Administratorhandbuch

Amazon Chime

Amazon Chime: Administratorhandbuch

Table of Contents

Sie müssen ein Amazon Chime Chime-Systemadministrator sein, um die Schritte in diesem Handbuch ausführen zu können. Wenn Sie Hilfe mit dem Amazon Chime Chime-Desktop-Client, der Web-App oder der mobilen App benötigen, finden Sie weitere Informationen unter Support erhalten im Amazon Chime Chime-Benutzerhandbuch.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Was ist Amazon Chime?

Amazon Chime ist ein Kommunikationsservice, der Online-Besprechungen mit einer sicheren und umfassenden Anwendung transformiert. Amazon Chime funktioniert geräteübergreifend, sodass Sie in Verbindung bleiben können. Sie können Amazon Chime für Online-Besprechungen, Videokonferenzen, Anrufe und Chats verwenden. Sie können Inhalte auch innerhalb und außerhalb Ihrer Organisation teilen. Amazon Chime ist ein vollständig verwalteter Service, der sicher in derAWS Cloud ausgeführt wird, sodass die IT-Abteilung keine komplexen Infrastrukturen bereitstellen und verwalten muss.

Weitere Informationen finden Sie unter Amazon Chime.

Administrationsübersicht

Als Administrator verwenden Sie die Amazon Chime Chime-Konsole, um wichtige Aufgaben auszuführen, z. B. das Erstellen von Amazon Chime Chime-Konten und die Verwaltung von Benutzern und Berechtigungen. Um auf die Amazon Chime Chime-Konsole zuzugreifen und ein Amazon Chime-Administratorkonto zu erstellen, erstellen Sie zunächst einAWS Konto. Weitere Informationen finden Sie unter Voraussetzungen für Amazon Chime Chime-Systemadministratoren.

Erste Schritte

Nachdem Sie das abgeschlossen habenVoraussetzungen für Amazon Chime Chime-Systemadministratoren, können Sie Ihr Amazon Chime-Administratorkonto erstellen und konfigurieren und dann Benutzer hinzufügen. Wählen Sie Pro- oder Basic-Berechtigungen für Ihre Benutzer.

Wenn Sie bereit für den Einstieg sind, sehen Sie sich folgendes Tutorial an:

- Erste Schritte

Weitere Informationen zum Benutzerzugriff und zu Benutzerberechtigungen finden Sie unter Verwaltung der Benutzerberechtigungen und des Zugriffs. Weitere Informationen zu den Funktionen, auf die Benutzer mit Pro- und Basic-Berechtigungen zugreifen können, finden Sie unter Preise.

Preise

Amazon Chime bietet nutzungsabhängige Preise. Sie zahlen nur für Benutzer mit Pro-Berechtigungen, die Meetings hosten, und nur an den Tagen, an denen diese Meetings gehostet werden. Meetings-Teilnehmern und Chat-Benutzern entstehen keine Kosten.

Es fallen keine Gebühren für Benutzer mit Basic-Berechtigungen an. Basic-Benutzer können keine Meetings abhalten. Sie können jedoch an Meetings teilnehmen und die Chat-Funktion verwenden. Weitere Informationen zu Preisen und Funktionen, auf die Benutzer mit Pro- und Basic-Berechtigungen zugreifen können, finden Sie unter Preise.

Ressourcen

Weitere Informationen zum Amazon Chime finden Sie in den folgenden Ressourcen:

- Amazon Chime Hilfecenter
- Amazon Chime Chime-Schulungsvideos

Voraussetzungen für Amazon Chime Chime-Systemadministratoren

Sie benötigen ein AWS Konto, um auf die Amazon Chime Chime-Konsole zugreifen und ein Amazon Chime Chime-Administratorkonto erstellen zu können.

Ein Amazon Web Services Services-Konto erstellen

Bevor Sie ein Administratorkonto für Amazon Chime erstellen können, müssen Sie zunächst ein AWS Konto erstellen. chime

Themen

- Melden Sie sich an für ein AWS-Konto
- Erstellen Sie einen Benutzer mit Administratorzugriff

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Weitere Informationen zur Einrichtung Ihres Amazon Chime-Administratorkontos finden Sie unterErste Schritte.

Erste Schritte

Der einfachste Weg für Ihre Benutzer, mit Amazon Chime zu beginnen, besteht darin, die Amazon Chime Pro-Version herunterzuladen und 30 Tage lang kostenlos zu verwenden. Weitere Informationen finden Sie unter Herunterladen von Amazon Chime.

Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon Amazon

Um die Amazon Chime Pro-Version nach Ablauf der 30-tägigen kostenlosen Testphase weiterhin verwenden zu können, müssen Sie ein Amazon Chime Chime-Administratorkonto erstellen und Ihre Benutzer zu diesem Konto hinzufügen. Zum Einstieg müssen Sie zuerst die Voraussetzungen für Amazon Chime Chime-Systemadministratoren erfüllen, zu denen die Erstellung eines AWS-Kontos gehört. Anschließend können Sie ein Amazon Chime Chime-Administratorkonto erstellen und konfigurieren und Benutzer hinzufügen, indem Sie die folgenden Aufgaben ausführen.

Aufgaben

- Schritt 1: Erstellen eines Amazon Chime Chime-Administratorkontos
- Schritt 2 (optional): Konfigurieren von Kontoeinstellungen
- Schritt 3: Hinzufügen von Benutzern zu Ihrem Konto
- (Optional) Amazon Chime Chime-Chime-Chime-Chime-Chime-Konto einrichten

Schritt 1: Erstellen eines Amazon Chime Chime-Administratorkontos

Nach dem Erstellen derVoraussetzungen für Amazon Chime Chime-Systemadministratoren Schritte können Sie nun ein Amazon Chime Chime-Administratorkonto erstellen.

So erstellen Sie ein Amazon Chime Chime-Administratorkonto

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Klicken Sie auf der Seite Accounts (Konten) auf New account (Neues Konto).
3. Geben Sie unter Account Name (Kontoname) einen Namen für das Konto ein und wählen Sie Create account (Konto erstellen).
4. (Optional) Wählen Sie aus, ob Amazon Chime die optimaleAWS Region für Ihre Besprechungen aus allen verfügbaren Regionen auswählen lassen oder ob Sie nur die von Ihnen ausgewählten

Regionen verwenden möchten. Weitere Informationen finden Sie unter Verwalten von Meeting-Einstellungen.

Schritt 2 (optional): Konfigurieren von Kontoeinstellungen

Standardmäßig werden neue Konten als Teamkonten erstellt. Wenn Sie es vorziehen, eine Domain zu beanspruchen und sich mit Ihrem eigenen Identitätsanbieter oder Okta SSO zu verbinden, können Sie auf ein Enterprise-Konto umsteigen. Weitere Informationen zu Team- und Enterprise-Konten finden Sie unter Wählen Sie zwischen einem Amazon Chime Team-Konto oder einem Enterprise-Konto.

So konvertieren Sie ein Team-Konto in ein Enterprise-Konto

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie in Accounts (Konten) den Namen des Kontos aus.
3. Wählen Sie in Identity (Identität) Getting Started (Erste Schritte) aus.
4. Führen Sie die in der Konsole angezeigten Schritte aus, um Ihre Domäne zu beanspruchen.
5. (Optional) Führen Sie die in der Konsole angezeigten Schritte aus, um den Identitätsanbieter einzurichten und die Verzeichnisgruppe zu konfigurieren.

Weitere Informationen zum Beantragen von Domänen finden Sie unter Beantragen einer Domäne. Weitere Informationen zum Einrichten von Identitätsanbietern finden Sie unter Herstellen einer Verbindung mit Active Directory und Herstellen einer Verbindung mit Okta-SSO.

Sie können auch Kontorichtlinien für Optionen wie die Fernsteuerung geteilter Bildschirme und die Amazon Chime Chime-Funktion „Ruf mich an“ zulassen oder deaktivieren.

So konfigurieren Sie Kontorichtlinien

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Accounts (Konten) den Namen des Kontos, das Sie konfigurieren möchten.
3. Wählen Sie in Settings (Einstellungen) die Option Meetings aus.
4. Aktivieren oder deaktivieren Sie in Policies (Richtlinien) die Kontenrichtlinienoptionen, die Sie zulassen oder deren Zulassung Sie deaktivieren möchten.
5. Wählen Sie Change.

Weitere Informationen finden Sie unter Verwalten von Meeting-Einstellungen.

Schritt 3: Hinzufügen von Benutzern zu Ihrem Konto

Nachdem Ihr Amazon Chime Team-Konto erstellt wurde, laden Sie sich und Ihre Benutzer ein, diesem Konto beizutreten. Wenn Sie Ihr Konto auf ein Enterprise-Konto upgraden, müssen Sie Ihre Benutzer nicht einladen. Nehmen Sie stattdessen ein Upgrade auf ein Enterprise-Konto vor und beantragen Sie Ihre Domäne. Weitere Informationen finden Sie unter Schritt 2 (optional): Konfigurieren von Kontoeinstellungen.

So fügen Sie Ihrem Amazon Chime Chime-Konto Benutzer hinzu

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Accounts (Konten) den Namen Ihres Kontos aus.
3. Klicken Sie auf der Seite Users (Benutzer) auf Invite users (Benutzer einladen).
4. Geben Sie die E-Mail-Adressen der Benutzer ein, die Sie einladen möchten, einschließlich Ihrer eigenen, und wählen Sie Invite users (Benutzer einladen).

Die eingeladenen Benutzer erhalten E-Mail-Einladungen, dem von Ihnen erstellten Amazon Chime Team-Konto beizutreten. Wenn sie ihre Amazon Chime Chime-Benutzerkonten registrieren, erhalten sie standardmäßig Pro-Berechtigungen, und ihre 30-Tage-Testversion endet. Wenn sie sich bereits mit ihrer geschäftlichen E-Mail-Adresse für ein Amazon Chime Chime-Benutzerkonto angemeldet haben, können sie dieses Konto weiterhin verwenden. Sie können auch die Amazon Chime-Client-App jederzeit herunterladen, indem sie Amazon Chime herunterladen wählen und sich mit ihrem Benutzerkonto anmelden.

Ihnen wird ein Benutzer nur dann berechnet, wenn er ein Meeting abhält. Es fallen keine Gebühren für Benutzer mit Basic-Berechtigungen an. Basic-Benutzer können keine Meetings abhalten. Sie können jedoch an Meetings teilnehmen und die Chat-Funktion verwenden. Weitere Informationen zur Preisgestaltung und zu den Funktionen, auf die Benutzer mit Pro- und Basic-Berechtigungen zugreifen können, finden Sie unter Abos und Preise.

So ändern Sie Benutzerberechtigungen

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Accounts (Konten) den Namen Ihres Kontos aus.

3. Wählen Sie auf der Seite Users (Benutzer) den oder die Benutzer aus, für den/die Sie Berechtigungen ändern möchten.
4. Wählen Sie User actions (Benutzeraktionen), Assign user permission (Benutzerberechtigung zuweisen).
5. Wählen Sie für Permissions (Berechtigungen) die Option Pro oder Basic.
6. Wählen Sie Assign (Zuweisen).

Sie können anderen Benutzern Administratorberechtigungen gewähren und auch deren Zugriff auf die Amazon Chime Chime-Konsole für Ihr Konto kontrollieren. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon Chime.

(Optional) Amazon Chime Chime-Chime-Chime-Chime-Chime-Konto einrichten

Die folgenden Telefonoptionen sind für Amazon Chime-Administratorkonten verfügbar:

Amazon Amazon Amazon Amazon Amazon Amazon Chime Amazon Chime

Ermöglicht es Ihren Benutzern, Telefonanrufe und Textnachrichten direkt von Amazon Chime aus zu senden und zu empfangen. Geben Sie Ihre Telefonnummern in der Amazon Chime Chime-Konsole an oder übertragen Sie bestehende Telefonnummern. Weisen Sie die Telefonnummern Ihren Amazon Chime-Benutzern zu und gewähren Sie ihnen die Berechtigung, Telefonanrufe und Textnachrichten mit Amazon Chime zu senden und zu empfangen. Weitere Informationen erhalten Sie unter Verwaltung von Telefonnummern in Amazon Chime und Portieren von Telefonnummern.

Amazon Chime Chime-Amazon

Stellt einen SIP-Trunking-Dienst für ein vorhandenes Telefonsystem bereit. Portieren Sie bestehende Telefonnummern oder stellen Sie neue Telefonnummern in der Amazon Chime Chime-Konsole bereit. Weitere Informationen finden Sie unter Verwaltung von Amazon Chime Voice Connectors im Amazon Chime SDK-Administrationshandbuch.

Verwaltung Ihrer Amazon Chime Chime-Konten

Sie können Amazon Chime als Einzelbenutzer oder als Gruppe ohne Administratoren verwenden. Wenn Sie jedoch Administratorfunktionen hinzufügen oder Amazon Chime Pro erwerben möchten, müssen Sie ein Amazon Chime Chime-Konto in der erstellen. AWS Management Console Informationen zum Erstellen eines Amazon Chime-Administratorkontos oder weitere Informationen zum Kauf von Amazon Chime Pro finden Sie unter. Erste Schritte

Weitere Informationen zu den verschiedenen Typen von Amazon Chime Chime-Administratorkonten finden Sie unterWählen Sie zwischen einem Amazon Chime Team-Konto oder einem Enterprise-Konto. Weitere Informationen zur Verwaltung eines vorhandenen Administratorkontos finden Sie in den folgenden Themen.

