chatbots à un salon de discussion. Une fois qu'un chatbot est ajouté à un salon de discussion, les membres du salon de discussion peuvent interagir avec le bot à l'aide des commandes fournies par le créateur du bot. Pour de plus amples informations, consultez la section suivante de cette rubrique.

Les utilisateurs de Linux et de macOS peuvent créer un exemple de chatbot personnalisé. Pour plus d'informations, veuillez consulter la rubriqueCréez des chatbots personnalisés pour Amazon Chime.

Content

Utilisation de chatbots avec Amazon Chime

Si vous administrez un compte Amazon Chime Enterprise, vous pouvez créer jusqu'à 10 chatbots à intégrer à Amazon Chime. Les chatbots ne peuvent être utilisés que dans les salons de discussion créés par les membres de votre compte. Seuls les administrateurs de salons de discussion peuvent ajouter des chatbots à un salon de discussion. Une fois qu'un chatbot est ajouté à un salon de discussion, les membres du salon de discussion peuvent interagir avec le bot à l'aide des commandes fournies par le créateur du bot. Pour plus d'informations, veuillez consulter la rubriqueUtiliser des chatbotsdans leGuide de l'utilisateur d'Amazon Chime.

Vous pouvez également utiliser le fonctionnement de l'API Amazon Chime pour activer ou arrêter les chatbots pour votre compte Amazon Chime. Pour plus d'informations, veuillez consulter Mettre à jour les chatbots.

> **Note**
>
> Vous ne pouvez pas supprimer de chatbots. Pour empêcher l'utilisation d'un chatbot sur votre compte, utilisez Amazon ChimeUpdateBotFonctionnement de l'API dansRéférence de l'API

Amazon Chime. Lorsque vous arrêtez un chatbot, les administrateurs de salon de discussion peuvent le supprimer d'un salon de discussion, mais ils ne peuvent pas l'ajouter à un salon de discussion. Les utilisateurs qui utilisent @mention un chatbot arrêté dans un salon de discussion reçoivent un message d'erreur.

Prérequis

Avant de commencer la procédure d'intégration de chatbots à Amazon Chime, remplissez les conditions préalables suivantes :

- Créez un chatbot.
- Créez le point de terminaison sortant pour Amazon Chime afin d'envoyer des événements à votre bot. Choisissez entre un ARN de fonction AWS Lambda ou un point de terminaison HTTPS. Pour plus d'informations sur Lambda, consultez le guide du développeur AWS Lambda.

Bonnes pratiques de DNS pour les points de terminaison HTTPS

Nous vous recommandons de suivre les bonnes pratiques ci-dessous lors de l'affectation d'un DNS pour votre point de terminaison HTTPS :

- Utilisez un sous-domaine DNS dédié au point de terminaison du robot.
- N'utilisez que des enregistrements A pour pointer vers le point de terminaison du robot.
- Protégez vos serveurs DNS et le serveur de registre DNS pour empêcher un détournement de noms de domaine.
- Utilisez les certificats intermédiaires TLS valides qui sont dédiées au point de terminaison du robot.
- Vérifiez cryptographiquement la signature du message du bot avant d'agir sur un message du bot.

Après avoir créé votre chatbot, utilisezAWS Command Line Interface(AWS CLI) ou le fonctionnement de l'API Amazon Chime pour effectuer les tâches décrites dans les sections suivantes.

Tâches

- Étape 1 : Intégrer un chatbot à Amazon Chime
- Étape 2 : configurer le point de terminaison de sortie d'un chatbot Amazon Chime
- Étape 3 : ajouter le chatbot à un salon de discussion Amazon Chime

- Authentifier les demandes de chatbot
- Mettre à jour les chatbots

Étape 1 : Intégrer un chatbot à Amazon Chime

Une fois que vous avez terminé leexigences, intégrez votre chatbot à Amazon Chime à l'aide duAWS CLIou API Amazon Chime.

> **Note**
>
> Ces procédures créent un nom et une adresse e-mail pour votre chatbot. Les noms et adresses e-mail des Chatbots ne peuvent pas être modifiés une fois qu'ils ont été créés.

AWS CLI

Pour intégrer un chatbot à l'aide duAWS CLI

1. Pour intégrer votre chatbot à Amazon Chime, utilisez lecreate-botcommande dans leAWS CLI.

```
aws chime create-bot --account-id 12a3456b-7c89-012d-3456-78901e23fg45 --display-
name exampleBot --domain example.com
```

   a. Entrez un nom d'affichage du chatbot comportant jusqu'à 55 caractères alphanumériques ou spéciaux (tels que +, -, %).

   b. Entrez le nom de domaine enregistré pour votre compte Amazon Chime Enterprise.

2. Amazon Chime renvoie une réponse qui inclut l'ID du bot.

```
"Bot": {
        "CreatedTimestamp": "timeStamp",
        "DisplayName": "exampleBot",
        "Disabled": exampleBotFlag,
        "UserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
        "BotId": "botId",
        "UpdatedTimestamp": "timeStamp",
        "BotType": "ChatBot",
        "SecurityToken": "securityToken",
        "BotEmail": "displayName-chimebot@example.com"
```

```
        }
```

3. Copiez et enregistrez l'ID et l'adresse e-mail du bot à utiliser dans les procédures suivantes.

API Amazon Chime

Pour intégrer un chatbot à l'aide de l'API Amazon Chime

1. Pour intégrer votre chatbot à Amazon Chime, utilisez leCreateBotFonctionnement de l'API dansRéférence de l'API Amazon Chime.

   a. Entrez un nom d'affichage du chatbot comportant jusqu'à 55 caractères alphanumériques ou spéciaux (tels que +, -, %).

   b. Entrez le nom de domaine enregistré pour votre compte Amazon Chime Enterprise.

2. Amazon Chime renvoie une réponse qui inclut l'ID du bot. Copiez et enregistrez l'identifiant et l'adresse e-mail du bot. L'adresse e-mail du bot ressemble à ceci :*exampleBot*-chimebot@*example.com*.

Kit SDK AWS pour Java

L'exemple de code suivant montre comment intégrer un chatbot à l'aide duAWSSDK pour Java.

```
CreateBotRequest createBotRequest = new CreateBotRequest()
    .withAccountId("chimeAccountId")
    .withDisplayName("exampleBot")
    .withDomain("example.com");

chime.createBot(createBotRequest);
```

Amazon Chime renvoie une réponse qui inclut l'ID du bot. Copiez et enregistrez l'identifiant et l'adresse e-mail du bot. L'adresse e-mail du bot ressemble à ceci :*exampleBot*-chimebot@*example.com*.

Étape 2 : configurer le point de terminaison de sortie d'un chatbot Amazon Chime

Après avoir créé un identifiant de chatbot pour votre compte Amazon Chime Enterprise, configurez votre point de terminaison sortant pour qu'Amazon Chime l'utilise pour envoyer des messages à votre bot. Le point de terminaison sortant peut être unAWS Lambdafonction ARN ou point de terminaison

HTTPS que vous avez créé dans le cadre duexigences. Pour plus d'informations sur Lambda, consultez le guide du développeur AWS Lambda.

> **Note**
>
> Si le point de terminaison HTTPS sortant de votre bot n'est pas configuré ou est vide, les administrateurs du salon de discussion ne peuvent pas ajouter le bot au salon de discussion. De plus, les utilisateurs du salon de discussion ne peuvent pas interagir avec le bot.

AWS CLI

Pour configurer un point de terminaison sortant pour votre chatbot, utilisez leput-events-configurationcommande dans leAWS CLI. Configurez un ARN de fonction Lambda ou un point de terminaison HTTPS sortant.

Lambda ARN

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --lambda-function-arn arn:aws:lambda:us-
east-1:111122223333:function:function-name
```

HTTPS endpoint

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --outbound-events-https-endpoint https://example.com:8000
```

Amazon Chime répond avec l'ID du bot et le point de terminaison HTTPS.

```
{
    "EventsConfiguration": {
        "BotId": "BotId",
        "OutboundEventsHTTPSEndpoint": "https://example.com:8000"
    }
}
```

API Amazon Chime

Pour configurer le point de terminaison sortant de votre chatbot, utilisez Amazon ChimePutEventsConfigurationFonctionnement de l'API dansRéférence de l'API Amazon Chime. Configurez un ARN de fonction Lambda ou un point de terminaison HTTPS sortant.

- Si vous configurez un ARN de fonction Lambda— Amazon Chime appelle Lambda pour ajouter l'autorisation d'autoriser l'administrateur Amazon Chime àAWScompte pour appeler l'ARN de la fonction Lambda fourni. Ceci est suivi d'une invocation de course à sec pour vérifier qu'Amazon Chime est autorisé à appeler la fonction. Si l'ajout d'autorisations échoue ou si l'invocation du dry run échoue, alors le`PutEventsConfiguration`La requête renvoie une erreur HTTP 4xx.
- Si vous configurez un point de terminaison HTTPS sortant— Amazon Chime vérifie votre point de terminaison en envoyant une requête HTTP Post avec une charge utile Challenge JSON au point de terminaison HTTPS sortant que vous avez indiqué à l'étape précédente. Votre point de terminaison HTTPS sortant doit répondre en renvoyant le paramètre Challenge au format JSON. Les exemples suivants illustrent la demande et une réponse valide.

  Request

```
HTTPS POST

JSON Payload:
{
   "Challenge":"00000000000000000000",
   "EventType" : "HTTPSEndpointVerification"
}
```

  Response

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "Challenge":"00000000000000000000"
}
```

Si le challenge handshake échoue, la demande `PutEventsConfiguration` renvoie une erreur HTTP 4xx.

Kit SDK AWS pour Java

L'exemple de code suivant montre comment configurer un point de terminaison à l'aide duAWSSDK pour Java.

```
PutEventsConfigurationRequest putEventsConfigurationRequest = new
 PutEventsConfigurationRequest()
     .withAccountId("chimeAccountId")
     .withBotId("botId")
     .withOutboundEventsHTTPSEndpoint("https://www.example.com")
     .withLambdaFunctionArn("arn:aws:lambda:region:account-id:function:function-name");

 chime.putEventsConfiguration(putEventsConfigurationRequest):
```

Étape 3 : ajouter le chatbot à un salon de discussion Amazon Chime

Seul un administrateur de salon de discussion peut ajouter un chatbot à un salon de discussion. Ils utilisent l'adresse e-mail du chatbot créée dansÉtape 1.

Pour ajouter un chatbot à une salle de conversation

1. Ouvrez le client de bureau ou l'application Web Amazon Chime.
2. Choisissez l'icône d'engrenage dans le coin supérieur droit, puis choisissezGérez les webhooks et les bots.
3. Choisissez Add bot (ajouter un robot).
4. PourAdresse de courrier électronique, entrez l'adresse e-mail du bot.
5. Choisissez Add (Ajouter).

Le nom du robot s'affiche dans la liste des salles de conversation. Si des actions supplémentaires sont nécessaires pour ajouter un chatbot à un salon de discussion, fournissez-les à l'administrateur du salon de discussion.

Une fois le chatbot ajouté au salon de discussion, fournissez les commandes du chatbot aux utilisateurs de votre salon de discussion. Pour ce faire, vous pouvez programmer votre chatbot pour

qu'il envoie une aide de commande au salon de discussion lorsqu'il reçoit l'invitation au salon de discussion. AWS recommande également de créer une commande d'aide que les utilisateurs de votre chatbot pourront utiliser.

Authentifier les demandes de chatbot

Vous pouvez authentifier les demandes envoyées à votre chatbot depuis un salon de discussion Amazon Chime. Pour ce faire, calculez une signature en fonction de la demande. Vérifiez ensuite que la signature calculée correspond à celle de l'en-tête de la demande. Amazon Chime utilise le hachage HMAC SHA256 pour générer la signature.

Si votre chatbot est configuré pour Amazon Chime à l'aide d'un point de terminaison HTTPS sortant, suivez les étapes d'authentification suivantes.

Pour valider une demande signée d'Amazon Chime concernant un chatbot avec un point de terminaison HTTPS sortant configuré

1. Obtenez l'en-tête Chime-Signature à partir de la demande HTTP.
2. Obtenez l'en-tête Chime-Request-Timestamp et le corps de la demande. Utilisez ensuite une barre verticale comme séparateur entre les deux éléments afin de former une chaîne.
3. Utilisez leSecurityTokende CreateBot réponse comme clé initiale deHMAC_SHA_256, et hachez la chaîne que vous avez créée à l'étape 2.
4. Encodez l'octet haché avec l'encodeur Base64 en une chaîne de signature.
5. Comparez cette signature calculée à celle de l'en-tête Chime Signature.

L'exemple de code suivant montre comment générer une signature à l'aide de Java.

```
       private final String DELIMITER = "|";
       private final String HMAC_SHA_256 = "HmacSHA256";

       private String generateSignature(String securityToken, String requestTime,
String requestBody)
       {
           try {
               final Mac mac = Mac.getInstance(HMAC_SHA_256);
               SecretKeySpec key = new SecretKeySpec(securityToken.getBytes(UTF_8),
HMAC_SHA_256);
               mac.init(key);
```

```
            String data = requestTime + DELIMITER + requestBody;
            byte[] rawHmac = mac.doFinal(data.getBytes(UTF_8));

            return Base64.getEncoder().encodeToString(rawHmac);
            }
        catch (Exception e) {
            throw e;
            }
    }
```

Le point de terminaison HTTPS sortant doit répondre à la demande Amazon Chime avec`200 0K`dans les 2 secondes. Sinon, la demande échoue. Si le point de terminaison HTTPS sortant n'est pas disponible au bout de 2 secondes, probablement en raison d'un délai de connexion ou de lecture, ou si Amazon Chime reçoit un code de réponse 5xx, Amazon Chime réessaie la demande deux fois. La première nouvelle tentative est envoyée 200 millisecondes après l'échec de la demande initiale. La deuxième nouvelle tentative est envoyée 400 millisecondes après l'échec de la nouvelle tentative précédente. Si le point de terminaison HTTPS sortant est toujours indisponible après la deuxième nouvelle tentative, la demande échoue.

> **Note**
>
> L'en-tête Chime-Request-Timestamp change chaque fois que la demande est renouvelée.

Si votre chatbot est configuré pour Amazon Chime à l'aide d'un ARN de fonction Lambda, suivez les étapes d'authentification suivantes.

Pour valider une demande signée d'Amazon Chime pour un chatbot avec une fonction Lambda (ARN) configurée

1. Obtenez leSignature de carillonetHorodatage de la demande Chime-Requestà partir de la requête LambdaClientContext, au format JSON codé en Base64.

   ```
   {
   "Chime-Signature" : "1234567890",
   "Chime-Request-Timestamp" : "2019-04-04T21:30:43.181Z"
   }
   ```

2. Obtenez le corps de la demande à partir de la charge utile de la demande.

3. Utilisez leSecurityTokendeCreateBotréponse comme clé initiale deHMAC_SHA_256, et hachez la chaîne que vous avez créée.
4. Encodez l'octet haché avec l'encodeur Base64 en une chaîne de signature.
5. Comparez cette signature calculée à celle de l'en-tête Chime Signature.

Si uncom.amazonaws.SdkClientExceptionse produit pendant l'appel Lambda, Amazon Chime réessaie la demande deux fois.

Mettre à jour les chatbots

En tant qu'administrateur du compte Amazon Chime, vous pouvez utiliser l'API Amazon Chime avec leAWSSDK ouAWS CLIpour consulter les détails de votre chatbot. Vous pouvez également activer ou empêcher l'utilisation de vos chatbots sur votre compte. Vous pouvez également régénérer les jetons de sécurité pour votre chatbot.

Pour de plus amples informations, consultez les rubriques suivantes duRéférence de l'API Amazon Chime:

- GetBot— Obtient les détails de votre chatbot, tels que l'adresse e-mail et le type de bot.
- UpdateBot— Active ou empêche l'utilisation d'un chatbot sur votre compte.
- RegenerateSecurityToken— Régénère le jeton de sécurité de votre chatbot.

Vous pouvez également modifier lePutEventsConfigurationpour votre chatbot. Par exemple, si votre chatbot a été initialement configuré pour utiliser un point de terminaison HTTPS sortant, vous pouvez supprimer la configuration d'événements précédente et créer une nouvelle configuration d'événements pour un ARN de fonction Lambda.

Pour de plus amples informations, consultez les rubriques suivantes duRéférence de l'API Amazon Chime:

- DeleteEventsConfiguration
- PutEventsConfiguration

Événements Amazon Chime envoyés aux chatbots

Les événements suivants sont envoyés à votre chatbot depuis Amazon Chime :

- Inviter— Envoyé lorsque votre chatbot est ajouté à un salon de discussion Amazon Chime
- Mentionner— Envoyé lorsqu'un utilisateur d'un salon de discussion @mentions votre chatbot
- Supprimer— Envoyé lorsque votre chatbot est retiré d'un salon de discussion Amazon Chime

Les exemples suivants montrent la charge utile JSON envoyée à votre chatbot pour chacun de ces événements.

Example : Inviter un événement

```
            {
              "Sender": {
                           "SenderId": "user@example.com",
                           "SenderIdType": "EmailId"
                         },
              "Discussion": {
                           "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                           "DiscussionType": "Room"
                           },
              "EventType": "Invite",
              "InboundHttpsEndpoint": {
                                        "EndpointType": "Persistent",
                                        "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                      },
              "EventTimestamp": "2019-04-04T21:27:52.736Z"
            }
```

Example : Mentionnez un événement

```
            {
                "Sender": {
                           "SenderId": "user@example.com",
                           "SenderIdType": "EmailId"
                         },
                "Discussion": {
                               "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                               "DiscussionType": "Room"
```

```
                            },
                "EventType": "Mention",
                "InboundHttpsEndpoint": {
                                            "EndpointType": "ShortLived",
                                            "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                        },
                "EventTimestamp": "2019-04-04T21:30:43.181Z",
                "Message": "@botDisplayName@example.com Hello Chatbot"
            }
```

> **Note**
>
> L'URL `InboundHttpsEndpoint` d'un événement Mention expire 2 minutes après son envoi.

Example : Supprimer un événement