Themen

Wählen Sie zwischen einem Amazon Chime Team-Konto oder einem Enterprise-Konto

Wenn Sie ein Amazon Chime Chime-Administratorkonto erstellen, wählen Sie, ob Sie ein Team-Konto oder ein Enterprise-Konto erstellen möchten. Weitere Informationen zum Erstellen eines Amazon Chime Chime-Administratorkontos finden Sie unterErste Schritte.

Team-Konto

Mit einem Team-Konto können Sie Benutzer einladen und ihnen Amazon Chime Pro-Berechtigungen gewähren, ohne Anspruch auf eine E-Mail-Domain erheben zu müssen. Weitere Informationen zu den Pro- und Basic-Berechtigungen finden Sie unter Pläne und Preise.

Sie können Benutzer von jeder E-Mail-Domain einladen, die nicht von einer anderen Organisation beansprucht wurde. Benutzer werden Ihnen nur berechnet, wenn sie Meetings abhalten. Benutzer in Ihrem Team-Konto können die Amazon Chime Chime-App verwenden, um nach anderen Amazon Chime Chime-Benutzern zu suchen und diese zu kontaktieren, die für dasselbe Konto registriert sind. Wir empfehlen außerdem ein Team-Konto für die Bezahlung von Pro-Benutzern außerhalb Ihrer Organisation.

Unternehmenskonto

Mit einem Enterprise-Konto haben Sie mehr Kontrolle über die Benutzer aus den Domänen Ihrer Organisation. Sie können wählen, ob Sie sich mit Ihrem eigenen Identitätsanbieter oder mit Okta SSO verbinden möchten, um sich zu authentifizieren und Pro- oder Basic-Berechtigungen zuzuweisen. Amazon Chime unterstützt auch Microsoft Active Directory.

Um ein Enterprise-Konto zu erstellen, müssen Sie mindestens eine E-Mail-Domain beanspruchen. Dadurch wird sichergestellt, dass alle Benutzer, die sich mit Ihren beanspruchten Domains bei Amazon Chime anmelden, in Ihrem zentral verwalteten Amazon Chime Chime-Konto enthalten sind. Für die Verwaltung Ihrer Benutzer über eine unterstützte Verzeichnisintegration sind Unternehmenskonten erforderlich. Weitere Informationen finden Sie unter Beantragen einer Domäne und Herstellen einer Verbindung mit Active Directory.

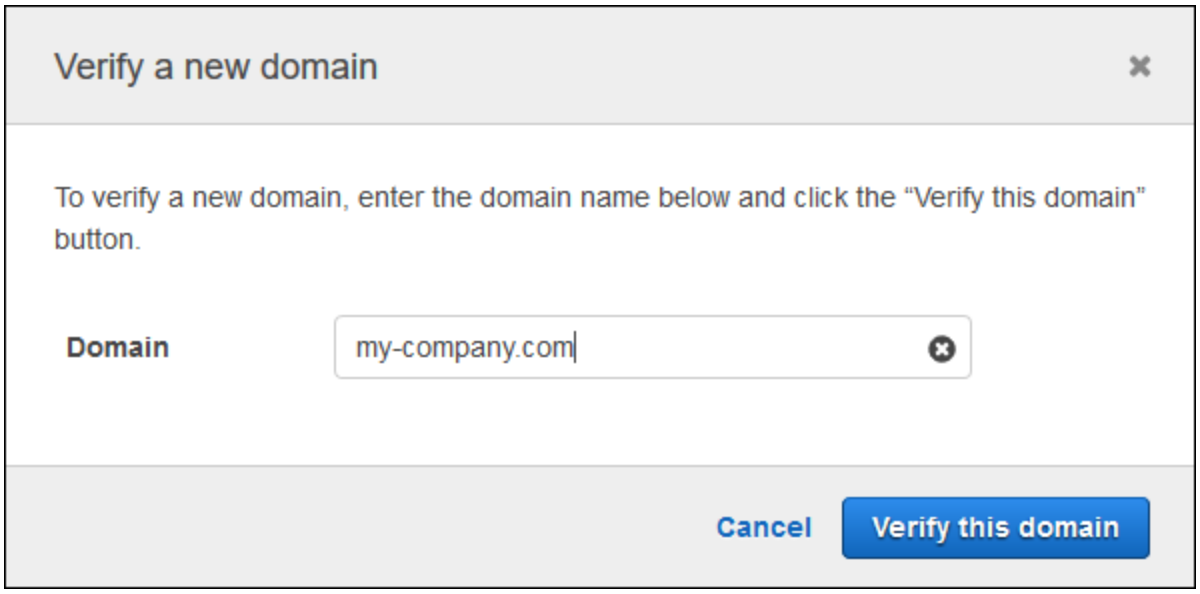
Sie können die Benutzeraktivierung und Sperrung auch von Ihrem Enterprise-Konto aus verwalten. Weitere Informationen finden Sie unter Verwaltung der Benutzerberechtigungen und des Zugriffs.

Beantragen einer Domäne

Um ein Enterprise-Konto zu erstellen und von der größeren Kontrolle zu profitieren, die damit über Ihr Konto und Benutzer verliehen wird, müssen Sie mindestens einen E-Mail-Domäne beantragen.

So beantragen Sie eine Domäne

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Konten den Namen des Teamkontos aus.
3. Klicken Sie im Navigationsbereich auf Identity, Domains.
4. Wählen Sie auf der Seite Domains (Domänen) Claim a new domain (Neue Domäne beantragen).
5. Geben Sie für Domain (Domäne) die Domäne ein, die Ihre Organisation für E-Mail-Adressen verwendet. Wählen Sie Verify this domain (Diese Domäne überprüfen).



6. Befolgen Sie die Anweisungen auf dem Bildschirm, um zum DNS-Server einen TXT-Datensatz für Ihre Domäne hinzuzufügen. Im Allgemeinen umfasst der Vorgang die Anmeldung beim Konto Ihrer Domain, das Suchen der DNS-Einträge für Ihre Domain und das Hinzufügen eines TXT-Eintrags mit dem von Amazon Chime bereitgestellten Namen und Wert. Weitere Informationen zum Aktualisieren der DNS-Datensätze für Ihre Domäne finden Sie in der Dokumentation für Ihren DNS-Anbieter oder Ihre Domänennamen-Vergabestelle.

   Amazon Chime prüft, ob dieser Datensatz vorhanden ist, um sicherzustellen, dass Sie Eigentümer der Domain sind. Nachdem die Domäne überprüft wurde, ändert sich ihr Status von Pending verification (Ausstehende Verifizierung) in Verified (Verifiziert).

> **Note**
>
> Die Weitergabe der DNS-Änderung und Überprüfung durch Amazon Chime kann bis zu 24 Stunden dauern.

7. Wenn Ihre Organisation zusätzliche Domänen oder Subdomänen für E-Mail-Adressen verwendet, wiederholen Sie dieses Verfahren für jede Domain.

Weitere Informationen zur Fehlerbehebung im Zusammenhang mit der Beanspruchung von Domänen finden Sie unter Why isn't my domain claim request getting verified?

Umwandlung eines Teamkontos in ein Enterprise-Konto

Um ein bestehendes Team-Konto in ein Enterprise-Konto umzuwandeln, beanspruchen Sie eine oder mehrere E-Mail-Domains in der Amazon Chime Chime-Konsole. Weitere Informationen zu den Unterschieden zwischen Team- und Enterprise-Konten finden Sie unterWählen Sie zwischen einem Amazon Chime Team-Konto oder einem Enterprise-Konto. Weitere Informationen zur Inanspruchnahme einer Domain finden Sie unterBeantragen einer Domäne.

So konvertieren Sie ein Team-Konto in ein Enterprise-Konto

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie in Accounts (Konten) den Namen des Kontos aus.
3. Wählen Sie in Identity (Identität) Getting Started (Erste Schritte) aus.
4. Führen Sie die in der Konsole angezeigten Schritte aus, um Ihre Domäne zu beanspruchen.
5. (Optional) Führen Sie die in der Konsole angezeigten Schritte aus, um den Identitätsanbieter einzurichten und die Verzeichnisgruppe zu konfigurieren.

Nachdem Ihr Konto in ein Enterprise-Konto umgewandelt wurde, können Sie entscheiden, ob Sie eine Verbindung zu einer Active Directory-Instance herstellen möchten. AWS Directory Service Durch die Verbindung mit einer Active Directory-Instance können sich Ihre Benutzer mit ihren Active Directory-Anmeldeinformationen bei Amazon Chime anmelden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Active Directory.

Wenn Sie keine Verbindung zu einer Active Directory-Instance herstellen, können sich Ihre Benutzer weiterhin mit Login with Amazon (LWA) oder ihren Amazon.com-Kontoanmeldedaten bei Amazon Chime anmelden.

Umbenennen Ihres Kontos

In den folgenden Schritten wird erklärt, wie Sie die Amazon Chime Chime-Team- und Unternehmenskonten, die Sie verwalten, umbenennen. Der von Ihnen gewählte Name erscheint in den E-Mails, in denen Benutzer eingeladen werden, Amazon Chime beizutreten.

So benennen Sie Ihr Konto um

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.

   Die Seite Konten wird standardmäßig angezeigt.
2. Wählen Sie in der Spalte Kontoname das Konto aus, das Sie umbenennen möchten.
3. Wählen Sie im linken Bereich unter Einstellungen die Option Konto aus.

   Die Seite mit der Kontoübersicht wird angezeigt.
4. Öffnen Sie die Liste mit den Kontoaktionen und wählen Sie Konto umbenennen.

   Das Dialogfeld „Konto umbenennen“ wird angezeigt.
5. Geben Sie den neuen Kontonamen ein und wählen Sie Speichern.

Löschen Ihres Kontos

Wenn Sie Ihr AWS Konto in der löschen AWS Management Console, werden Ihre Amazon Chime Chime-Konten automatisch gelöscht. Alternativ können Sie die Amazon Chime-Konsole verwenden, um ein Amazon Chime Team- oder Enterprise-Konto zu löschen.

> **Note**
>
> Benutzer, die nicht mit einem Team- oder Enterprise-Konto verwaltet werden, können mithilfe des Amazon Chime Assistant-Befehls „Delete me“ eine Löschung beantragen. Weitere Informationen finden Sie unter Amazon Chime Assistant verwenden.

So löschen Sie ein Teamkonto

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie das Konto in der Spalte Account name (Kontoname) und Account (Konto) under Settings (Einstellungen) aus.
3. Im Navigationsbereich wird die Seite Users (Benutzer) angezeigt.
4. Wählen Sie die Benutzer und dann User actions (Benutzeraktionen), Remove user (Benutzer entfernen) aus.
5. Wählen Sie im Navigationsbereich Accounts (Konten), Account actions (Kontoaktionen) und Delete account (Konto löschen).
6. Bestätigen Sie, dass Sie das Konto löschen möchten.

Amazon Chime löscht alle Benutzerdaten, wenn Sie Ihr Konto löschen. Dazu gehört die Kündigung eines AWS Kontos, einzelner Amazon Chime Chime-Konten oder nicht verwalteter Amazon Chime Chime-Benutzer. Davon ausgenommen sind Daten ohne Inhalt, die sich auf Benutzerkonten und die Nutzung von Amazon Chime beziehen (Serviceattribute, die unter die Kundenvereinbarung fallen), die von Amazon Chime generiert werden.

So löschen Sie ein Enterprise-Konto

1. Entfernen Sie die Domänen.

> **Note**
>
> Wenn Sie eine Domäne entfernen, passiert Folgendes:
>
> - Mit der Domäne verknüpfte Benutzer werden sofort bei allen Geräten abgemeldet und verlieren den Zugriff auf alle Kontakte, Chat-Unterhaltungen und Chatrooms.
> - Meetings, die von Benutzern aus dieser Domäne geplant wurden, starten nicht mehr.
> - Gesperrte Benutzer werden weiterhin auf den Seiten Users (Benutzer) und User detail (Benutzerdetails) mit dem Status Suspended (Gesperrt) angezeigt und können nicht auf ihre Daten zugreifen. Sie können mit ihrer E-Mail-Adresse keine neuen Amazon Chime Chime-Konten erstellen.
> - Registrierte Benutzer werden auf den Seiten Users (Benutzer) und User detail (Benutzerdetails) mit dem Status Released (Freigegeben) angezeigt und können nicht

auf ihre Daten zugreifen. Sie können mit ihrer E-Mail-Adresse ein neues Amazon Chime Chime-Konto erstellen.