```
            {
                "Sender": {
                            "SenderId": "user@example.com",
                            "SenderIdType": "EmailId"
                          },
                "Discussion": {
                               "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                               "DiscussionType": "Room"
                             },
                "EventType": "Remove",
                "EventTimestamp": "2019-04-04T21:27:29.626Z"
            }
```

Création de webhooks pour Amazon Chime

Les webhooks permettent aux applications Web de communiquer entre elles en temps réel. Généralement, les webhooks envoient des notifications lorsqu'une action se produit. Supposons, par exemple, que vous gérez un site d'achat en ligne. Les webhooks peuvent vous avertir lorsqu'un client

ajoute des articles à son panier, paie une commande ou envoie un commentaire. Les webhooks ne nécessitent pas autant de programmation que les applications traditionnelles et n'utilisent pas autant de puissance de traitement. Sans webhook, un programme doit rechercher des données fréquemment afin de les obtenir en temps réel. Avec un webhook, l'application d'envoi publie les données immédiatement.

Les webhooks entrants que vous créez peuvent envoyer des messages de manière programmatique aux salons de discussion Amazon Chime. Par exemple, un webhook peut informer une équipe du service client de la création d'un nouveau ticket prioritaire et ajouter un lien vers le ticket dans le salon de discussion.

Les messages de webhooks peuvent être mis en forme avec Markdown et peuvent inclure des émoticônes. Les liens HTTP et les adresses e-mail s'affichent sous forme de liens actifs. Les messages peuvent également inclure les annotations @All et @Present pour alerter respectivement tous les membres et les membres présents d'une salle de conversation. Pour mentionner (@mention) directement un participant d'une salle de conversation, utilisez son alias ou son adresse e-mail complète. Par exemple, `@alias` ou `@alias@domain.com`.

Les webhooks peuvent uniquement faire partie d'un salon de discussion et ne peuvent pas être partagés. Les administrateurs de salon de discussion Amazon Chime peuvent ajouter jusqu'à 10 webhooks pour chaque salon de discussion.

Après avoir créé un webhook, vous pouvez l'intégrer à un salon de discussion Amazon Chime, comme indiqué dans la procédure suivante.

Pour intégrer un webhook à un salon de discussion

1. Obtenez l'URL du webhook auprès de l'administrateur du salon de discussion. Pour plus d'informations, voirAjouter des webhooks à un salon de discussiondans leGuide de l'utilisateur d'Amazon Chime.
2. Utilisez l'URL du webhook dans le script ou l'application que vous avez créé pour envoyer des messages au salon de discussion :

   a. L'URL accepte une requête HTTP POST.

   b. Les webhooks Amazon Chime acceptent une charge utile JSON à l'aide d'une seule cléContenu. Voici un exemple de commande curl avec un exemple de charge utile :

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/
json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
```

```
sample.com email test: marymajor@example.com All member callout: @All All
 Present member callout: @Present"}'
```

Ce qui suit est un exemplePowerShellcommande pour les utilisateurs de Windows :

```
Invoke-WebRequest -Uri '<Insert your webhook URL here>' -Method 'Post' -
ContentType 'application/JSON' -Body '{"Content":"Message Body emoji test: :) :
+1: link test: http://sample.com email test: marymajor@example.com All member
 callout: @All All Present member callout: @Present"}'
```

Lorsque le programme externe envoie la requête HTTP POST à l'URL de webhook, le serveur vérifie que le webhook est valide et qu'une salle de conversation lui est attribuée. Le webhook s'affiche dans la liste de la salle de conversation avec une icône de webhook en regard de son nom. Les messages de la salle de conversation envoyés par le webhook apparaissent dans la salle de conversation sous le nom du webhook suivi de (Webhook).

> **Note**
>
> CORS n'est actuellement pas activé pour les webhooks.

Résolution des erreurs liées au webhook

voici une liste d'erreurs liées aux webhooks :

- La limite de fréquence de webhook entrant par webhook est de 1 TPS par salle de conversation. La limitation entraîne une erreur HTTP 429.
- La taille des messages publiés par un webhook doit être inférieure ou égale à 4 Ko. Une charge utile de message plus importante génère une erreur HTTP 413.
- Les messages publiés par un webhook avec des annotations @All et @Present fonctionnent uniquement pour les salles de conversation avec 50 membres maximum. S'il existe plus de 50 membres, une erreur HTTP 400 est générée.
- Si l'URL de webhook est régénérée, l'utilisation de l'ancienne URL génère une erreur HTTP 404.
- Si l'URL de webhook est supprimée, l'utilisation de l'ancienne URL génère une erreur HTTP 404.
- Des URL de webhook non valides génèrent des erreurs HTTP 403.
- Si le service n'est pas disponible, l'utilisateur reçoit une erreur HTTP 503 dans la réponse.

Support administratif pour Amazon Chime

> **Note**
>
> Pour obtenir de l'aide concernant votre compte d'achat Amazon, rendez-vous sur le service client sur amazon.com.

Si vous devez contacter le support technique d'Amazon Chime, choisissez l'une des options suivantes :

- Si vous avez un compte AWS Support, rendez-vous au Centre d'assistance et envoyez un ticket.
- Sinon, ouvrez le AWS Management Consoleet choisissez Amazon Chime, Support, Submit request.

Fournissez autant d'informations que possible parmi les suivantes :

- Description détaillée du problème.
- Heure à laquelle le problème s'est produit et indication de votre fuseau horaire.
- Votre version d'Amazon Chime. Pour trouver votre numéro de version :
  - Dans Windows, choisissez Aide, À propos d'Amazon Chime.
  - Dans macOS, choisissez Amazon Chime, About Amazon Chime (À propos d'Amazon Chime).
  - Dans iOS et Android, choisissez Settings (Paramètres), About (À propos de).
- ID de référence du journal. Pour trouver cet ID :
  - Dans Windows et macOS, choisissez Help (Aide), Send Diagnostic Logs (Envoyer des journaux de diagnostic).
  - Dans iOS et Android, choisissez Settings (Paramètres), Send Diagnostic Logs (Envoyer des journaux de diagnostic).
- ID de la réunion si votre problème concerne à une réunion.

Sécurité dans Amazon Chime

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 cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Chime, consultez la section Services AWS concernés par programme de conformité Services AWS .
- 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 Chime. Les rubriques suivantes expliquent comment configurer Amazon Chime pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services AWS qui vous aident à surveiller et à sécuriser vos ressources Amazon Chime.

Rubriques

- Utilisation des rôles liés à un service pour Amazon Chime
- Journalisation et surveillance dans Amazon Chime
- Validation de conformité pour Amazon Chime
- Résilience dans Amazon Chime
- Sécurité de l'infrastructure dans Amazon Chime
- Comprendre les mises à jour automatiques d'Amazon Chime

Gestion des identités et des accès pour Amazon Chime

AWS Identity and Access Management (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 Chime. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon Chime.

Utilisateur du service : si vous utilisez le service Amazon Chime pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'Amazon Chime dans le cadre de votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Amazon Chime, consultez. Résolution des problèmes d'identité et d'accès à Amazon Chime

Administrateur du service — Si vous êtes responsable des ressources Amazon Chime au sein de votre entreprise, vous avez probablement un accès complet à Amazon Chime. C'est à vous de déterminer les fonctionnalités et les ressources Amazon Chime auxquelles les utilisateurs de votre

service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Amazon Chime, consultez. Comment Amazon Chime fonctionne avec IAM

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon Chime. Pour consulter des exemples de politiques basées sur l'identité Amazon Chime que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité Amazon Chime

Authentification par des identités

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

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser

l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

AWS utilisateur root du compte

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service.

FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des 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 est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des

documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. Pour la ressource dans laquelle se trouve la politique,

cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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.

AWS politiques gérées pour Amazon Chime

Pour ajouter des autorisations à des utilisateurs, des groupes et des rôles, il est plus facile d'utiliser des politiques gérées par AWS que d'écrire des politiques 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.

AWS les 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 parfois des autorisations supplémentaires à une politique AWS gérée 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 plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque 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 ReadOnlyd'accès AWS géré fournit un accès en lecture seule à tous les AWS services et ressources. Quand un service lance une nouvelle fonctionnalité, 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.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance 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 Chime fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon Chime, vous devez connaître les fonctionnalités IAM disponibles avec Amazon Chime. Pour obtenir une vue d'ensemble de la manière dont Amazon Chime et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur l'identité Amazon Chime
- Ressources
- Exemples

Politiques basées sur l'identité Amazon Chime

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 Chime 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. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations

nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Clés de condition

Amazon Chime ne fournit aucune clé de condition spécifique au service. Pour afficher toutes les clés de condition globales AWS , consultez la rubrique Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Ressources

Amazon Chime ne prend pas en charge la spécification des ARN des ressources dans une politique.

Exemples

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

Prévention du problème de l'adjoint confus entre services

Le problème des adjoints confus est un problème de sécurité de l'information qui se produit lorsqu'une entité non autorisée à effectuer une action appelle une entité plus privilégiée pour effectuer l'action. Cela peut permettre à des acteurs malveillants d'exécuter des commandes ou de modifier des ressources qu'ils n'auraient pas l'autorisation d'exécuter ou d'accéder autrement. Pour plus d'informations, consultez la section Le problème de confusion des adjoints dans le guide de AWS Identity and Access Management l'utilisateur.

Dans AWS, l'usurpation d'identité interservices peut mener à un scénario d'adjoint confus. L'usurpation d'identité entre services se produit lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Un acteur malveillant peut utiliser le service d'appel pour modifier les ressources d'un autre service en utilisant des autorisations qu'il n'aurait pas normalement obtenues.

AWS fournit aux responsables du service un accès géré aux ressources de votre compte afin de vous aider à protéger la sécurité de vos ressources. Nous vous recommandons d'utiliser la clé de contexte

des conditions `aws:SourceAccount` globales dans vos politiques de ressources. Ces clés limitent les autorisations qu'Amazon Chime accorde à un autre service pour cette ressource.