- Wenn Sie ein Active Directory-Konto haben und eine Domain entfernen, die mit der primären E-Mail-Adresse eines Benutzers verknüpft ist, kann der Benutzer nicht auf Amazon Chime zugreifen und sein Profil wird gelöscht. Wenn Sie eine Domain entfernen, die mit der sekundären E-Mail-Adresse eines Benutzers verknüpft ist, kann sich dieser nicht mit dieser E-Mail-Adresse anmelden, hat aber weiterhin Zugriff auf seine Amazon Chime Chime-Kontakte und -Daten.
- Wenn Sie ein Enterprise OpenID Connect (OIDC) -Konto haben und eine Domain entfernen, die mit der primären E-Mail-Adresse eines Benutzers verknüpft ist, kann der Benutzer nicht mehr auf Amazon Chime zugreifen und sein Profil wird gelöscht.

2. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
3. Wählen Sie auf der Seite Konten den Namen des Teamkontos aus.
4. Klicken Sie im Navigationsbereich auf Settings (Einstellungen), Domains (Domänen).
5. Wählen Sie auf der Seite Domains (Domänen) die Option Remove domain (Domäne entfernen) aus.
6. Wählen Sie im Navigationsbereich Accounts (Konten), Account actions (Kontoaktionen) und Delete account (Konto löschen).
7. Bestätigen Sie, dass Sie das Konto löschen möchten.

Amazon Chime löscht alle Benutzerdaten, wenn Sie Ihr Konto löschen. Dazu gehört die Kündigung eines AWS Kontos, einzelner Amazon Chime Chime-Konten oder nicht verwalteter Amazon Chime Chime-Benutzer. Davon ausgenommen sind Daten ohne Inhalt, die sich auf Benutzerkonten und die Nutzung von Amazon Chime beziehen (Serviceattribute, die unter die Kundenvereinbarung fallen), die von Amazon Chime generiert werden.

Verwalten von Meeting-Einstellungen

Verwalten Sie Ihre Meeting-Einstellungen von der Amazon Chime Chime-Konsole aus.

Einstellungen der Meeting-Richtlinien

Verwalten Sie die Kontorichtlinien in der Amazon Chime Chime-Konsole unter Einstellungen, Besprechungen. Wählen Sie aus den folgenden Richtlinienoptionen aus.

Gemeinsame Kontrolle in der Bildschirmfreigabe aktivieren

Legen Sie fest, ob Benutzer in Ihrer Organisation während des Meetings die gemeinsame Steuerung ihrer Computer gewähren können. Teilnehmern, die gemeinsame Kontrolle über die Computer Ihres Benutzers anzufordern, wird in einer Fehlermeldung mitgeteilt, dass Remote-Kontrolle nicht verfügbar ist.

Ausgehende Anrufe aktivieren, um an Meetings teilzunehmen

Aktiviert die Funktion „Mich anrufen“ von Amazon Chime. Bietet Besprechungsteilnehmern die Möglichkeit, an Besprechungen teilzunehmen, indem sie einen Telefonanruf von Amazon Chime erhalten.

Einstellungen für Meeting-Anwendungen

Verwalten Sie den Zugriff auf die Meeting-Anwendung in der Amazon Chime Chime-Konsole unter Einstellungen, Meetings. Sie können die folgenden Optionen auswählen:

Erlauben Sie Benutzern, sich mit der Amazon Chime Meetings-App für Slack bei Amazon Chime anzumelden

Mit dieser Option können sich Benutzer in Ihrer Organisation über die Amazon Chime Meetings-App für Slack bei Amazon Chime anmelden. Weitere Informationen finden Sie unter Einrichtung der Amazon Chime Meetings-App für Slack.

Einstellungen für die Region des Meetings

Um die Qualität der Besprechungen zu verbessern und die Latenz zu reduzieren, verarbeitet Amazon Chime Besprechungen in der optimalen AWS Region für alle Teilnehmer. Sie können wählen, ob Amazon Chime die optimale Region für ein Meeting aus allen verfügbaren Regionen auswählen lässt oder ob Sie nur die von Ihnen ausgewählten Regionen verwenden möchten.

Sie können diese Einstellung jederzeit über die Meetings-Einstellungen Ihres Kontos aktualisieren. In Ihren Meeting-Einstellungen können Sie auch den Prozentsatz Ihrer Amazon Chime Chime-Meetings einsehen, die in jeder Region verarbeitet werden.

So aktualisieren Sie die Einstellungen der Meeting-Region

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.

2. Wählen Sie auf der Seite Accounts (Konten) den Namen Ihres Kontos aus.
3. Klicken Sie im Navigationsbereich auf Settings (Einstellungen), Meetings.
4. Wählen Sie bei Regions (Regionen) eine der folgenden Optionen aus:
   - Verwenden Sie alle verfügbaren Regionen, um die Meeting-Qualität sicherzustellen — Ermöglicht Amazon Chime, die Meeting-Verarbeitung für Sie zu optimieren.
   - Nur die von mir ausgewählten Regionen verwenden — Ermöglicht es Ihnen, Regionen aus dem Drop-down-Menü auszuwählen.
5. Wählen Sie Speichern.

Verwalten von Chat-Aufbewahrungsrichtlinien

Wenn Sie ein oder mehrere Amazon Chime Enterprise-Konten verwalten, können Sie Richtlinien zur Chat-Aufbewahrung für Folgendes festlegen:

- Chat-Konversationen, an denen nur Mitglieder Ihres Enterprise-Kontos teilnehmen.
- Chatrooms, die von Mitgliedern Ihres Enterprise-Kontos erstellt wurden.

Eine Aufbewahrungsrichtlinie löscht Nachrichten automatisch auf der Grundlage des von Ihnen festgelegten Zeitraums. Sie können Zeiträume von einem Tag bis zu 15 Jahren einstellen.

> **Note**
>
> Amazon Chime Enterprise-Konten haben eine Aufbewahrungsfrist von 90 Tagen. Die Richtlinie gilt für Konversationen mit Benutzern, die dem Konto angehören, und für Benutzer, die dem Konto nicht angehören.
> Aufbewahrungsrichtlinien gelten nicht für Folgendes:
>
> - Chat-Konversationen, an denen Mitglieder von Amazon Chime Enterprise-Konten nicht beteiligt sind
> - Chatrooms, die von Benutzern erstellt wurden, die keinem Amazon Chime Enterprise-Konto angehören

Wie sich Aufbewahrungsrichtlinien auf Amazon Chime Chime-Benutzer auswirken

Die Aufbewahrungsrichtlinien, die die Administratoren von Enterprise-Konten festlegen, wirken sich unterschiedlich auf Amazon Chime Chime-Benutzer aus, je nachdem, ob die Benutzer demselben Enterprise-Konto, einem anderen Enterprise-Konto oder einem Team-Konto angehören oder ob die Benutzer keinem Konto angehören.

Chat-Konversationen von Enterprise-Mitgliedern

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chat-Konversationen für Enterprise-Kontomitglieder auswirken.

Wenn die Chat-Konversation...	Die Aufbewahrungsrichtlinie ist...
Nur andere Mitglieder des Enterprise-Kontos des Benutzers	Vom Administrator des Benutzers festgelegt
Jeder Benutzer außerhalb des Enterprise-Kontos des Benutzers	Automatisch auf 90 Tage eingestellt

Chaträume für Enterprise-Mitglieder

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chatrooms für Enterprise-Kontomitglieder auswirken.

Wenn der Chatraum von...	Die Aufbewahrungsrichtlinie ist...
Ein Mitglied des Enterprise-Kontos des Benutzers	Vom Administrator des Benutzers festgelegt
Ein weiteres Enterprise-Kontomitglied	Vom Administrator des anderen Kontos festgelegt
Ein Nicht-Enterprise-Kontomitglied	Nicht zutreffend

Chat-Konversationen von Teammitgliedern

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chat-Konversationen für Teamkontomitglieder auswirken.

Wenn die Chat-Konversation...	Die Aufbewahrungsrichtlinie ist...
Nur Benutzer, die nicht Mitglied eines Enterprise-Kontos sind	Nicht zutreffend
Mindestens ein Mitglied eines Enterprise-Kontos	Automatisch auf 90 Tage eingestellt

Chatrooms für Teammitglieder

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chatrooms für Teamkontomitglieder auswirken.

Wenn der Chatraum von...	Die Aufbewahrungsrichtlinie ist...
Ein Teamkontobenutzer	Nicht zutreffend
Jeder, der kein Enterprise-Kontomitglied ist	Nicht zutreffend
Ein Mitglied eines Enterprise-Kontos	Vom Administrator des Enterprise-Kontos festgelegt

Amazon Chime Chime-Benutzer, die nicht Mitglieder eines Enterprise- oder Team-Kontos sind, unterliegen nur in Chatrooms, die von einem Mitglied eines Enterprise-Kontos erstellt wurden, den Aufbewahrungsrichtlinien für Chatrooms.

Chat-Konversationen mit Empfängern, die nicht zu einem Enterprise- oder Teamkonto gehören

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chat-Konversationen für Benutzer auswirken, die kein Amazon Chime Enterprise- oder Team-Konto sind.

Wenn die Chat-Konversation...	Die Aufbewahrungsrichtlinie ist...
Nur Benutzer, die nicht Mitglied eines Enterprise-Kontos sind	Nicht zutreffend

Wenn die Chat-Konversation...	Die Aufbewahrungsrichtlinie ist...
Mindestens ein Mitglied eines Enterprise-Kontos	Automatisch auf 90 Tage eingestellt

Chatrooms, die von Benutzern erstellt wurden, die nicht zu einem Enterprise- oder Teamkonto gehören

Die folgende Tabelle zeigt, wie sich Aufbewahrungsrichtlinien auf Chatrooms für Benutzer auswirken, die keine Mitglieder eines Amazon Chime Enterprise- oder Team-Kontos sind.

Wenn der Chatraum von...	Die Aufbewahrungsrichtlinie ist...
Ein Benutzer, der kein Mitglied eines Enterprise- oder Teamkontos ist	Nicht zutreffend
Ein Teamkontobenutzer	Nicht zutreffend
Ein Mitglied eines Enterprise-Kontos	Vom Administrator des Enterprise-Kontos festgelegt

Aktivieren der Chat-Aufbewahrung

Amazon Chime Enterprise-Kontoadministratoren können die Amazon Chime Chime-Konsole verwenden, um die Chat-Aufbewahrung für Chat-Konversationen und Chatrooms in ihrem Konto zu aktivieren. Sie können die Konsole auch verwenden, um die Chat-Aufbewahrungsfristen zu aktualisieren oder die Chat-Aufbewahrung jederzeit zu deaktivieren.

So aktivieren Sie die Chat-Aufbewahrung

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Konten den Namen des Kontos aus.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Retention aus.
4. Stellen Sie auf der Seite Aufbewahrung unter Aufbewahrung von Chat-Konversationen den Schieberegler auf Ein.

5. Geben Sie unter Aufbewahrungszeitraum eine Zahl in das erste Feld ein, öffnen Sie dann die Liste neben dem Feld und wählen Sie Tage, Wochen oder Jahre aus.
6. Wiederholen Sie unter Aufbewahrung im Chatroom die Schritte 4—5. Wenn Sie fertig sind, wählen Sie Speichern aus.

Innerhalb eines Tages nach der Festlegung einer Aufbewahrungsfrist verlieren Benutzer in Ihrem Konto den Zugriff auf Nachrichten, die außerhalb der Aufbewahrungsfrist gesendet wurden.

Chat-Nachrichten wiederherstellen

> **Note**
>
> Sie müssen ein Amazon Chime Enterprise-Kontoadministrator sein, um diese Schritte ausführen zu können.

Sie können Chat-Nachrichten innerhalb von 30 Tagen nach der Festlegung einer Chat-Aufbewahrungsfrist wiederherstellen. Wenn Sie Chat-Nachrichten wiederherstellen, stellen Sie alle Nachrichten wieder her, die von allen Benutzern in Ihrem Amazon Chime Chime-Konto gesendet wurden.

Innerhalb dieses Zeitraums von 30 Tagen können Sie einen der folgenden Schritte ausführen, um Nachrichten wiederherzustellen:

- Verwenden Sie die Amazon Chime Console, um die Datenspeicherung zu deaktivieren.

  -ODER-
- Verlängern Sie die Aufbewahrungsfrist.

Nach Ablauf der 30-tägigen Nachfrist werden alle Chat-Nachrichten, die unter die Aufbewahrungsfrist fallen, dauerhaft gelöscht. Neue Chat-Nachrichten werden dauerhaft gelöscht, sobald sie die Aufbewahrungsfrist überschritten haben.

Informationen zum Einstellen oder Ändern einer Aufbewahrungsfrist finden Sie Aktivieren der Chat-Aufbewahrung weiter oben in diesem Abschnitt.

Chat-Nachrichten werden auch dauerhaft aus Amazon Chime gelöscht, wenn Sie oder ein Kontomitglied eine der folgenden Aktionen ausführen:

- Löschen Sie einen Amazon Chime Chime-Chatroom. Weitere Informationen zum Löschen von Chatrooms finden Sie unter Löschen von Chatrooms im Amazon Chime Chime-Benutzerhandbuch.
- Beenden Sie ein Amazon Chime Chime-Meeting, in dem Chat-Nachrichten vorhanden sind.