L'exemple suivant montre une politique de compartiment S3 qui utilise la clé de contexte de condition `aws:SourceAccount` globale dans le compartiment `CallDetailRecords` S3 configuré pour éviter le problème de confusion des adjoints.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonChimeAclCheck668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your-cdr-bucket"
        },
        {
            "Sid": "AmazonChimeWrite668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your-cdr-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "112233446677"
                }
            }
        }
    ]
}
```

Politiques basées sur les ressources Amazon Chime

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

Autorisation basée sur les balises Amazon Chime

Amazon Chime ne prend pas en charge le balisage des ressources ni le contrôle d'accès en fonction des balises.

Rôles IAM d'Amazon Chime

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

Utilisation d'informations d'identification temporaires avec Amazon Chime

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 STS API telles que AssumeRoleou GetFederationToken.

Amazon Chime 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 qui exécutent des actions en votre nom. Les rôles liés à un service apparaissent dans votre compte IAM, et les services possèdent les rôles. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

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

Rôles de 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 Chime ne prend pas en charge les rôles de service.

Exemples de politiques basées sur l'identité Amazon Chime

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou à modifier des ressources Amazon Chime. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS 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

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon Chime 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 votre Compte 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.

- Accorder 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser 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 spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique 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 le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 console Amazon Chime

Pour accéder à la console Amazon Chime, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon Chime 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 console Amazon Chime, associez également la AmazonChimeReadOnlypolitique AWS gérée suivante aux entités. Pour plus d'informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:List*",
                "chime:Get*",
                "chime:SearchAvailablePhoneNumbers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

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

Permettre aux utilisateurs un accès complet à Amazon Chime

La AmazonChimeFullAccesspolitique AWS gérée suivante accorde à un utilisateur IAM un accès complet aux ressources Amazon Chime. La politique donne à l'utilisateur l'accès à toutes les opérations Amazon Chime, ainsi qu'à d'autres opérations qu'Amazon Chime doit être en mesure d'effectuer en votre nom.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        },
        {
            "Action": [
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:DescribeResourcePolicies",
                "logs:PutResourcePolicy",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:CreateQueue"
            ],
```

```
            "Resource": [
                "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
            ]
        }
    ]
}
```

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 or AWS .

```
{
    "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": "*"
        }
    ]
}
```

Autorisation des utilisateurs à accéder aux actions de gestion des utilisateurs

Utilisez la AmazonChimeUserManagementpolitique AWS gérée pour autoriser les utilisateurs à accéder aux actions de gestion des utilisateurs dans la console Amazon Chime.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
                "chime:GetUser",
                "chime:GetUserByEmail",
                "chime:InviteUsers",
                "chime:InviteUsersFromProvider",
                "chime:SuspendUsers",
                "chime:ActivateUsers",
                "chime:UpdateUserLicenses",
                "chime:ResetPersonalPIN",
                "chime:LogoutUser",
                "chime:ListDomains",
                "chime:GetDomain",
                "chime:ListDirectories",
                "chime:ListGroups",
                "chime:SubmitSupportRequest",
                "chime:ListDelegates",
                "chime:ListAccountUsageReportData",
                "chime:GetMeetingDetail",
                "chime:ListMeetingEvents",
                "chime:ListMeetingsReportData",
                "chime:GetUserActivityReportData",
```

```
                "chime:UpdateUser",
                "chime:BatchUpdateUser",
                "chime:BatchSuspendUser",
                "chime:BatchUnsuspendUser",
                "chime:AssociatePhoneNumberWithUser",
                "chime:DisassociatePhoneNumberFromUser",
                "chime:GetPhoneNumber",
                "chime:ListPhoneNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime:AssociateSigninDelegateGroupsWithAccount",
                "chime:DisassociateSigninDelegateGroupsFromAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`Cela permet aux connecteurs vocaux Amazon Chime de diffuser du contenu multimédia sur Amazon Kinesis Video Streams, de fournir des notifications de streaming et de synthétiser la parole à l'aide d'Amazon Polly. Cette politique accorde au service Amazon Chime Voice Connector l'autorisation d'accéder aux Amazon Kinesis Video Streams du client, d'envoyer des événements de notification à Amazon Simple Notification Service et Amazon Simple Queue Service, et d'utiliser Amazon Polly pour synthétiser la parole lors de l'utilisation des applications vocales et des actions du SDK Amazon Chime. `Speak` `SpeakAndGetDigits` Pour plus d'informations, consultez les exemples de politiques basées sur l'identité du SDK Amazon Chime dans le guide de l'administrateur du SDK Amazon Chime.

Amazon Chime met à jour les politiques gérées AWS

Le tableau suivant répertorie et décrit les mises à jour apportées à la politique Amazon Chime IAM.

Modification	Description	Date
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Mise à jour d'une stratégie existante	Amazon Chime Voice Connectors a ajouté de nouvelles autorisations pour vous permettre d'utiliser Amazon Polly pour synthétiser la parole. Ces autorisations sont requises pour utiliser les `Speak` actions et `SpeakAndGetDigits` dans les applications vocales du SDK Amazon Chime.	15 mars 2022
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Mise à jour d'une politique existante	Amazon Chime Voice Connector a ajouté de nouvelles autorisations pour autoriser l'accès à Amazon Kinesis Video Streams et envoyer des événements de notification aux réseaux sociaux et SQS. Ces autorisations sont requises pour que les connecteurs Amazon Chime Voice puissent diffuser du contenu multimédia sur Amazon Kinesis Video Streams et fournir des notifications de diffusion.	20 décembre 2021
Modification de la politique existante. Création d'utilisateurs ou de rôles IAM avec la politique du SDK Chime.	Amazon Chime a ajouté de nouvelles actions pour prendre en charge la validation étendue. Un certain nombre d'actions ont été ajoutées pour	23 septembre 2021

Modification	Description	Date
	permettre de répertorier et de baliser les participants et les ressources de la réunion, ainsi que pour démarrer et arrêter la transcription de la réunion.	
Amazon Chime a commencé à suivre les modifications	Amazon Chime a commencé à suivre les modifications apportées à ses politiques AWS gérées.	23 septembre 2021

Résolution des problèmes d'identité et d'accès à Amazon Chime

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

Rubriques

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

Je ne suis pas autorisé à effectuer une action dans Amazon Chime

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `chime:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 chime:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `chime:GetWidget`.

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

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 Chime.

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, un utilisateur doit 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 dans Amazon Chime. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer 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 ressources Amazon Chime

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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon Chime prend en charge ces fonctionnalités, consultez. Comment Amazon Chime fonctionne 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 tiers Comptes 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 connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation des rôles liés à un service pour Amazon Chime

Amazon Chime utilise des rôles liés à des servicesAWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Amazon Chime. Les rôles liés à un service sont prédéfinis par Amazon Chime et incluent toutes les autorisations requises par le service pour appeler d'autresAWS services en votre nom.

Un rôle lié à un service rend la configuration d'Amazon Chime plus efficace, car vous n'êtes pas obligé d'ajouter manuellement les autorisations nécessaires. Amazon Chime définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Amazon Chime peut endosser ses rôles. Les autorisations définies comprennent la stratégie d'approbation et la stratégie d'autorisations. La stratégie d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources Amazon Chime sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour obtenir des informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez les services qui comportent

un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Rubriques

- Utilisation de rôles avec des appareils Alexa for Business partagés
- Utilisation de rôles avec transcription en direct
- Utilisation de rôles avec les pipelines multimédia du SDK Amazon Chime

Utilisation de rôles avec des appareils Alexa for Business partagés

Les informations des sections suivantes expliquent comment utiliser les rôles liés à des services et accorder à Amazon Chime l'accès aux ressources Alexa for Business de votreAWS compte.

Rubriques

- Autorisations des rôles liés à un service pour Amazon Chime
- Création d'un rôle lié à un service pour Amazon Chime
- Modification d'un rôle lié à un service pour Amazon Chime
- Suppression d'un rôle lié à un service pour Amazon Chime
- Régions prises en charge pour les rôles liés à un service Amazon Chime

Autorisations des rôles liés à un service pour Amazon Chime

Amazon Chime utilise le rôle lié à un service appelé AWSServiceRoleForAmazonChime: permet d'accéder auxAWS services et ressources utilisés ou gérés par Amazon Chime, tels que les appareils partagés Alexa for Business.

Le rôle AWSServiceRoleForAmazonChime lié à un service approuve les services suivants pour assumer le rôle :

- `chime.amazonaws.com`

La politique d'autorisations liée au rôle permet à Amazon Chime d'effectuer l'action suivante sur la ressource spécifiée :

- Action : `iam:CreateServiceLinkedRole` sur `arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime`

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 Chime

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez Alexa for Business pour un appareil partagé dans Amazon Chime dansAWS Management ConsoleAWS CLI, ou l'AWSAPI, Amazon Chime crée automatiquement le rôle lié au service.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation Amazon Chime. Dans l'interface AWS CLI ou l'API AWS, créez un rôle lié à un service avec le nom de service `chime.amazonaws.com`. Pour de plus amples informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

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

Amazon Chime ne vous permet pas de modifier le rôle AWSServiceRoleForAmazonChime lié à un 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 à ce 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.

Suppression d'un rôle lié à un service pour Amazon Chime

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

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle.

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

Pour supprimer les ressources Amazon Chime utilisées par AWSServiceRoleForAmazonChime (console)

- Désactivez Alexa for Business pour tous les appareils partagés sur votre compte Amazon Chime.

  a. Ouvrez la console Amazon Chime à l'adresse https://chime.aws.amazon.com/.
  b. Choisissez Utilisateurs, Appareils partagés.
  c. Sélectionnez un appareil.
  d. Sélectionnez Actions.
  e. Choisissez Désactiver Alexa for Business.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForAmazonChime. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Amazon Chime

Amazon Chime prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Points de terminaison et quotas Amazon Chime.

Utilisation de rôles avec transcription en direct

Les informations contenues dans les sections suivantes expliquent comment créer et gérer un rôle lié à un service avec Amazon Chime Live Transcription. Pour plus d'informations sur le service de transcription en direct, consultez la section Utilisation de la transcription en direct du SDK Amazon Chime.

Rubriques

- Régions prises en charge Amazon Chime Rôle lié à Amazon Chime Service Amazon Chime.

Autorisations du rôle lié à Amazon Chime Live Transcription. Amazon Chime Live Transcription.

Amazon Chime Live Transcription utilise un rôle lié à un service nommé AWSServiceRoleForAmazonChimeTranscription: « Permet à Amazon Chime d'accéder à Amazon Transcribe et Amazon Transcribe Medical en votre nom ».

Le rôle AWSServiceRoleForAmazonChimeTranscription lié à un service.

- `transcription.chime.amazonaws.com`

La politique d'autorisations liée à Amazon Chime. Amazon Chime peut effectuer les actions suivantes sur les ressources spécifiées :

- Action : `transcribe:StartStreamTranscription` sur `all AWS resources`
- Action : `transcribe:StartMedicalStreamTranscription` sur `all AWS resources`

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 Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à Amazon Chime Live Transcription. Amazon Chime Live Transcription.

Vous utilisez la console IAM pour créer un rôle lié au service avec le cas d'utilisation Chime Transcription.

> **Note**
>
> Vous devez disposer des autorisations administratives IAM pour effectuer ces étapes. Si ce n'est pas le cas, contactez un administrateur système.

Pour créer le rôle

1. Connectez-vous à la console de gestion AWS et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
3. Choisissez le type de rôle AWS Service, puis Chime, puis Chime Transcription.
4. Choisissez Suivant.
5. Choisissez Suivant.
6. Modifiez la description selon vos besoins, puis choisissez Créer un rôle.

Vous pouvez également utiliser leAWS CLI ou l'AWSAPI pour créer un rôle lié au service avec le nom transcription.chime.amazonaws.com.

Dans l'interface de ligne de commande, exécutez cette commande :`aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Amazon Chime Live Transcription. Amazon Chime Live Transcription.

Amazon Chime ne vous permet pas de modifier le rôle AWSServiceRoleForAmazonChimeTranscription lié à un 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 à ce rôle. Toutefois, vous pouvez utiliser IAM pour modifier la description du rôle. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à Amazon Chime Live Transcription. Amazon Chime Live Transcription.

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

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

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForAmazonChimeTranscription. Pour plus d'informations, veuillez consulter Deleting a Service-Linked Role (Suppression d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Régions prises en charge Amazon Chime Rôle lié à Amazon Chime Service Amazon Chime.

Amazon Chime 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 les sections Points de terminaison et quotas Amazon Chime et Utilisation des régions multimédia du SDK Amazon Chime.

Utilisation de rôles avec les pipelines multimédia du SDK Amazon Chime

Les informations dans les sections suivantes expliquent comment créer et gérer un rôle lié à un service pour Amazon Chime SDK Media Pipelines.

Rubriques

- Autorisations des rôles liés à un service pour les pipelines multimédia du SDK Amazon Chime
- Création d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime
- Modification d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime
- Suppression d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime
- Régions prises en charge pour les rôles liés à un service dans les pipelines multimédia du SDK Amazon Chime

Autorisations des rôles liés à un service pour les pipelines multimédia du SDK Amazon Chime

Amazon Chime utilise le rôle lié au service nommé AWSServiceRoleForAmazonChimeSDKMediaPipelines: permet aux pipelines multimédia du SDK Amazon Chime d'accéder aux réunions du SDK Amazon Chime en votre nom.

Le rôle AWSServiceRoleForAmazonChimeSDKMediaPipelines lié à un service approuve les services suivants pour assumer le rôle :

- `mediapipelines.chime.amazonaws.com`

Le rôle permet à Amazon Chime d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `chime:CreateAttendee` sur `all AWS resources`
- Action : `chime:DeleteAttendee` sur `all AWS resources`
- Action : `chime:GetMeeting` sur `all AWS resources`

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 Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime

Vous utilisez la console IAM pour créer un rôle lié à un service avec le cas d'utilisation Amazon Chime SDK Media Pipelines*.

> **Note**
>
> Vous devez disposer des autorisations administratives IAM pour effectuer ces étapes. Si ce n'est pas le cas, contactez un administrateur système.

Pour créer le rôle

1. Connectez-vous à la console de gestion AWS et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
3. Choisissez le type de rôle AWSService, puis Chime, puis Chime SDK Media Pipelines.
4. Choisissez Suivant.
5. Choisissez Suivant.
6. Modifiez la description selon vos besoins, puis choisissez Créer un rôle.

Vous pouvez également utiliserAWS CLI ou l'AWSAPI pour créer un rôle lié à un service appelé mediapipelines.chime.amazonaws.com.

Dans leAWS CLI, exécutez cette commande :`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime

Amazon Chime ne vous permet pas de modifier le rôle AWSServiceRoleForAmazonChimeSDKMediaPipelines lié à un 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 à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour les pipelines multimédia du SDK Amazon Chime

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

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

Utilisez la console IAM, l'AWS CLI ou l'API AWS pour supprimer le rôle lié à un service AWSServiceRoleForAmazonChimeSDKMediaPipelines. Pour plus d'informations, veuillez consulter Deleting a Service-Linked Role (Suppression d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service dans les pipelines multimédia du SDK Amazon Chime

Amazon Chime prend en charge l'utilisation des rôles liés à un service dans toutes lesAWS régions où le service est disponible. Pour plus d'informations, consultez Points de terminaison et quotas Amazon Chime.

Journalisation et surveillance dans Amazon Chime

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'Amazon Chime et de vos autresAWS solutions. AWSfournit les outils suivants pour surveiller Amazon Chime, signaler les problèmes et déclencher des actions automatiques, si nécessaire :

- Amazon CloudWatch surveille vosAWS ressources et les applications que vous exécutez sur en temps réelAWS. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez connaître l' CloudWatch utilisation du processeur ou d'autres métriques de vos instances Amazon EC2 et démarrer automatiquement de nouvelles instances lorsque cela est nécessaire. Pour de plus amples informations, veuillez consulter le Guide de CloudWatch l'utilisateur Amazon.
- Amazon EventBridge fournit un flux d'événements système en temps quasi réel qui décrivent les modifications apportées auxAWS ressources. EventBridge permet de procéder à des calculs automatisés dirigés par les événements. Vous pouvez ainsi écrire des règles qui recherchent certains événements et déclenchent des actions automatisées dans d'autres services AWS lorsque ces événements se produisent. Pour de plus amples informations, veuillez consulter le Guide de EventBridge l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, stocker et accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent contrôler les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur Amazon CloudWatch Logs.
- AWS CloudTrail capture les appels d'API et les événements associés effectués par votre compte AWS ou au nom de ce dernier. Puis, il livre les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

- Journalisation des appels d'API Amazon Chime avecAWS CloudTrail

Surveillance d'Amazon Chime avec Amazon CloudWatch

Vous pouvez contrôler Amazon Chime à l'aide de CloudWatch, qui collecte les données brutes et les transforme en métriques lisibles en quasi temps réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour de plus amples informations, veuillez consulter le Guide de CloudWatch l'utilisateur Amazon.

CloudWatch métriques pour Amazon Chime

Amazon Chime envoie les métriques suivantes à CloudWatch.

L'espace de`AWS/ChimeVoiceConnector` noms inclut les statistiques suivantes pour les numéros de téléphone attribués à votreAWS compte et aux connecteurs vocaux Amazon Chime.

Métrique	Description
`InboundCallAttempts`	Nombre d'appels entrants tentés. Unités : nombre
`InboundCallFailures`	Nombre d'échecs d'appels entrants. Unités : nombre
`InboundCallsAnswered`	Nombre d'appels entrants qui reçoivent une réponse. Unités : nombre
`InboundCallsActive`	Nombre d'appels entrants actuellement actifs. Unités : nombre
`OutboundCallAttempts`	Nombre d'appels sortants tentés.