> **Note**
>
> Bei Bedarf können Sie Chat-Nachrichten aus einer Besprechung manuell kopieren und speichern, müssen dies jedoch tun, bevor die Besprechung endet. Weitere Informationen finden Sie unter Verwenden des Chats während eines Meetings im Amazon Chime Chime-Benutzerhandbuch.

Löschen von Chat-Nachrichten

Um die Richtlinien zur Datenspeicherung einzuhalten, speichert Amazon Chime alle Chat-Nachrichten und verhindert, dass Endbenutzer die von ihnen gesendeten Nachrichten löschen. Amazon Chime Chime-Systemadministratoren können jedoch zwei APIs verwenden, um einzelne Nachrichten aus Konversationen und Chatrooms zu löschen. Die Nachrichten müssen sich im Amazon Chime Chime-Konto des Administrators befinden.

Benutzer können das Löschen von Nachrichten beantragen, indem sie Ihnen eine Nachrichten-ID und eine entsprechende Konversations- oder Chatroom-ID senden. Das Thema Verwenden von Chat-Funktionen im Amazon Chime Chime-Benutzerhandbuch erklärt, wie das geht.

Wenn Sie eine Löschanfrage erhalten, können Sie Code schreiben oder die AWS CLI verwenden, um die folgenden APIs aufzurufen.

So entfernen Sie eine Nachricht

- Führen Sie eine der folgenden Aktionen aus:
  - Für Konversationsnachrichten — Verwenden Sie die RedactConversationMessageAPI.

    Führen Sie in der CLI den folgenden Befehl aus:

    ```
    aws chime redact-conversation-message --conversation-id id_string --message-id id_string
    ```
  - Für Chatroom-Nachrichten — Verwenden Sie die RedactRoomMessageAPI.

Führen Sie in der CLI den folgenden Befehl aus:

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

Herstellen einer Verbindung mit Active Directory

Wenn Sie Ihr Amazon Chime Chime-Administratorkonto mit einem Active Directory verbinden, können Sie von den folgenden Funktionen profitieren:

- Ihre Amazon Chime Chime-Benutzer können sich mit ihren Active Directory-Anmeldeinformationen anmelden.
- Als Amazon Chime Chime-Administrator entscheiden Sie, welche Sicherheitsfunktionen für Anmeldeinformationen hinzugefügt werden sollen, einschließlich Passwortrotation, Regeln zur Passwortkomplexität und Multi-Faktor-Authentifizierung.
- Wenn Sie Benutzerkonten aus Ihrem Active Directory entfernen, werden auch deren Amazon Chime Chime-Konten entfernt.
- Sie können angeben, welche Active Directory-Gruppen Amazon Chime Pro-Berechtigungen erhalten.
  - Mehrere Gruppen können so konfiguriert werden, dass sie Anspruch auf Basic- oder Pro-Berechtigungen haben.
  - Benutzer müssen Mitglied einer der Gruppen sein, um sich bei Amazon Chime anmelden zu können.
  - Benutzer in beiden Gruppen erhalten eine Pro-Lizenz.

Weitere Informationen zur Verwaltung von Benutzerberechtigungen finden Sie unterVerwaltung der Benutzerberechtigungen und des Zugriffs.

Voraussetzungen

Bevor Sie eine Verbindung zu Ihrem Active Directory in Amazon Chime herstellen können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass Sie über die richtigen AWS Identity and Access Management Berechtigungen zum Konfigurieren von Domänen, aktiven Verzeichnissen und Verzeichnisgruppen

verfügen. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon Chime.

- Erstellen Sie ein Verzeichnis AWS Directory Service , das in der Region USA Ost (Nord-Virginia) konfiguriert ist. Weitere Informationen finden Sie im Administrationshandbuch zu AWS Directory Service. Amazon Chime kann über AD Connector, Microsoft AD oder Simple AD eine Verbindung herstellen.
- Beanspruchen Sie eine Domain, um ein Amazon Chime Enterprise-Konto zu erstellen, oder konvertieren Sie Ihr bestehendes Team-Konto in ein Enterprise-Konto. Wenn Ihre Benutzer geschäftliche E-Mail-Adressen von mehr als einer Domain haben, stellen Sie sicher, dass Sie alle diese Domains beanspruchen. Weitere Informationen finden Sie unter Beantragen einer Domäne und Umwandlung eines Teamkontos in ein Enterprise-Konto.

Verbindung zu Ihrem Active Directory in Amazon Chime herstellen

Nachdem Sie Ihr Active Directory mit Amazon Chime verbunden haben, werden Ihre Benutzer aufgefordert, sich mit ihren Verzeichnisanmeldedaten anzumelden, wenn sie eine E-Mail-Adresse von einer der Domains verwenden, die Sie in Ihrem Amazon Chime Enterprise-Konto beansprucht haben.

So stellen Sie eine Verbindung zu Ihrem Active Directory in Amazon Chime her

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich für Identity Active Directory aus.
3. Wählen Sie unter Cloud-Verzeichnis-ID das AWS Directory Service Verzeichnis aus, das für Amazon Chime verwendet werden soll, und wählen Sie dann Connect.

   > **Note**
   >
   > Sie finden Ihre Verzeichnis-ID mithilfe der AWS Directory Service -Konsole.

4. Nachdem Ihr Verzeichnis eine Verbindung hergestellt hat, wählen Sie Neue Gruppe hinzufügen.
5. Geben Sie unter Gruppe den Gruppennamen ein. Der Name muss genau mit einer Active-Directory-Gruppe im Zielverzeichnis übereinstimmen. Active-Directory-Organisationseinheiten (OUs) werden nicht unterstützt.
6. Wählen Sie für Berechtigungen die Option Basic oder Pro aus.
7. Wählen Sie Add Group (Gruppe hinzufügen) aus.
8. (Optional) Wiederholen Sie diesen Vorgang, um weitere Verzeichnisgruppen zu erstellen.

Konfigurieren mehrerer E-Mail-Adressen

Nachdem Sie in Amazon Chime eine Verbindung zu Ihrem Active Directory hergestellt haben, können sich Benutzer mit ihren Active Directory-Anmeldeinformationen bei Amazon Chime anmelden. Ihren Benutzern können in Ihrem Active Directory mehrere E-Mail-Adressen zugewiesen werden. Damit sich Ihre Benutzer mit ihren Active Directory-Anmeldeinformationen bei Amazon Chime anmelden können, müssen Sie jede zutreffende E-Mail-Domain in Ihrem Amazon Chime Chime-Administratorkonto beanspruchen. Weitere Informationen finden Sie unter Beantragen einer Domäne.

> **Note**
>
> Wenn Ihre Benutzer versuchen, sich mit einer E-Mail-Adresse von einer Domain anzumelden, die nicht beansprucht wurde, werden sie aufgefordert, sich mit Log in with Amazon anzumelden. Sie können sich nicht bei Ihrem Administratorkonto anmelden, wenn sie eine E-Mail-Adresse von einer nicht beanspruchten Domain verwenden.

Bei der Anzeige von Benutzerdetails in der Amazon Chime-Konsole verwendet Amazon Chime die einzelne E-Mail-Adresse im `EmailAddress` Attribut aus Ihrem Active Directory als primäre E-Mail-Adresse jedes Benutzers. Dies ist die einzige E-Mail-Adresse, die Sie für den Benutzer in der Amazon Chime Chime-Konsole sehen können. Benutzer können sich jedoch mit allen zusätzlichen Adressen anmelden, die im `ProxyAddress` Attribut aufgeführt sind, sofern Sie diese Domains in Ihrem Amazon Chime Chime-Konto beanspruchen.

Beispiel einer falschen Konfiguration

Ein Benutzer mit dem Benutzernamen shirley.rodriguez ist Mitglied eines Amazon Chime-Kontos, das zwei Domains beansprucht hat: example.com und example.org. In Active Directory hat dieser Benutzer die folgenden drei E-Mail-Adressen:

- Primäre E-Mail-Adresse: shirley.rodriguez@example.com
- Proxy-E-Mail-Adresse 1: shirley.rodriguez@example2.com
- Proxy-E-Mail-Adresse 2: srodriguez@example.org

Dieser Benutzer kann sich mit shirley.rodriguez@example.com oder srodriguez@example.org und shirley.rodriguez bei Amazon Chime anmelden. Wenn sie versuchen, sich mit shirley.rodriguez@example2.com anzumelden, werden sie aufgefordert, sich bei Amazon

anzumelden, und sie sind nicht Teil Ihres verwalteten Kontos. Aus diesem Grund ist es wichtig, dass Sie alle E-Mail-Domains Ihrer Benutzer für sich beanspruchen.

Andere Amazon Chime Chime-Benutzer können diesen Benutzer als Kontakt hinzufügen, ihn zu Besprechungen einladen oder ihn als Delegierten hinzufügen, indem sie entweder die E-Mail-Adresse shirley.rodriguez@example.com oder srodriguez@example.org verwenden.

Beispiel einer richtigen Konfiguration

Ein Benutzer mit dem Benutzernamen shirley.rodriguez ist Mitglied eines Amazon Chime Chime-Kontos, das drei Domains beansprucht hat: example.com, example2.com und example.org. In Active Directory hat dieser Benutzer die folgenden drei E-Mail-Adressen:

- Primäre E-Mail-Adresse: shirley.rodriguez@example.com
- Proxy-E-Mail-Adresse 1: shirley.rodriguez@example2.com
- Proxy-E-Mail-Adresse 2: srodriguez@example.org

Dieser Benutzer kann sich mit jeder seiner geschäftlichen E-Mail-Adressen bei Amazon Chime anmelden. Andere Benutzer können ihn auch als Kontakt hinzufügen, ihn zu Besprechungen einladen oder ihn mit einer ihrer geschäftlichen E-Mail-Adressen als Delegierten hinzufügen.

Herstellen einer Verbindung mit Okta-SSO

Wenn Sie über ein Enterprise-Konto verfügen, können Sie zum Authentifizieren und Zuweisen von Benutzerberechtigungen eine Verbindung mit Okta-SSO herstellen.

> **Note**
>
> Wenn Sie ein Enterprise-Konto erstellen müssen, das Ihnen ermöglicht, alle Benutzer innerhalb einer bestimmten Gruppe von E-Mail-Adressendomänen zu verwalten, informieren Sie sich unter Beantragen einer Domäne.

Um Amazon Chime mit Okta zu verbinden, müssen zwei Anwendungen in der Okta Administration Console konfiguriert werden. Die erste Anwendung wird manuell konfiguriert und verwendet OpenID Connect, um Benutzer beim Amazon Chime Chime-Service zu authentifizieren. Die zweite Anwendung ist als Amazon Chime SCIM Provisioning im Okta Integration Network (OIN) verfügbar.

Es ist so konfiguriert, dass es Updates über Änderungen an Benutzern und Gruppen an Amazon Chime sendet.

So stellen Sie eine Verbindung mit Okta-SSO her

1. Erstellen Sie die Amazon Chime Chime-Anwendung (OpenID Connect) in der Okta Administration Console:

    1. Melden Sie sich bei dem Okta Administration Dashboard an und wählen Sie dann Add Application (Anwendung hinzufügen). Wählen Sie im Dialogfeld Create New Application (Neue Anwendung erstellen) nacheinander Web, Next (Weiter) aus.
    2. Konfigurieren der Application Settings (Anwendungseinstellungen):
        a. Name der Anwendung **`Amazon Chime`**.
        b. Geben Sie für Login Redirect URI (Anmeldungsumleitungs-URI) den folgenden Wert ein: **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
        c. Wählen Sie im Abschnitt Allowed Grant Types (Zugelassene Erteilungstypen) alle Optionen aus, um sie zu aktivieren.
        d. Wählen Sie im Drop-down-Menü Login initiated by (Anmeldung initiiert von) die Option Either (Okta or App) (Eine von beiden (Okta oder App)) aus und wählen Sie alle zugehörigen Optionen.
        e. Geben Sie für Initiate Login URI (Anmeldungsinitiierungs-URI) den folgenden Wert ein: **`https://signin.id.ue1.app.chime.aws/auth/okta`**
        f. Wählen Sie Speichern.
        g. Lassen Sie diese Seite geöffnet, da Sie die Angaben für Client ID (Client-ID), Client secret (Geheimer Client-Schlüssel) und Issuer URI (Aussteller-URI) für Schritt 2 benötigen.
2. Gehen Sie in der Amazon Chime Chime-Konsole wie folgt vor:

    1. Wählen Sie oben auf der Seite Okta single-sign on configuration (Okta-SSO-Konfiguration) die Option Set up incoming keys (Eingehende Schlüssel einrichten) aus.
    2. Im Dialogfeld Setup incoming Okta keys (Eingehende Okta-Schlüssel einrichten):
        a. Fügen Sie die Angaben für Client ID (Client-ID) und Client secret (Geheimer Client-Schlüssel) von der Seite Okta Application Settings (Okta-Anwendungseinstellungen) ein.
        b. Fügen Sie die entsprechende Issuer URI (Aussteller-URI) von der Seite Okta API ein. Der Aussteller-URI muss eine Okta-Domäne sein, z. B. `https://example.okta.com`.