Métrique	Description
	Unités : nombre
`OutboundCallFailures`	Nombre d'échecs d'appels sortants. Unités : nombre
`OutboundCallsAnswered`	Nombre d'appels sortants qui reçoivent une réponse. Unités : nombre
`OutboundCallsActive`	Nombre d'appels sortants actuellement actifs. Unités : nombre
`Throttles`	Nombre de fois où votre compte est limité lorsque vous tentez d'effectuer un appel. Unités : nombre
`Sip1xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 1xx. Unités : nombre
`Sip2xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 2xx. Unités : nombre
`Sip3xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 3xx. Unités : nombre
`Sip4xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 4xx. Unités : nombre

Métrique	Description
`Sip5xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 5xx. Unités : nombre
`Sip6xxCodes`	Nombre de messages SIP avec des codes d'état de niveau 6xx. Unités : nombre
`CustomerToVcRtpPackets`	Nombre de paquets RTP envoyés par le client à l'infrastructure Amazon Chime Voice Connector. Unités : nombre
`CustomerToVcRtpBytes`	Nombre d'octets envoyés par le client à l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTP. Unités : nombre
`CustomerToVcRtcpPackets`	Nombre de paquets RTCP envoyés par le client à l'infrastructure Amazon Chime Voice Connector. Unités : nombre
`CustomerToVcRtcpBytes`	Nombre d'octets envoyés par le client à l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTCP. Unités : nombre

Métrique	Description
`CustomerToVcPacketsLost`	Nombre de paquets perdus lors du transit entre le client et l'infrastructure Amazon Chime Voice Connector. Unités : nombre
`CustomerToVcJitter`	Instabilité moyenne des paquets envoyés par le client à l'infrastructure Amazon Chime Voice Connector. Unités : microsecondes
`VcToCustomerRtpPackets`	Nombre de paquets RTP envoyés au client depuis l'infrastructure Amazon Chime Voice Connector. Unités : nombre
`VcToCustomerRtpBytes`	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector au client sous forme de paquets RTP. Unités : nombre
`VcToCustomerRtcpPackets`	Nombre de paquets RTCP envoyés au client depuis l'infrastructure Amazon Chime Voice Connector. Unités : nombre
`VcToCustomerRtcpBytes`	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector au client sous forme de paquets RTCP. Unités : nombre

Métrique	Description
VcToCustomerPacketsLost	Nombre de paquets perdus lors du transit entre l'infrastructure Amazon Chime Voice Connector et le client. Unités : nombre
VcToCustomerJitter	Instabilité moyenne des paquets envoyés au client depuis l'infrastructure Amazon Chime Voice Connector. Unités : microsecondes
RTTBetweenVcAndCustomer	Le temps aller-retour moyen entre le client et l'infrastructure Amazon Chime Voice Connector . Unités : microsecondes
MOSBetweenVcAndCustomer	Le score d'opinion moyen (MOS) estimé associé aux flux vocaux entre le client et l'infrastructure Amazon Chime Voice Connector . Unités : score entre 1.0 et 4.4. Un score plus élevé indique une meilleure qualité audio perçue.
RemoteToVcRtpPackets	Nombre de paquets RTP envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector. Unités : nombre
RemoteToVcRtpBytes	Nombre d'octets envoyés de l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTP. Unités : nombre

Métrique	Description
RemoteToVcRtcpPackets	Nombre de paquets RTCP envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector. Unités : nombre
RemoteToVcRtcpBytes	Nombre d'octets envoyés de l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTCP. Unités : nombre
RemoteToVcPacketsLost	Nombre de paquets perdus lors du transit entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector. Unités : nombre
RemoteToVcJitter	Instabilité moyenne des paquets envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector. Unités : microsecondes
VcToRemoteRtpPackets	Nombre de paquets RTP envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante. Unités : nombre
VcToRemoteRtpBytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante sous forme de paquets RTP. Unités : nombre

Métrique	Description
VcToRemoteRtcpPackets	Nombre de paquets RTCP envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante. Unités : nombre
VcToRemoteRtcpBytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante sous forme de paquets RTCP. Unités : nombre
VcToRemotePacketsLost	Nombre de paquets perdus lors du transit entre l'infrastructure Amazon Chime Voice Connector et l'extrémité distante. Unités : nombre
VcToRemoteJitter	Instabilité moyenne des paquets envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante. Unités : microsecondes
RTTBetweenVcAndRemote	Le temps moyen aller-retour entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector. Unités : microsecondes
MOSBetweenVcAndRemote	Le score d'opinion moyen (MOS) estimé associé aux flux vocaux entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector. Unités : Unités : score entre 1.0 et 4.4. Un score plus élevé indique une meilleure qualité audio perçue.

CloudWatch dimensions pour Amazon Chime

Les CloudWatch dimensions que vous pouvez utiliser avec Amazon Chime figurent ci-dessous.

Dimension	Description
`VoiceConnectorId`	Identifiant du connecteur vocal Amazon Chime pour lequel afficher les statistiques.
`Region`	Région AWS associée à l'événement.

CloudWatch journaux pour Amazon Chime

Vous pouvez envoyer les métriques d'Amazon Chime Voice Connector à CloudWatch Logs. Pour plus d'informations, consultez la section Modification des paramètres d'Amazon Chime Voice Connector dans le Guide d'administration du SDK Amazon Chime.

Journaux de métriques de qualité des médias

Vous pouvez choisir de recevoir des journaux métriques de qualité multimédia pour votre Amazon Chime Voice Connector. Lorsque vous le faites, Amazon Chime envoie des statistiques détaillées par minute pour tous vos appels Amazon Chime Voice Connector à un groupe de CloudWatch journaux créé pour vous. Le nom du groupe de journaux est `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. Les champs suivants sont inclus dans les journaux, au format JSON.

Champ	Description
voice_connector_id	L'identifiant Amazon Chime Voice Connector qui transporte l'appel.
event_timestamp	Heure à laquelle les métriques sont émises, en millisecondes depuis l'époque UNIX (minuit le 1er janvier 1970) en UTC.
call_id	Correspond à l'identifiant de transaction.
from_sip_user	Utilisateur initiateur de l'appel.
from_country	Pays initiateur de l'appel.

Champ	Description
to_sip_user	Utilisateur destinataire de l'appel.
to_country	Pays destinataire de l'appel.
endpoint_id	Identifiant opaque indiquant l'autre point de terminaison de l'appel. À utiliser avec CloudWatch Logs Insights. Pour plus d'informations, consultez la section Analyse des données des CloudWatch journaux à l'aide de Logs Insights dans le guide de l'utilisateur d'Amazon CloudWatch Logs.
aws_region	Région AWS pour l'appel.
cust2vc_rtp_packets	Nombre de paquets RTP envoyés par le client à l'infrastructure Amazon Chime Voice Connector.
cust2vc_rtp_bytes	Nombre d'octets envoyés par le client à l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTP.
cust2vc_rtcp_packets	Nombre de paquets RTCP envoyés par le client à l'infrastructure Amazon Chime Voice Connector.
cust2vc_rtcp_bytes	Nombre d'octets envoyés par le client à l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTCP.
cust2vc_packets_lost	Nombre de paquets perdus lors du transit entre le client et l'infrastructure Amazon Chime Voice Connector.
cust2vc_jitter	Instabilité moyenne des paquets envoyés par le client à l'infrastructure Amazon Chime Voice Connector.

Champ	Description
vc2cust_rtp_packets	Nombre de paquets RTP envoyés au client depuis l'infrastructure Amazon Chime Voice Connector.
vc2cust_rtp_bytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector au client sous forme de paquets RTP.
vc2cust_rtcp_packets	Nombre de paquets RTCP envoyés au client depuis l'infrastructure Amazon Chime Voice Connector.
vc2cust_rtcp_bytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector au client sous forme de paquets RTCP.
vc2cust_packets_lost	Nombre de paquets perdus lors du transit entre l'infrastructure Amazon Chime Voice Connector et le client.
vc2cust_jitter	Instabilité moyenne des paquets envoyés au client depuis l'infrastructure Amazon Chime Voice Connector.
rtt_btwn_vc_and_cust	Le temps aller-retour moyen entre le client et l'infrastructure Amazon Chime Voice Connector .
mos_btwn_vc_and_cust	Le score d'opinion moyen (MOS) estimé associé aux flux vocaux entre le client et l'infrastructure Amazon Chime Voice Connector .
rem2vc_rtp_packets	Nombre de paquets RTP envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector.

Champ	Description
rem2vc_rtp_bytes	Nombre d'octets envoyés de l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTP.
rem2vc_rtcp_packets	Nombre de paquets RTCP envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector.
rem2vc_rtcp_bytes	Nombre d'octets envoyés de l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector sous forme de paquets RTCP.
rem2vc_packets_lost	Nombre de paquets perdus lors du transit entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector.
rem2vc_jitter	Instabilité moyenne des paquets envoyés depuis l'extrémité distante vers l'infrastructure Amazon Chime Voice Connector.
vc2rem_rtp_packets	Nombre de paquets RTP envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante.
vc2rem_rtp_bytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante sous forme de paquets RTP.
vc2rem_rtcp_packets	Nombre de paquets RTCP envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante.
vc2rem_rtcp_bytes	Nombre d'octets envoyés de l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante sous forme de paquets RTCP.

Champ	Description
vc2rem_packets_lost	Nombre de paquets perdus lors du transit entre l'infrastructure Amazon Chime Voice Connector et l'extrémité distante.
vc2rem_jitter	Instabilité moyenne des paquets envoyés depuis l'infrastructure Amazon Chime Voice Connector vers l'extrémité distante.
rtt_btwn_vc_and_rem	Le temps moyen aller-retour entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector.
mos_btwn_vc_and_rem	Le score d'opinion moyen (MOS) estimé associé aux flux vocaux entre l'extrémité distante et l'infrastructure Amazon Chime Voice Connector.

Journaux de messages SIP

Vous pouvez choisir de recevoir les journaux de messages SIP pour votre Amazon Chime Voice Connector. Lorsque vous le faites, Amazon Chime capture les messages SIP entrants et sortants et les envoie à un groupe de CloudWatch journaux créé pour vous. Le nom du groupe de journaux est `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. Les champs suivants sont inclus dans les journaux, au format JSON.

Champ	Description
voice_connector_id	L'identifiant du connecteur vocal Amazon Chime.
aws_region	Région AWS associée à l'événement.
event_timestamp	Heure à laquelle le message est capturé, en millisecondes depuis l'époque UNIX (minuit le 1er janvier 1970) en UTC.

Champ	Description
call_id	L'identifiant d'appel Amazon Chime Voice Connector.
sip_message	Message SIP complet capturé.

Automatiser Amazon Chime avec EventBridge

Amazon vous EventBridge permet d'automatiser vosAWS services et de répondre automatiquement à des événements système tels que des problèmes de disponibilité d'application ou des modifications de ressource. Pour plus d'informations sur les événements de réunion, consultez la section Événements de réunion dans le Guide du développeur Amazon Chime.