3. Richten Sie die Amazon Chime SCIM Provisioning-Anwendung in der Okta Administration Console ein, um ausgewählte Identitäts- und Gruppenmitgliedschaftsinformationen mit Amazon Chime auszutauschen:

   1. Wählen Sie in der Okta Administration Console Applications, Add Application, suchen Sie nach Amazon Chime SCIM Provisioning und fügen Sie die Anwendung hinzu.

      > **Important**
      >
      > Wählen Sie während der erstmaligen Einrichtung sowohl Do not display application to users (Anwendung nicht Benutzern anzeigen) und Do not display application icon in the Okta Mobile App (Anwendungssymbol nicht in der mobilen Okta-App anzeigen) aus und klicken Sie dann auf Done (Fertig).

   2. Wählen Sie auf der Registerkarte Provisioning (Bereitstellung) die Option Configure API Integration (API-Integration konfigurieren) und danach Enable API Integration (API-Integration aktivieren) aus. Lassen Sie diese Seite geöffnet, da Sie für den folgenden Schritt einen API-Zugriffsschlüssel kopieren müssen.
   3. Wählen Sie in der Amazon Chime Chime-Konsole Create access key aus, um einen API-Zugriffsschlüssel zu erstellen. Kopieren Sie ihn in das Feld Okta API Token (Okta-API-Token) im Dialogfeld Configure API Integration (API-Integration konfigurieren). Wählen Sie dann Test the Integration (Integration testen) und klicken Sie auf Save (Speichern).
   4. Konfigurieren Sie die Aktionen und Attribute, die Okta zur Aktualisierung von Amazon Chime verwendet. Klicken Sie auf der Registerkarte Provisioning (Bereitstellung) im Bereich To App (Zur App) auf Edit (Bearbeiten). Wählen Sie unter den Optionen Enable Users (Benutzer aktivieren), Update User Attributes (Benutzerattribute aktualisieren) und Deactivate Users (Benutzer deaktivieren) aus. Klicken Sie dann auf Save (Speichern).
   5. Erteilen Sie auf der Registerkarte Assignments (Zuweisungen) Benutzerberechtigungen für die neue SCIM-App.

      > **Important**
      >
      > Wir empfehlen, Berechtigungen über eine Gruppe zu gewähren, die alle Benutzer enthält, die Zugriff auf Amazon Chime haben sollten, unabhängig von der Lizenz. Bei der Gruppe muss es sich um die gleiche Gruppe handeln, wie die Gruppe, mit

der die benutzerbezogene OIDC-Anwendung zuvor in Schritt 1 zugewiesen wurde. Andernfalls können sich Endbenutzer nicht anmelden.

6. Konfigurieren Sie auf der Registerkarte Push-Gruppen, welche Gruppen und Mitgliedschaften mit Amazon Chime synchronisiert werden. Diese Gruppen werden verwendet, um zwischen Basic- und Pro-Benutzern zu unterscheiden.

4. Konfigurieren Sie Verzeichnisgruppen in Amazon Chime:

   1. Navigieren Sie in der Amazon Chime Chime-Konsole zur Okta-Single-Sign-On-Konfigurationsseite.
   2. Wählen Sie unter Directory groups (Verzeichnisgruppen) die Option Add new groups (Neue Gruppen hinzufügen) aus.
   3. Geben Sie den Namen einer Verzeichnisgruppe ein, die zu Amazon Chime hinzugefügt werden soll. Der Name muss mit einer der zuvor in Schritt 3-f konfigurierten Push Groups (Push-Gruppen) exakt übereinstimmen.
   4. Bestimmen Sie, ob Benutzer in dieser Gruppe, Basic- oder Pro-Fähigkeiten erhalten sollen, und klicken Sie auf Save (Speichern). Wiederholen Sie diesen Vorgang, um zusätzliche Gruppen zu konfigurieren.

      > **Note**
      >
      > Wenn in einer Fehlermeldung darauf hingewiesen wird, dass die Gruppe nicht gefunden wurde, wurden die beiden Systeme möglicherweise nicht synchronisiert. Bitte warten Sie einige Minuten und wählen Sie dann erneut Add new groups (Neue Gruppen hinzufügen).

Die Auswahl der Funktionen Basic oder Pro für die Benutzer in Ihrer Verzeichnisgruppe wirkt sich auf die Lizenz, die Funktionen und die Kosten dieser Benutzer in Ihrem Amazon Chime Enterprise-Konto aus. Weitere Informationen finden Sie unter -Preisgestaltung.

Bereitstellen des Amazon Chime Chime-Add-Ins für Outlook

Amazon Chime bietet zwei Add-Ins für Microsoft Outlook: das Amazon Chime Add-In für Outlook unter Windows und das Amazon Chime Add-In für Outlook. Mit diesen Add-ins werden die gleichen Zeitplanungsfunktionen verfügbar, sie unterstützen jedoch Benutzer unterschiedlicher Typen. Microsoft Office 365-Abonnenten und Organisationen, die Microsoft Exchange 2013 oder höher

vor Ort verwenden, können das Amazon Chime Add-In für Outlook verwenden. Windows-Benutzer mit einem lokalen Exchange-Server, auf dem Exchange Server 2010 oder früher ausgeführt wird, und Outlook 2010-Benutzer müssen das Amazon Chime Chime-Add-In für Outlook unter Windows verwenden.

Windows-Benutzer, die nicht berechtigt sind, das Amazon Chime Add-in für Outlook zu installieren, sollten sich für das Amazon Chime Add-in für Outlook unter Windows entscheiden.

Informationen zur Auswahl des richtigen Add-ins für Sie und Ihr Unternehmen siehe Choosing the Right Outlook-Add-In.

Wenn Sie das Amazon Chime Add-In für Outlook für Ihre Organisation wählen, können Sie es Ihren Benutzern mit zentraler Bereitstellung bereitstellen. Weitere Informationen finden Sie im Amazon Chime Add-In für Outlook-Installationshandbuch für Administratoren.

Einrichtung der Amazon Chime Meetings-App für Slack

Wenn du Slack Enterprise Grid Organizations verwendest und eine Slack-Organisation besitzt oder verwaltest, kannst du die Amazon Chime Meetings-App für Slack für deine Organisationen einrichten. Wenn du ein Workspace-Administrator in Slack bist, kannst du die Amazon Chime Meetings-App für Slack für deine Workspaces einrichten.

Die Schritte in den folgenden Abschnitten erklären, wie du beide Arten von Einstellungen durchführst und wie du zusätzliche Aufgaben wie die Migration eines Workspace zu einer Organisation erledigst.

Themen

Installation der Amazon Chime Meetings-App für Slack in einer Organisation

Durch die Installation der Amazon Chime Meetings-App für Slack in einer Slack-Organisation können Benutzer Sofortbesprechungen und Anrufe mit anderen Benutzern in den verschiedenen Workspaces dieser Organisation starten. Außerdem können Workspace-Administratoren die Meeting-Anwendung

Amazon Chime Meetings App for Slack automatisch in allen neuen Workspaces installieren. In den folgenden Schritten wird erklärt, wie.

> **Note**
>
> Bei den folgenden Schritten wird davon ausgegangen, dass du Inhaber oder Administrator einer Organisation bist und dass du dich bei der Slack-Managementkonsole anmelden kannst.

So richten Sie die Amazon Chime Meetings-App für Slack in einer Organisation ein

1. Wähle im linken Bereich der Slack-Managementkonsole Apps aus.

   Die Apps-Seite wird angezeigt und listet die installierten Apps der Organisation auf, falls vorhanden.
2. Wähle in der oberen rechten Ecke der Seite Apps verwalten und wähle dann App installieren.

   Das Dialogfeld „Eine zu installierende App suchen“ wird angezeigt.
3. Suchen Sie weiter **`Amazon Chime Meetings`** und wählen Sie es dann in den Suchergebnissen aus.

   Das Dialogfeld Amazon Chime Meetings zu Workspaces hinzufügen wird angezeigt und listet die Workspaces in der Organisation auf.
4. Wählen Sie den Workspace oder die Workspaces aus, in denen Sie die Amazon Chime Meetings-App für Slack installieren möchten.
5. Wählen Sie optional Standard für future Workspaces, wenn Sie die Amazon Chime Meetings-App für Slack automatisch in allen neuen Workspaces installieren möchten, und wählen Sie dann Weiter.

   Das Dialogfeld „Die angeforderten Berechtigungen dieser App überprüfen“ wird angezeigt und zeigt die Berechtigungen und Aktionen für die Amazon Chime Meetings-App für Slack an.
6. Wählen Sie Weiter aus.
7. Wenn du dich dafür entschieden hast, die Amazon Chime Meetings-App für Slack standardmäßig in neuen Workspaces zu installieren, wähle Ich bin bereit, diese App als Standard für future Workspaces festzulegen und wähle dann Speichern. Andernfalls wählen Sie einfach Speichern.

> **Note**
>
> Sie können OAuth auch verwenden, um Apps in Ihren Organisationen zu installieren. Weitere Informationen findest du in der Slack-Hilfe unter Installation mit OAuth.

Installation der Amazon Chime Meetings-App für Slack in Workspaces

Durch die Installation der Amazon Chime Meetings-App für Slack in einem Workspace können Benutzer Sofortbesprechungen und Telefonate mit anderen Benutzern in diesem Workspace starten. Benutzer benötigen kein Amazon Chime-Benutzerprofil, um die Amazon Chime Meetings-App für Slack zu verwenden. Sie können sich jederzeit mit ihren Slack-Benutzerprofilen anmelden und Anrufe oder Besprechungen starten. Wenn Benutzer Besprechungen mit mehr als einer anderen Person abhalten müssen, müssen Sie ein Amazon Chime Team-Konto einrichten und diesen zusätzlichen Benutzern Pro-Berechtigungen gewähren. Weitere Informationen zum Starten von Amazon Chime-Anrufen und -Besprechungen finden Sie unter Verwenden der Amazon Chime Meetings-App für Slack im Amazon Chime Chime-Benutzerhandbuch. Weitere Informationen zur Einrichtung eines Amazon Chime Team-Kontos finden Sie Workspaces mit Amazon Chime Team-Konten verknüpfen in diesem Handbuch.

Um die Amazon Chime Meetings-App für Slack für Slack-Workspaces zu installieren

1. Navigiere zum App-Verzeichnis von Slack und suche die Amazon Chime Meetings-App.
2. Wähle Zu Slack hinzufügen, um die Amazon Chime Meetings-App für Slack aus dem App-Verzeichnis von Slack zu installieren.
3. Konfiguriere die Einstellung Anrufe in deinem Slack-Workspace mit Amazon Chime auf Anrufe in Slack aktivieren.

Workspaces zu Organisationen migrieren

Wenn du eine Slack-Organisation besitzt, kannst du Workspaces in diese Organisation migrieren. Weitere Informationen zur Migration von Workspaces findest du in der Slack-Hilfe unter Workspaces zu Enterprise Grid migrieren.

Workspaces mit Amazon Chime Team-Konten verknüpfen

Verknüpfen Sie Ihren Workspace mit einem Amazon Chime Team-Konto, um die Berechtigungen Ihrer Benutzer zu verwalten. Sie können Meeting-Gastgeber auf Amazon Chime Pro upgraden, sodass sie Besprechungen mit bis zu 250 Teilnehmern und 25 Videokacheln starten und Telefonnummern zur Audioeinwahl hinzufügen können. Weisen Sie Benutzern Amazon Chime Basic-Berechtigungen zu, damit sie one-on-one Besprechungen starten oder an Amazon Chime Chime-Besprechungen teilnehmen können. Weitere Informationen finden Sie unter Amazon Chime Chime-Preise.

> **Note**
>
> Wenn du ein Amazon Chime Team-Konto mit deinem Slack-Workspace verknüpfst, können sich Benutzer über die Amazon Chime Meetings-App für Slack bei Amazon Chime anmelden. Sie können diese Einstellung jederzeit ändern. Weitere Informationen finden Sie unter Verwalten von Meeting-Einstellungen.

Bevor du deinen Slack-Workspace mit einem Amazon Chime Team-Konto verknüpfen kannst, musst du ein AWS Konto erstellen. Weitere Informationen darüber, wie du ein AWS Konto erstellst, findest du unter. Voraussetzungen für Amazon Chime Chime-Systemadministratoren

Um deinen Slack-Workspace mit einem Amazon Chime Team-Konto zu verknüpfen, wenn du die Amazon Chime Meetings-App für Slack installierst

1. Wählen Sie unmittelbar nach der Installation der Amazon Chime Meetings-App für Slack in Ihrem Slack-Workspace die Option Jetzt upgraden aus.
2. Folgen Sie den Anweisungen, um sich mit Ihren AWS Kontoanmeldeinformationen bei der Amazon Chime-Konsole anzumelden.
3. Folgen Sie den Anweisungen, um ein neues Team-Konto in Amazon Chime zu erstellen, oder wählen Sie ein vorhandenes aus.

   - Neues Konto erstellen — Erstellen Sie ein neues Amazon Chime Chime-Konto, zu dem Sie Ihre Slack-Benutzer einladen können. Geben Sie einen Kontonamen ein, wählen Sie aus, ob Sie Ihre Slack-Benutzer einladen möchten, und wählen Sie dann Create (Erstellen) aus.
   - Wählen Sie ein bestehendes Konto — Wählen Sie ein vorhandenes Amazon Chime Chime-Konto aus, zu dem Sie Ihre Slack-Benutzer einladen möchten. Wählen Sie das Konto und dann Invite (Einladen)aus.

Wenn Sie Ihre Slack-Benutzer zu Amazon Chime einladen, erhalten sie eine E-Mail-Einladung. Wenn sie die Einladung annehmen, werden sie automatisch auf Amazon Chime Pro aktualisiert.

Wenn du deinen Slack-Workspace bei der Installation der Amazon Chime Meetings-App für Slack nicht mit einem Amazon Chime Team-Konto verknüpft hast, kannst du dies nachträglich tun, indem du die folgenden Schritte ausführst.

Um deinen Slack-Workspace mit einem Amazon Chime Team-Konto zu verknüpfen, nachdem du die Amazon Chime Meetings-App für Slack installiert hast

1. Melde dich mit deinem Konto an. AWS
2. Melden Sie sich in Ihrem Slack Workspace als Administrator an.
3. Gehen Sie zu https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Folgen Sie den Anweisungen, um ein neues Team-Konto in Amazon Chime zu erstellen, oder wählen Sie ein vorhandenes Konto aus.

    - Neues Konto erstellen — Erstellen Sie ein neues Amazon Chime Chime-Konto, zu dem Sie Ihre Slack-Benutzer einladen können. Geben Sie einen Kontonamen ein, wählen Sie aus, ob Sie Ihre Slack-Benutzer einladen möchten, und wählen Sie dann Create (Erstellen) aus.
    - Wählen Sie ein bestehendes Konto — Wählen Sie ein vorhandenes Amazon Chime Chime-Konto aus, zu dem Sie Ihre Slack-Benutzer einladen möchten. Wählen Sie das Konto und dann Invite (Einladen)aus.

Verwalten von Benutzern

> **Note**
>
> Bei den Schritten in diesem Abschnitt wird davon ausgegangen, dass Sie über eine Reihe von Benutzer-E-Mail-Adressen verfügen oder dass Sie Ihr Administratorkonto mit Active Directory verbunden haben. Weitere Informationen finden Sie unterHerstellen einer Verbindung mit Active Directory, in diesem Handbuch.

Sie verwenden die Amazon Chime Chime-Konsole, um Benutzer hinzuzufügen und zu verwalten. Sie fügen Benutzer hinzu, indem Sie sie einladen. Wenn sie Ihre Einladungen annehmen, werden sie unter Benutzer angezeigt. Dort werden alle Benutzer in Ihrem Konto und deren Benutzerdetails aufgeführt. Weitere Informationen finden Sie unter Anzeigen von Benutzerdetails.

Administratoren von Konten, die Login with Amazon (LWA) verwenden, sehen auch Optionen zur Verwaltung von Berechtigungsstufen und zum Entfernen von Benutzern aus einem Konto. Diese Aktionen werden über Active Directory oder Okta verwaltet, je nachdem, für welche dieser Aktionen Sie ein Konto konfigurieren. Weitere Informationen finden Sie unter Verwaltung der Benutzerberechtigungen und des Zugriffs.

Inhalt

Hinzufügen von Benutzern

Sie fügen Benutzer zu einem Amazon Chime Chime-Konto hinzu, indem Sie sie einladen, dem Konto beizutreten. Sie senden Einladungen an potenzielle Benutzer von der Amazon Chime Chime-Konsole aus. In diesen Schritten wird erklärt, wie.

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.

   Eine Liste der Konten, die Sie verwalten, wird angezeigt.
2. Wählen Sie das Konto aus, zu dem Sie Mitglieder hinzufügen möchten, und wählen Sie dann Benutzer einladen aus.

   Das Dialogfeld „Neue Benutzer einladen“ wird angezeigt.
3. Geben Sie die E-Mail-Adressen der Benutzer ein, die Sie einladen möchten. Trennen Sie die einzelnen Adressen durch ein Semikolon (;).
4. Wählen Sie Invite users.

Die neuen Benutzer werden in der Liste angezeigt. Wenn Sie Benutzer zu einem Team-Konto einladen, werden ihre Daten erst angezeigt, wenn sie Ihre Einladung annehmen.

Anzeigen von Benutzerdetails

In der Amazon Chime Chime-Konsole können Sie unter Benutzer eine Liste aller Benutzer in Ihrem Konto und deren Benutzerdetails einsehen. Suchen Sie anhand seiner E-Mail-Adresse nach einem bestimmten Benutzer und wählen Sie seinen Namen aus, um dessen Benutzerdetails zu sehen. Unter Benutzerdetails können Sie detaillierte Informationen über den Benutzer einsehen und dessen Benutzerkonto aktualisieren.

In der folgenden Tabelle sind die Benutzerdetails aufgeführt, die in der Konsole angezeigt werden.

> **Note**
>
> Vollständige Benutzerdetails werden Team-Kontobenutzern erst angezeigt, nachdem sie ihre Einladungen angenommen haben.

Feld	Beschreibung	Beispiel
Anzeigename	Der Name des Benutzers, der in Amazon Chime angezeigt wird. Für Benutzer von Login with Amazon (LWA) ist dies der vollständige Name. Für Active Directory-Benutzer wird das DISPLAY_NAME_ATTRIBUTE verwendet.	Major, Mary
E-Mail-Adresse	Für LWA-Benutzer ist dies die für die Registrierung verwendete die E-Mail-Adresse. Für Active Directory-Benutzer wird die primäre E-Mail-Adresse von Active Directory angezeigt.	mary.major@example.com
Registrierung	Der aktuelle Registrierungsstatus des Benutzers. Die möglichen Werte sind für Enterprise-Konten, an die keine Einladungen gesendet werden, anders als für Teamkonten, an die Einladungen gesendet werden.	Registriert, Nicht registriert (für ein Teamkonto) oder Gesperrt (für ein Enterprise-Konto)
Permission tier (Berechtigungsstufe)	Standardmäßig auf Pro eingestellt, um Benutzern das Abhalten von Besprechungen zu ermöglichen. Kann in Basic geändert werden.	Pro, Basic
Invited (Eingeladen)	Für Teamkonten das Datum, an dem der Benutzer zum Konto eingeladen wurde.	01/05/2020

Feld	Beschreibung	Beispiel
Joined (Beigetreten)	Das Datum, an dem sich der Benutzer zum ersten Mal bei Amazon Chime angemeldet hat. Für Pro-Testbenutzer ist dies auch das Datum, an dem ihre Pro-Testversion begann.	01.10.2020
Personal PIN (Persönliche PIN)	Die persönliche Meeting-PIN, mit der der Benutzer Meetings planen kann.	0123456789
Privacy setting (Datensch utzeinstellung)	Die aktuell vom Benutzer ausgewählte Einstellung.	Public (Öffentlich) oder Private (Privat)
Meetings attended (Teilgeno mmene Meetings)	Die Anzahl der Meetings, an denen ein Benutzer teilgenom men hat.	87
Meetings organized (Abgehalt ene Meetings)	Die Anzahl der Meetings, die ein Benutzer abgehalten hat.	12
Meeting satisfaction (Zufriede nheit mit dem Meeting)	Der Prozentsatz der positiven Antworten auf die end-of-me eting Umfrage.	92%
Last active date (Datum zuletzt aktiv)	Das Datum, an dem der Benutzer zuletzt aktiv war.	12.06.2020
Chat messages sent (Gesendete Chat-Nachrichten)	Die Anzahl der Chat-Nach richten, die der Benutzer gesendet hat.	1025
"Phone number (Telefonn ummer)"	Die einem Benutzer zugewiesene Telefonnummer (sofern vorhanden).	+12065550100

Verwaltung der Benutzerberechtigungen und des Zugriffs

Verwalten Sie, auf welche Funktionen Ihre Amazon Chime Chime-Benutzer zugreifen können, indem Sie ihnen Pro- oder Basic-Berechtigungen zuweisen. Benutzer mit Basisberechtigungen können keine Besprechungen veranstalten, aber sie können an Besprechungen teilnehmen und den Chat nutzen. Weitere Informationen zu den Funktionen, auf die Benutzer mit Pro- und Basic-Berechtigungen zugreifen können, finden Sie unter Pläne und Preise.

Legen Sie fest, wer sich bei Ihrem Amazon Chime-Administratorkonto anmelden kann, indem Sie Benutzer einladen oder sperren. Nur Administratoren von Enterprise-Konten können Benutzer sperren. Teamkontoadministratoren können Benutzer aus ihren Konten entfernen, sodass sie nicht mehr für die Benutzerberechtigungen zahlen. Sie können den Benutzer jedoch nicht sperren, um ihn daran zu hindern, sich anzumelden. Weitere Informationen zu den Unterschieden zwischen Enterprise- und Teamkonten finden Sie unterVerwaltung Ihrer Amazon Chime Chime-Konten.

Verwalten von Benutzerberechtigungen

Als Amazon Chime Chime-Administrator können Sie Pro- und Basic-Berechtigungen für die Benutzer in Ihrem Amazon Chime Chime-Konto verwalten.

Wenn Active Directory oder Okta für Ihr Amazon Chime Chime-Konto konfiguriert ist, verwalten Sie Benutzerberechtigungen über die Mitgliedschaft in ihrer Verzeichnisgruppe. Wenn Sie Active Directory oder Okta nicht konfiguriert haben, verwalten Sie die Benutzerberechtigungen über die Amazon Chime Chime-Konsole.

Teamkonten und Enterprise Login with Amazon

Wenn Sie ein Amazon Chime Team-Konto oder ein Enterprise LWA-Konto verwalten, bei dem sich Benutzer mit ihren Login with Amazon (LWA) -Konten anmelden, können Sie Pro- und Basic-Berechtigungen in der Amazon Chime Chime-Konsole verwalten.

Um Benutzerberechtigungen für Team- und Enterprise LWA-Konten zu verwalten

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie für Konten den Namen des Amazon Chime Chime-Kontos.
3. Wählen Sie Users (Benutzer) aus.
4. Wählen Sie die Benutzer aus und klicken Sie auf Aktionen, Berechtigungen zuweisen.
5. Wählen Sie eine der folgenden Berechtigungen:

- Profi
- Basic

6. Wählen Sie Assign (Zuweisen).

Enterprise Active Directory- oder Enterprise OpenID Connect (Okta) -Konten

Wenn sich Ihre Benutzer mit Active Directory- oder Okta-Anmeldeinformationen anmelden, verwalten Sie ihre Berechtigungen, indem Sie sie zu Mitgliedern einer Verzeichnisgruppe machen, der Pro- oder Basic-Berechtigungen zugewiesen wurden.

Um einem Benutzer Pro-Berechtigungen zuzuweisen, machen Sie ihn zu einem Mitglied einer Active Directory- oder Okta-Gruppe, der Sie Pro-Berechtigungen zugewiesen haben. Um einem Benutzer Basisberechtigungen zuzuweisen, machen Sie ihn zu einem Mitglied einer Gruppe, der Sie Basisberechtigungen zugewiesen haben. Benutzer, die weder über Pro- noch Basic-Berechtigungen verfügen, können sich nicht bei Amazon Chime anmelden.

Verwalten des Benutzerzugriffs

Wenn Sie ein Amazon Chime Chime-Konto verwalten, können Sie Benutzer einladen, damit sie sich bei Ihrem Konto anmelden können. Administratoren von Unternehmenskonten können den Benutzerzugriff sperren, um sie daran zu hindern, sich bei dem Konto anzumelden.

Benutzer eines Teamkontos einladen und entfernen

Wenn Sie ein Team-Konto verwalten, verwenden Sie die Amazon Chime-Konsole, um Benutzer aus einer beliebigen E-Mail-Domain einzuladen.

> **Note**
>
> Die kostenlose 30-tägige Pro-Testversion eines Benutzers endet, wenn er Ihre Einladung annimmt.

So laden Sie Benutzer zu einem Teamkonto ein

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie für Konten den Namen des Team-Kontos.

3. Wählen Sie „Benutzer“, „Benutzer einladen“.
4. Geben Sie die E-Mail-Adressen der Benutzer ein, die Sie einladen möchten, und trennen Sie mehrere E-Mail-Adressen durch ein Semikolon (). **;**
5. Wählen Sie Invite users.

Mit dem folgenden Verfahren werden Benutzer von Ihrem Teamkonto getrennt, indem alle ihnen zugewiesenen Pro- oder Basic-Berechtigungen entfernt werden. Entfernte Benutzer können sich weiterhin bei Amazon Chime anmelden, sie sind jedoch keine bezahlten Mitglieder Ihres Amazon Chime Chime-Kontos mehr.

So entfernen Sie Benutzer aus einem Teamkonto

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie für Konten den Namen des Team-Kontos.
3. Wählen Sie Users (Benutzer) aus.
4. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie Aktionen, Benutzer entfernen.