Lorsqu'Amazon Chime génère des événements, il les envoie vers EventBridge pour une livraison optimale, ce qui signifie qu'Amazon Chime essaie d'envoyer tous les événements à EventBridge, mais dans de rares cas, un événement peut ne pas être livré. Pour plus d'informations, consultez la section Événements liés auxAWS services dans le Guide de EventBridge l'utilisateur Amazon.

> **Note**
>
> Si vous devez chiffrer des données, vous devez utiliser des clés gérées par Amazon S3. Nous ne prenons pas en charge le chiffrement côté serveur à l'aide des clés principales du client stockées dans le service de gestion desAWS clés.

Automatiser les connecteurs vocaux Amazon Chime avec EventBridge

Les actions pouvant être déclenchées automatiquement pour les connecteurs vocaux Amazon Chime sont les suivantes :

- Appel d'une fonction AWS Lambda
- Lancement d'une tâche Amazon Elastic Container Service
- Relais de l'événement à Amazon Kinesis Video Streams
- Activation d'une machine d'état AWS Step Functions
- Notification d'une rubrique Amazon SNS ou d'une file d'attente Amazon SQS

Voici quelques exemples d'utilisation EventBridge avec les connecteurs vocaux Amazon Chime :

- Activation d'une fonction Lambda pour télécharger le son d'un appel une fois celui-ci terminé.
- Lancer une tâche Amazon ECS pour activer la transcription en temps réel après le démarrage d'un appel.

Pour de plus amples informations, veuillez consulter le Guide de EventBridge l'utilisateur Amazon.

Événements de streaming Amazon Chime Voice Connector

Les connecteurs vocaux Amazon Chime prennent en charge l'envoi d'événements EventBridge lorsque les événements décrits dans cette section se produisent.

La diffusion en continu sur Amazon Chime Voice Connector démarre

Les connecteurs vocaux Amazon Chime envoient cet événement lorsque le streaming multimédia vers Kinesis Video Streams démarre.

Example Données d'événement

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "direction": "Outbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>;",
```

```
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>;\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

Fin de la diffusion en continu sur Amazon Chime Voice Connector

Les connecteurs vocaux Amazon Chime envoient cet événement lorsque le streaming multimédia vers Kinesis Video Streams se termine.

Example Données d'événement

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "streamingStatus": "ENDED",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
```

```
        "transactionId": "12345678-1234-1234",
        "callId": "1112-2222-4333",
        "direction": "Inbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "version": "0"
    }
}
```

Mises à jour en streaming d'Amazon Chime Voice Connector

Les connecteurs vocaux Amazon Chime envoient cet événement lorsque le streaming multimédia vers Kinesis Video Streams est mis à jour.

Example Données d'événement

Voici un exemple de données pour cet événement.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
```

```
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "updateHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "streamingStatus": "UPDATED",
        "transactionId": "12345678-1234-1234",
        "version": "0",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4"
    }
}
```

La diffusion en continu d'Amazon Chime Voice Connector échoue

Les connecteurs vocaux Amazon Chime envoient cet événement lorsque le streaming multimédia vers Kinesis Video Streams échoue.

Example Données d'événement

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
```

```
  "region": "us-east-1",
  "resources": [],
  "detail": {
       "streamingStatus":"FAILED",
       "voiceConnectorId":"abcdefghi",
       "transactionId":"12345678-1234-1234",
       "callId":"1112-2222-4333",
       "direction":"Inbound",
       "failTime":"yyyy-mm-ddThh:mm:ssZ",
       "failureReason": "Internal failure",
       "version":"0"
  }
}
```

Journalisation des appels d'API Amazon Chime avecAWS CloudTrail

Amazon Chime est intégré àAWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dans Amazon Chime. CloudTrail capture tous les appels d'API pour Amazon Chime en tant qu'événements, y compris les appels de la console Amazon Chime et les appels de code à des API Amazon Chime. Si vous créez un journal d'activité, vous pouvez activer la livraison continue des CloudTrail événements dans un compartiment Amazon S3, y compris les événements pour Amazon Chime. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Amazon Chime, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

Informations sur Amazon Chime dans CloudTrail

CloudTrail est activé dans votreAWS compte lors de la création de ce dernier. Lorsque des appels d'API sont effectués depuis la console d'administration Amazon Chime, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements deAWS services dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votreAWS compte, y compris les événements pour Amazon Chime, créez un journal de suivi. Un journal CloudTrail de suivi permet de livrer

des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions . Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en détail les données d'événement collectées dans les journaux CloudTrail et agir en conséquence. Pour plus d'informations, reportez-vous à :

- 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 actions Amazon Chime sont enregistrées CloudTrail et sont documentées dans la référence de l'API Amazon Chime. Par exemple, les appels aux`ResetPersonalPIN` sections`CreateAccount`,`InviteUsers` et génèrent des entrées dans les fichiers CloudTrail journaux. Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les autorisations 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 requête a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des entrées des fichiers journaux Amazon Chime

Un journal de suivi est une configuration qui permet la remise d'événements sous forme de fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace de pile ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

Les entrées pour Amazon Chime sont identifiées par la source de l'événement chime.amazonaws.com.

Si vous avez configuré Active Directory pour votre compte Amazon Chime, consultez la section Journalisation des appels d'API AWS Directory Service à l'aide de CloudTrail. Ceci explique comment surveiller les problèmes susceptibles d'affecter la capacité de connexion de vos utilisateurs Amazon Chime.

L'exemple suivant montre une entrée de CloudTrail journal pour Amazon Chime :


```
{"eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":" AAAAAABBBBBBBBEXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice ",
            "accountId":"0123456789012",
            "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
            "sessionContext":{
               "attributes":{
                  "mfaAuthenticated":"false",
                  "creationDate":"2017-07-24T17:57:43Z"
               },
               "sessionIssuer":{
                  "type":"Role",
                  "principalId":"AAAAAABBBBBBBBEXAMPLE",
                  "arn":"arn:aws:iam::123456789012:role/Joe",
                  "accountId":"123456789012",
                  "userName":"Joe"
               }
            }
         } ,
         "eventTime":"2017-07-24T17:58:21Z",
         "eventSource":"chime.amazonaws.com",
         "eventName":"AddDomain",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"72.21.198.64",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
         "errorCode":"ConflictException",
         "errorMessage":"Request could not be completed due to a conflict",
         "requestParameters":{
            "domainName":"example.com",
            "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
```