Alle Pro- oder Basic-Berechtigungen, die den Benutzern zugewiesen wurden, werden entfernt. Die Benutzer können die automatische Vervollständigung nicht mehr verwenden, um neue Teambenutzer in ihren Kontakten zu finden.

Nutzer eines Enterprise-Kontos einladen und sperren

Wenn Sie ein Enterprise-Konto verwalten, werden alle Benutzer, die sich mit einer E-Mail-Adresse aus Ihren beanspruchten Domains für Amazon Chime registrieren, automatisch zu Ihrem Konto hinzugefügt. Wenn Sie Active Directory oder Okta konfiguriert haben, müssen die Benutzer auch Mitglieder der Verzeichnisgruppe sein, die Sie für Amazon Chime konfiguriert haben.

So laden Sie Benutzer zu einem Enterprise-Konto ein

- Senden Sie eine Einladungs-E-Mail an die Benutzer in Ihrer Organisation und weisen Sie sie an, die Schritte unter Erstellen eines Amazon Chime Chime-Kontos im Amazon Chime Chime-Benutzerhandbuch zu befolgen.

Benutzer melden sich mit einer E-Mail-Adresse von einer der Domains an, die Sie für Ihr Konto beansprucht haben. Nachdem sie die Schritte zur Erstellung ihrer Amazon Chime Chime-

Benutzerkonten abgeschlossen haben, werden sie automatisch in der Amazon Chime Chime-Konsole unter „Benutzer Ihres Unternehmenskontos“ angezeigt.

Mit dem folgenden Verfahren werden Benutzer von einem Enterprise-Konto gesperrt, für das Active Directory oder Okta nicht konfiguriert sind. Dadurch wird verhindert, dass sich die Benutzer bei Amazon Chime anmelden.

So sperren Sie Benutzer für ein Enterprise-Konto.

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie für Konten den Namen des Enterprise-Kontos.
3. Wählen Sie Users (Benutzer) aus.
4. Wählen Sie die Benutzer aus, die gesperrt werden sollen, und wählen Sie Aktionen, Benutzer sperren.
5. Aktivieren Sie das Kontrollkästchen und wählen Sie Sperren.

Wenn Sie Active Directory oder Okta für Ihr Enterprise-Konto konfiguriert haben, gehen Sie wie folgt vor, um Benutzer zu sperren.

So sperren Sie Benutzer für ein Enterprise Active Directory- oder OpenID Connect-Konto (Okta)

- Führen Sie eine der folgenden Aktionen aus:
  - Sperren Sie den Benutzer von Ihrem Active Directory- oder Okta-Administrator-Dashboard aus oder markieren Sie ihn als inaktiv.
  - Entfernen Sie den Benutzer aus jeder Active Directory-Gruppe, der Basic- oder Pro-Berechtigungen zugewiesen wurden.

Ändern der persönlichen Meeting-PINs

Eine persönliche Meeting-PIN ist eine statische ID, die beim Registrieren des Benutzers erstellt wird. Die PIN erleichtert es einem Amazon Chime-Benutzer, Besprechungen mit anderen Amazon Chime Chime-Benutzern zu vereinbaren. Bei Verwendung einer persönlichen Meeting-PIN müssen sich Leiter von Meetings keine Meeting-Details für jedes neue von ihnen geplante Meeting merken.

Wenn ein Benutzer Bedenken hat, dass seine persönliche Meeting-PIN gefährdet sei, können Sie seine PIN zurücksetzen und eine neue ID erstellen. Nachdem Sie eine persönliche Meeting-PIN

aktualisiert haben, muss der Benutzer alle Meetings aktualisieren, die mit der alten persönlichen Meeting-PIN geplant wurden.

So ändern Sie eine persönliche Meeting-PIN

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Konten den Namen des Amazon Chime Chime-Kontos aus.
3. Klicken Sie im Navigationsbereich auf Users (Benutzer).
4. Suchen Sie nach Benutzern, deren PIN geändert werden muss.
5. Um die Seite User detail (Benutzerdetails) zu öffnen, wählen Sie den Namen des Benutzers.
6. Wählen Sie User actions (Benutzeraktionen), Reset personal PIN (PIN zurücksetzen), Confirm (Bestätigen).

Verwalten von Pro-Testversionen

Wenn ein Benutzer eine Einladung des Amazon Chime Teams annimmt oder zu einem Enterprise-Konto hinzugefügt wird, endet seine kostenlose Testversion und er hat Pro-Berechtigungen. Auf diese Weise kann er weiterhin geplante Meetings hosten. Wenn die Berechtigungsstufe des Benutzers in "Basic" geändert wird, wird verhindert, dass er als Meeting-Host agiert.

Bei der nutzungsabhängigen Preisgestaltung von Amazon Chime zahlen Sie nur für Benutzer, die Besprechungen an den Tagen veranstalten, an denen sie sie veranstalten. Meetings-Teilnehmern und Chat-Benutzern entstehen keine Kosten.

Pro-Benutzer werden als Active Pro einstuft, wenn das von ihnen abgehaltene Meeting an einem Kalendertag endete und mindestens eine der folgenden Bedingungen zutrifft:

- Das Meeting war geplant.
- Das Meeting umfasste mehr als zwei Teilnehmer.
- Das Meeting enthielt mindestens ein Aufzeichnungsereignis.
- Das Meeting umfasste einen DFÜ-Teilnehmer.
- Das Meeting umfasste einen Teilnehmer, der mit H.323 oder SIP beitrat.

Weitere Informationen finden Sie unter Preise und Pläne.

Anfordern von Benutzeranhängen

Wenn Sie ein Enterprise-Konto verwalten und über die entsprechenden Berechtigungen verfügen, können Sie die Anlagen, die Ihre Benutzer in Amazon Chime hochladen, anfordern und empfangen. Sie können Anlagen abrufen, die Benutzer in Einzel- und Gruppenkonversationen oder in von ihnen erstellte Chatrooms hochgeladen haben.

> **Note**
>
> Wenn Sie ein Amazon Chime Team-Konto verwalten, können Sie auf ein Enterprise-Konto umsteigen, indem Sie eine oder mehrere Domains beanspruchen. Alternativ können Sie Benutzer aus dem Team-Konto entfernen, sodass diese nicht verwalteten Benutzer ihre Anlagen mit dem Amazon Chime Assistant abrufen können.

So fordern Sie Benutzeranhänge an

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie auf der Seite Konten den Namen des Amazon Chime Chime-Kontos aus.
3. Wählen Sie unter Settings (Einstellungen) die Optionen Account (Konto), Account actions (Kontoaktionen), Request attachments (Anhänge anfordern) aus.
4. Innerhalb von etwa 24 Stunden finden Sie auf der Seite mit der Kontoübersicht einen Link zu einer Datei mit einer Liste der vorsignierten URLs, über die Sie auf jeden Anhang zugreifen.
5. Laden Sie die Datei herunter.

> **Note**
>
> Achten Sie darauf, dass eine entsprechende Ebene der Zugriffskontrolle für die Datei beibehalten wird. Jeder Benutzer, der die Datei erhält, kann die bereitgestellte URL-Liste verwenden, um die verknüpften Anhänge herunterzuladen.
> Vorsignierte URLs laufen nach 6 Tagen ab. Sie können alle 7 Tage eine Anfrage übermitteln.

Um AWS Identity and Access Management (IAM) -Richtlinien zur Verwaltung des Zugriffs auf die Amazon Chime-Verwaltungskonsole und die Aktion Anlagen anfordern zu verwenden, verwenden Sie eine der von Amazon Chime verwalteten Richtlinien (FullAccess, UserManagement, oder).

ReadOnly Alternativ können Sie die benutzerdefinierten Richtlinien aktualisieren, sodass sie die Aktionen `StartDataExport` und `RetrieveDataExport` enthalten. Weitere Informationen zu diesen Aktionen finden Sie unter Von Amazon Chime definierte Aktionen im IAM-Benutzerhandbuch.

So verwaltet Amazon Chime automatische Updates

Amazon Chime bietet verschiedene Möglichkeiten, seine Clients zu aktualisieren. Die Methode variiert, je nachdem, ob Sie Amazon Chime in einem Browser, auf Ihrem Desktop oder auf einem Mobilgerät ausführen.

Die Amazon Chime Chime-Webanwendung — https://app.chime.aws — wird immer mit den neuesten Funktionen und Sicherheitsupdates geladen.

Der Amazon Chime Chime-Desktop-Client sucht immer nach Updates, wenn Sie „Beenden“ oder „Abmelden“ wählen. Dies gilt für Windows- und MacOS-Computer. Während Sie den Client ausführen, sucht er alle drei Stunden nach Updates. Sie können auch nach Updates suchen, indem Sie im Windows-Hilfemenü oder im macOS Amazon Chime-Menü die Option Nach Updates suchen wählen.

Wenn der Desktop-Client ein Update erkennt, fordert Amazon Chime den Benutzer auf, es zu installieren, es sei denn, er befindet sich in einem laufenden Meeting. Sie nehmen an einer laufenden Besprechung teil, wenn:

- Sie nehmen an einer Besprechung teil.
- Sie wurden zu einem Treffen eingeladen, das noch nicht abgeschlossen ist.

Amazon Chime fordert sie auf, die neueste Version zu installieren, und bietet einen 15-Sekunden-Countdown, sodass sie die Installation verschieben können. Benutzer wählen „Später testen“, um das Update zu verschieben.

Wenn Benutzer ein Update verschieben und nicht an einem laufenden Meeting teilnehmen, sucht der Client nach drei Stunden nach dem Update und fordert sie erneut auf, es zu installieren. Die Installation beginnt, wenn der Countdown endet.

> **Note**
>
> Auf einem macOS-Computer müssen Benutzer „Jetzt neu starten“ wählen, um mit dem Update zu beginnen.

Auf Mobilgeräten — Die mobilen Amazon Chime Chime-Anwendungen verwenden die vom App Store und Google Play bereitgestellten Aktualisierungsoptionen, um die neueste Version des Amazon Chime Chime-Clients bereitzustellen. Sie können auch das Verwaltungssystem für mobile Geräte verwenden, um Updates bereitzustellen.

Benutzer zu einem anderen Teamkonto migrieren

Sie migrieren Benutzer zu anderen Teamkonten, indem Sie ein Zielkonto erstellen und konfigurieren, falls noch keines vorhanden ist. Anschließend fügen Sie Benutzer zum Zielkonto hinzu. Die folgenden Schritte führen Sie zu Informationen zum Abschluss der einzelnen Teile einer Migration.

Um Benutzer zu migrieren

1. Wenn Sie kein Ziel-Teamkonto haben, erstellen Sie eines. Weitere Informationen finden Sie unter Schritt 1: Erstellen eines Amazon Chime Chime-Administratorkontos.
2. Konfigurieren Sie das Konto nach Bedarf. Weitere Informationen finden Sie unter Schritt 2 (optional): Konfigurieren von Kontoeinstellungen.
3. Fügen Sie dem Konto Benutzer hinzu. Weitere Informationen finden Sie unter Schritt 3: Hinzufügen von Benutzern zu Ihrem Konto.

Verwaltung von Telefonnummern in Amazon Chime

Sie verwenden die Amazon Chime Chime-Konsole, um Telefonnummern bereitzustellen. Wenn Sie Nummern bereitstellen, fordern Sie diese aus einem von Amazon Chime verwalteten Nummernpool an. Wenn Sie die Zuweisung von Nummern aufheben und sie anschließend löschen, kehren sie in den Pool zurück. Wenn Sie Nummern portieren, portieren Sie sie in und aus Amazon Chime.

> **Note**
>
> Wenn Sie die Amazon Chime-Konsole verwenden, können Sie nur Amazon Chime Business Calling-Nummern bereitstellen. Wenn Sie internationale Nummern benötigen, verwenden Sie Amazon Chime Voice Connectors und SIP-Medienanwendungen. Dazu müssen Sie zunächst ein Amazon Chime SDK-Administratorkonto erstellen. Weitere Informationen finden Sie in den folgenden Themen im Amazon Chime SDK-Administratorhandbuch:
>
> - Voraussetzungen
> - Verwaltung des Telefonnummernbestands
> - Verwaltung von Voice Connectors
> - Verwaltung von SIP-Medienanwendungen

In den Themen der folgenden Abschnitte wird erklärt, wie Sie Amazon Chime Chime-Telefonnummern bereitstellen und verwalten.

Inhalt

Bereitstellen von Telefonnummern

Verwenden Sie die Amazon Chime Chime-Konsole, um Telefonnummern für Ihr Amazon Chime Chime-Konto bereitzustellen. Die Zahlen stammen aus einem Pool, der von Amazon Chime verwaltet wird. Wählen Sie Amazon Chime Business Calling, um Ihren bestehenden Amazon Chime Chime-Benutzern Telefonnummern bereitzustellen und zuzuweisen.

Wenn die Bereitstellung abgeschlossen ist, werden die Telefonnummern in Ihrem Inventar angezeigt. Anschließend weisen Sie sie einzelnen Benutzern zu.