```
        },
        "responseElements":null,
        "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
        "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
    }
```


Validation de conformité pour Amazon Chime

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services dans le cadre de plusieurs programmes de AWS conformité, tels que SOC, PCI, FedRAMP et HIPAA.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

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

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit 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 AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.

- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config 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— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Amazon Chime

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, Amazon Chime propose différentes fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour plus d'informations, consultez les sections Gestion des groupes Amazon Chime Voice Connector et Diffusion du contenu multimédia Amazon Chime Voice Connector vers Kinesis dans le guide d'administration du SDK Amazon Chime.

Sécurité de l'infrastructure dans Amazon Chime

En tant que service géré, Amazon Chime est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

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

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Comprendre les mises à jour automatiques d'Amazon Chime

Amazon Chime propose différentes méthodes pour mettre à jour ses clients. La méthode varie selon que vos utilisateurs exécutent Amazon Chime dans un navigateur, sur votre ordinateur de bureau ou sur un appareil mobile.

L'application Web Amazon Chime (https://app.chime.aws) intègre toujours les dernières fonctionnalités et correctifs de sécurité.

Le client de bureau Amazon Chime vérifie les mises à jour chaque fois qu'un utilisateur choisit de quitter ou de se déconnecter. Cela s'applique aux machines Windows et macOS. Lorsque les

utilisateurs exécutent le client, celui-ci vérifie les mises à jour toutes les trois heures. Les utilisateurs peuvent également vérifier les mises à jour en choisissant Vérifier les mises à jour dans le menu Aide de Windows ou dans le menu Amazon Chime de macOS.

Lorsque le client de bureau détecte une mise à jour, Amazon Chime invite les utilisateurs à l'installer, sauf s'ils participent à une réunion en cours. Les utilisateurs sont en réunion permanente lorsque :

- Ils assistent à une réunion.
- Ils ont été invités à une réunion qui est toujours en cours.

Amazon Chime les invite à installer la dernière version et leur donne un compte à rebours de 15 secondes pour qu'ils puissent reporter l'installation. Choisissez Essayer plus tard pour reporter la mise à jour.

Lorsque les utilisateurs reportent une mise à jour alors qu'ils ne participent pas à une réunion en cours, le client vérifie l'existence de la mise à jour au bout de trois heures et les invite à nouveau à l'installer. L'installation commence à la fin du compte à rebours.

> **Note**
>
> Sur un ordinateur macOS, les utilisateurs doivent choisir Redémarrer maintenant pour commencer la mise à jour.

Sur un appareil mobile : les applications mobiles Amazon Chime utilisent les options de mise à jour proposées par l'App Store et Google Play pour fournir la dernière version du client Amazon Chime. Vous pouvez également distribuer des mises à jour par le biais de votre système de gestion des appareils mobiles. Cette rubrique part du principe que vous savez comment procéder.

Historique du document pour Amazon Chime

Le tableau suivant décrit les modifications importantes apportées au guide de l'administrateur Amazon Chime à compter du mois de mars 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Publication du guide d'administration du SDK Amazon Chime	Les rubriques du SDK Amazon Chime sont désormais publiées dans le Guide d'administration du SDK Amazon Chime. Pour plus d'informations, consultez le Guide d'administration du SDK Amazon Chime.	24 mars 2022
Mises à jour de la politique IAM	Les modifications apportées aux politiques IAM gérées par AWS sont désormais suivies dans ce guide de l'administrateur. Consultez les exemples de politiques basées sur l'identité Amazon Chime.	23 septembre 2021
Rôles liés à un service	Les administrateurs peuvent désormais créer des rôles liés à un service pour Amazon Live Transcription et consulter les messages d'événements au début et à la fin d'une opération de transcription en direct Amazon Chime. Pour plus d'informations, consultez les sections Utilisation des rôles pour la transcription en direct et Automatisation	12 août 2021

	d'Amazon Chime CloudWatch avec les événements.	
Applications et règles multimédia SIP	Les administrateurs peuvent créer des applications multimédia SIP et des règles à utiliser avec le connecteu r vocal et AWS Lambda les fonctions Amazon Chime. Pour plus d'informations, consultez la section Gestion des applications et des règles SIP dans le manuel Amazon Chime Administrator Guide.	18 novembre 2020
Numéros de routage des appels d'urgence Amazon Chime Voice Connector	Les administrateurs Amazon Chime peuvent configure r des numéros de routage des appels d'urgence pour un Amazon Chime Voice Connector. Pour plus d'informa tions, consultez la section Configuration des numéros de routage des appels d'urgence pour votre Amazon Chime Voice Connector, dans le guide de l'administrateur Amazon Chime.	1er juillet 2020

Amazon Chime sur Dolby Voice Huddle	Amazon Chime propose une expérience de réunion native ou de première partie sur le matériel de conférence audio et vidéo Dolby Voice Huddle. Pour plus d'informations, consultez Configuration d'Amazon Chime sur du matériel Dolby, dans le guide de l'administrateur Amazon Chime.	3 juin 2020
Configuration des politiques de rétention des discussions	Les administrateurs Amazon Chime peuvent définir des politiques de rétention des discussions pour leurs comptes d'entreprise. Pour plus d'informations, consultez la section Gestion des politiques de rétention des discussions dans le manuel Amazon Chime Administrator Guide.	21 mai 2020
Supprimer les messages de chat	Si vous pouvez programmer, vous pouvez utiliser deux API Amazon Chime pour supprimer les messages des forums de discussion et des conversations de votre compte. Pour plus d'informations, consultez la section Suppression de messages individuels dans le manuel Amazon Chime Administrator Guide.	18 mai 2020

CloudWatch statistiques de qualité multimédia pour Amazon Chime Voice Connector	Amazon Chime prend en charge l'envoi d'indicateurs de qualité multimédia pour votre Amazon Chime Voice Connector à. CloudWatch Pour plus d'informations, consultez la section Surveillance d'Amazon Chime avec CloudWatch, dans le manuel Amazon Chime Administrator Guide.	23 janvier 2020
Application Amazon Chime Meetings pour Slack	Amazon Chime prend en charge l'application Amazon Chime Meetings pour Slack. Pour plus d'informations, consultez la section Configuration de l'application Amazon Chime Meetings pour Slack dans le guide de l'administrateur Amazon Chime.	4 décembre 2019
Paramètres de la région de réunion	Amazon Chime prend en charge le traitement des réunions dans la AWS région optimale pour tous les participants. Pour plus d'informations, consultez la section Paramètres des régions de réunion dans le manuel Amazon Chime Administrator Guide.	3 décembre 2019

Compatibilité avec l'enregistrement multimédia basé sur le protocole SIP (SIPREC)	Les connecteurs vocaux Amazon Chime permettent de diffuser du contenu multimédia depuis une infrastructure vocale compatible SIPREC vers Kinesis Video Streams. Pour plus d'informations, consultez la section Compatibilité de l'enregistrement multimédia basé sur le protocole SIP (SIPREC) dans le manuel Amazon Chime Administrator Guide.	25 novembre 2019
Amazon Chime sur Dolby Voice Room	Si vous souhaitez que les utilisateurs puissent participer facilement à des réunions, Amazon Chime propose une expérience de réunion native ou directe sur le matériel de conférence audio et vidéo Dolby Voice Room. Pour plus d'informations, consultez Configuration d'Amazon Chime sur Dolby Voice Room, dans le guide de l'administrateur Amazon Chime.	29 octobre 2019

Mise à jour des noms d'appels sortants	Définissez un nom d'appel par défaut qui apparaît aux destinataires des appels sortants passés à l'aide des numéros de téléphone de votre inventaire Amazon Chime. Pour plus d'informations, consultez la section Mise à jour des noms d'appels sortants dans le manuel Amazon Chime Administrator Guide.	24 octobre 2019
Diffusion de contenu multimédia sur Amazon Kinesis	Diffusez le son des appels téléphoniques depuis Amazon Chime Voice Connectors vers Kinesis Video Streams à des fins d'analyse, d'apprentissage automatique et d'autres traitements. Pour plus d'informations, consultez les sections Diffusion de contenu multimédia Amazon Chime Voice Connector vers Kinesis et Utilisation du rôle lié au service Amazon Chime Voice Connector dans le guide de l'administrateur Amazon Chime.	24 octobre 2019

Surveillance d'Amazon Chime avec Amazon CloudWatch	Surveillez Amazon Chime à l'aide d'Amazon Chime CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Pour plus d'informations, consultez la section Surveillance d'Amazon Chime avec CloudWatch, dans le manuel Amazon Chime Administrator Guide.	24 octobre 2019
Groupes de connecteurs vocaux Amazon Chime	Créez un groupe Amazon Chime Voice Connector qui inclut les connecteurs vocaux Amazon Chime créés dans différentes régions. AWS Cela permet aux appels entrants de basculer entre les régions, ce qui crée un mécanisme tolérant aux pannes pour le repli en cas d'événements de disponibilité. Pour plus d'informations, consultez la section Utilisation des groupes Amazon Chime Voice Connector dans le manuel Amazon Chime Administrator Guide.	24 octobre 2019

Mises à jour de configuration réseau	Amazon Chime simplifie ses exigences en matière de pare-feu. Pour plus d'informations, consultez la section Configuration du réseau et exigences en bande passante dans le manuel Amazon Chime Administrator Guide.	6 septembre 2019
Réunions modérées	Amazon Chime prend en charge les réunions modérées. Pour plus d'informations, consultez la section Rejoindre une réunion modérée dans le manuel Amazon Chime Administrator Guide.	25 juillet 2019
Validation de conformité pour Amazon Chime	Amazon Chime est un service éligible à la loi HIPAA. Pour plus d'informations, consultez la section Validation de conformité pour Amazon Chime dans le manuel Amazon Chime Administrator Guide.	11 juin 2019
Portage de numéros de téléphone gratuits	Amazon Chime prend en charge le portage de numéros de téléphone gratuits aux États-Unis pour les utiliser avec les connecteurs vocaux Amazon Chime. Pour plus d'informations, consultez la section Portage de numéros de téléphone existants dans le manuel Amazon Chime Administrator Guide.	28 mai 2019

Gestion des numéros de téléphone dans Amazon Chime	Utilisez Amazon Chime Business Calling pour fournir et attribuer des numéros de téléphone aux utilisateurs d'Amazon Chime. Intégrez un connecteur vocal Amazon Chime à un système téléphonique existant. Pour plus d'informations, consultez la section Gestion des numéros de téléphone dans Amazon Chime dans le manuel Amazon Chime Administrator Guide.	18 mars 2019
Complément Amazon Chime pour Outlook	Amazon Chime fournit deux compléments pour Microsoft Outlook : le complément Amazon Chime pour Outlook sous Windows et le complément Amazon Chime pour Outlook. Ces modules complémentaires offrent les mêmes fonctionnalités de planification, mais prennent en charge différents types d'utilisateurs. Pour plus d'informations, consultez la section Déploiement du complément pour Outlook dans le manuel Amazon Chime Administrator Guide.	12 mars 2019
Diverses mises à jour	Diverses mises à jour apportées à la mise en page et l'organisation des rubriques.	11 février 2019

Fonction « Appelez-moi » d'Amazon Chime	Les administrateurs peuvent activer la fonction « Call me » d'Amazon Chime dans leurs paramètres de réunions. Pour plus d'informations, consultez la section Gestion des paramètres de réunion dans le manuel Amazon Chime Administrator Guide.	22 août 2018
Connectez-vous à Okta SSO	Si vous disposez d'un compte d'entreprise, vous pouvez vous connecter à Okta SSO pour vous authentifier et attribuer des autorisations utilisate ur. Pour plus d'informations, consultez Connect to Okta SSO dans le manuel Amazon Chime Administrator Guide.	1er août 2018
Demander des pièces jointes aux utilisateurs	Recevez les pièces jointes téléchargées sur Amazon Chime par les utilisateurs. Pour plus d'informations, consultez la section Demander des pièces jointes aux utilisate urs dans le manuel Amazon Chime Administrator Guide.	23 avril 2018
Afficher des données de rapport supplémentaires	Afficher des données de rapport supplémentaires. Pour plus d'informations, consultez la section Afficher les rapports dans le manuel Amazon Chime Administrator Guide.	30 mars 2018

Attribuer aux utilisateurs des autorisations Pro ou Basic	Affecter aux utilisateurs des autorisations de base ou Pro. Pour plus d'informations, consultez Gérer l'accès et les autorisations des utilisateurs dans le manuel Amazon Chime Administrator Guide.	29 mars 2018