So stellen Sie Telefonnummern bereit

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie Orders (Beantragungen), Provision phone numbers (Telefonnummern bereitstellen).
4. Wählen Sie Geschäftliche Anrufe und dann Weiter aus.
5. Suchen Sie nach verfügbaren Telefonnummern. Wählen Sie die gewünschten Telefonnummern aus und klicken Sie dann auf Provision (Bereitstellen).

Die Telefonnummern werden während der Bereitstellung in Ihren Listen „Bestellungen“ und „Ausstehende Bestellungen“ angezeigt.

Portieren von Telefonnummern

Neben der Bereitstellung von Telefonnummern können Sie auch Nummern Ihres Telefonanbieters in Ihr Inventar übernehmen. Dazu gehören auch gebührenfreie Nummern.

> **Note**
>
> Wenn Sie internationale Nummern portieren, Amazon Chime Voice Connectors verwenden oder SIP-Medienanwendungen verwenden müssen, müssen Sie ein Amazon Chime SDK-Administratorkonto erstellen und die Amazon Chime SDK-Konsole verwenden. Weitere Informationen dazu finden Sie unter Voraussetzungen im Amazon Chime SDK-Administratorhandbuch.

In den folgenden Abschnitten wird erklärt, wie Telefonnummern portiert werden.

Themen

Voraussetzungen für die Portierung von Nummern

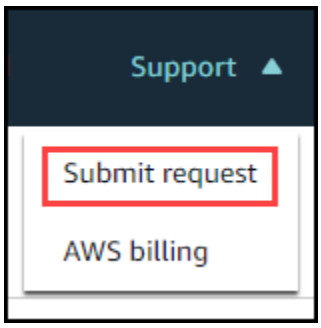
Um Nummern zu portieren, benötigen Sie einen Letter of Agency (LOA). Sie benötigen eine LOA für inländische Telefonnummern. Laden Sie das Formular Letter of Agency (LOA) herunter und füllen Sie es aus. Wenn Sie Telefonnummern verschiedener Netzbetreiber portieren müssen, füllen Sie für jeden Mobilfunkanbieter eine separate LOA aus.

Portierung von Telefonnummern in

Sie erstellen eine Support-Anfrage, um bestehende Telefonnummern zu portieren.

So portieren Sie Telefonnummern

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie in der Befehlsleiste oben auf der Seite Support und anschließend Anfrage einreichen aus.



   Dadurch gelangen Sie zur AWS Support-Konsole.

> **Note**
>
> Sie können auch direkt zur AWS Support Center-Seite wechseln. Wählen Sie in diesem Fall „Kundenvorgang erstellen“ und gehen Sie dann wie folgt vor.

3. Gehen Sie unter Wie können wir helfen wie folgt vor:

   a. Wählen Sie Konto und Fakturierung aus.

   b. Wählen Sie in der Serviceliste Chime SDK (Number Management) aus.

   c. Wählen Sie in der Kategorienliste die Option Phone Number Port In aus.

   d. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).

4. Gehen Sie unter Zusätzliche Informationen wie folgt vor

   a. Geben Sie unter Betreff ein**`Porting phone numbers in`**.

   b. Geben Sie unter Beschreibung die folgenden Informationen ein:

      Für die Portierung von US-Nummern:

      - Fakturierungstelefonnummer (BTN) des Kontos.
      - Name der autorisierenden Person. Dies ist die Person, die für die Kontofakturierung beim aktuellen Anbieter zuständig ist.
      - Aktueller Anbieter, falls bekannt.
      - Servicekonto-Nummer, wenn diese Informationen beim aktuellen Anbieter vorhanden sind.
      - Service-PIN, falls verfügbar.
      - Service-Adresse und Kundenname, wie in Ihrem aktuellen Anbietervertrag aufgeführt.
      - Angefordertes Datum und Uhrzeit für die Portierung.
      - (Optional) Wenn Sie Ihre Abrechnungstelefonnummer (BTN) portieren möchten, wählen Sie eine der folgenden Optionen aus:
        - Ich portiere mein BTN und möchte es durch ein neues BTN ersetzen, das ich zur Verfügung stelle. Ich kann bestätigen, dass sich diese neue BTN auf demselben Konto wie der aktuelle Mobilfunkanbieter befindet.
        - Ich portiere meine BTN und möchte mein Konto bei meinem aktuellen Netzbetreiber schließen.

- Ich portiere meine BTN, weil mein Konto derzeit so eingerichtet ist, dass jede Telefonnummer ihre eigene BTN ist. (Wählen Sie diese Option nur aus, wenn Ihr Konto beim aktuellen Netzbetreiber auf diese Weise eingerichtet ist.)
- Nachdem Sie eine Option ausgewählt haben, fügen Sie der Anfrage Ihr Letter of Agency (LOA) bei.

Für die Portierung internationaler Nummern:

- Für Telefonnummern außerhalb der USA müssen Sie den Produkttyp SIP Media Application Dial-In verwenden.
- Art der Nummer (lokal oder gebührenfrei)
- Vorhandene Telefonnummern zum Portieren.
- Schätzen Sie das Nutzungsvolumen ein
- Land

c. Wählen Sie in der Liste Telefonnummerntyp die Option Business Calling, SIP Media Application Dial-In oder Voice Connector aus.

d. Geben Sie unter Telefonnummer mindestens eine Telefonnummer ein, auch wenn Sie mehrere Nummern portieren.

e. Geben Sie unter Portierungsdatum das gewünschte Portierungsdatum ein.

f. Geben Sie unter Portierungszeit die gewünschte Uhrzeit ein.

g. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).

5. Wählen Sie unter Jetzt lösen oder kontaktieren Sie uns die Option Kontaktieren Sie uns aus.
6. Wählen Sie aus der Liste Bevorzugte Kontaktsprache eine Sprache aus
7. Wählen Sie Web oder Telefon. Wenn Sie Telefon wählen, geben Sie Ihre Telefonnummer ein. Wenn Sie fertig sind, wählen Sie Senden.

AWS Support informiert Sie darüber, ob Ihre Telefonnummern von Ihrem bestehenden Mobilfunkanbieter portiert werden können. Wenn Sie können, müssen Sie alle erforderlichen Dokumente einreichen. In den Schritten im nächsten Abschnitt wird erklärt, wie Sie diese Dokumente einreichen.

Einreichen der erforderlichen Dokumente

Nachdem der AWS Support mitgeteilt hat, dass Sie Telefonnummern portieren können, müssen Sie alle erforderlichen Dokumente einreichen. In den folgenden Schritten wird erklärt, wie das geht.

> **Note**
>
> AWS Der Support bietet einen sicheren Amazon S3 S3-Link zum Hochladen aller angeforderten Dokumente. Fahren Sie erst fort, wenn Sie den Link erhalten haben.

Um Dokumente einzureichen

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Melden Sie sich bei Ihrem AWS Konto an und öffnen Sie dann den Amazon S3 S3-Upload-Link, der speziell für Ihr Konto generiert wurde.

   > **Note**
   >
   > Der Link läuft nach zehn Tagen ab. Er wurde speziell für das Konto generiert, das den Fall erstellt hat. Für den Link ist ein autorisierter Benutzer aus dem Konto erforderlich, um den Upload durchzuführen.

3. Wählen Sie Dateien hinzufügen und wählen Sie dann die Ausweisdokumente aus, die sich auf Ihre Anfrage beziehen.
4. Erweitern Sie den Bereich „Berechtigungen“ und wählen Sie „Individuelle ACL-Berechtigungen angeben“ aus.
5. Wählen Sie am Ende des Abschnitts Zugriffskontrollliste (ACL) die Option Empfänger hinzufügen aus und fügen Sie dann den vom AWS Support bereitgestellten Schlüssel in das Feld Empfänger ein.
6. Wählen Sie unter Objekte das Kontrollkästchen „Lesen“ und anschließend „Hochladen“ aus.

Nachdem Sie den Letter of Agency (LOA) vorgelegt haben, AWS Support bestätigen Sie mit Ihrem bestehenden Mobilfunkanbieter, dass die Informationen auf der LOA korrekt sind. Wenn die in dem LOA bereitgestellten Informationen nicht mit den Informationen übereinstimmen, die Ihrem Telefonnetzbetreiber vorliegen, nimmt AWS Support zu Ihnen auf, um die in dem LOA bereitgestellten Informationen zu aktualisieren.

Status der Anfrage wird angezeigt

In den folgenden Schritten wird erklärt, wie Sie die Amazon Chime Chime-Konsole verwenden, um den Status Ihrer Portierungsanfragen einzusehen.

Um den Status einzusehen

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich die Option Telefonnummernverwaltung aus.
3. Wählen Sie den Tab Bestellungen.

In der Spalte Status wird der Status Ihrer Anfrage angezeigt. AWS Support kontaktiert Sie bei Bedarf auch mit Updates und Anfragen nach weiteren Informationen. Weitere Informationen finden Sie unter Definitionen des Portierungsstatus für Telefonnummern, weiter unten in diesem Abschnitt.

Zuweisung von portierten Nummern

Nachdem Ihr Mobilfunkanbieter bestätigt hat, dass die LOA korrekt ist, überprüft und genehmigt er den angeforderten Port. Anschließend teilen sie das Datum und die Uhrzeit des Portierens AWS Support mit (Firm Order Commit, FOC).

Am FOC-Datum werden die portierten Telefonnummern für die Verwendung aktiviert. Anschließend müssen Sie die Nummern Benutzern im gewünschten Konto zuweisen.

Um Telefonnummern zuzuweisen

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich die Option Telefonnummernverwaltung aus.
3. Aktivieren Sie auf der Registerkarte Inventar das Kontrollkästchen neben der Nummer, die Sie zuweisen möchten, und wählen Sie dann Zuweisen aus.

   > **Note**
   >
   > Sie können jeweils nur eine Nummer auswählen.

4. Wählen Sie auf der Seite „+1-Telefonnummer einem Benutzerprofil zuweisen“ das Konto für die Nummer aus und klicken Sie dann auf Weiter.

5. Wählen Sie den Benutzer aus, dem Sie die Nummer zuweisen möchten, und wählen Sie dann Zuweisen.

Rufnummern herausnehmen

Sie portieren Nummern aus Amazon Chime, indem Sie eine Portierungsanfrage bei Ihrem erfolgreichen Mobilfunkanbieter stellen. Wenn Sie Informationen an Ihren erfolgreichen Mobilfunkanbieter senden, geben Sie Ihre AWS Konto-ID als Konto-ID an, die mit der portierten Telefonnummer verknüpft ist.

Wenn der Portierungsprozess abgeschlossen ist und der Mobilfunkanbieter, der den Zuschlag erhalten hat, die Nummern hat, müssen Sie die Zuweisung der Nummern aufheben und sie aus Ihrem Inventar löschen. Weitere Informationen finden Sie unter Aufheben der Zuweisung von Amazon Chime Business Calling-Telefonnummern und Löschen von Telefonnummern in diesem Handbuch.

⚠ Important

- Die Fähigkeit, Nummern zu übertragen, hängt davon ab, ob die Fluggesellschaft, die den Zuschlag erhalten hat, diese Nummern akzeptieren kann.
- Die Überprüfung der Echtheit der Port-Out-Anfrage des Gewinners ist für die Sicherheit Ihrer Telefonnummer von entscheidender Bedeutung. Wenn die Kontodaten nicht korrekt sind (z. B. weil die Konto-ID nicht übereinstimmt), kann es sein, dass Ihr Antrag auf Abmeldung abgelehnt wird, was zu Verzögerungen führt und Sie Ihre Anfrage erneut einreichen müssen.

(Optional) Wie fordere ich eine PIN an, um deine Nummer zu schützen

Für zusätzliche Sicherheit können Sie uns kontaktieren, um eine PIN auf Ihre Nummer anzuwenden. Der Mobilfunkanbieter, der den Zuschlag erhält, verwendet dann diese PIN. Dazu gehen Sie wie folgt vor:

Um eine PIN anzufordern

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Kontakt die Option Support aus.

Dadurch gelangen Sie zur AWS Support-Konsole.

> **Note**
>
> Sie können auch direkt zur AWS Support Center-Seite wechseln. Wählen Sie in diesem Fall „Kundenvorgang erstellen“ und gehen Sie dann wie folgt vor.

3. Gehen Sie unter Wie können wir helfen wie folgt vor:
   a. Wählen Sie Konto und Fakturierung aus.
   b. Wählen Sie in der Serviceliste Chime SDK (Number Management) aus.
   c. Wählen Sie in der Kategorienliste die Option Phone Number Port Out aus.
   d. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
4. Gehen Sie unter Zusätzliche Informationen wie folgt vor
   a. Geben Sie unter Betreff ein**`Porting phone numbers out`**.
   b. Geben Sie unter Beschreibung Folgendes ein.

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

      > **Note**
      >
      > Sie müssen eine alphanumerische PIN mit 4 bis 10 Zeichen angeben.

AWS Der Support ordnet der Telefonnummer eine PIN zu. Wenn Sie den Port bei Ihrem Mobilfunkanbieter anfragen, geben Sie Ihre AWS Konto-ID und PIN an. Wir werden diese Informationen verwenden, um alle für Ihre Nummer eingegangenen Portanfragen zu validieren.

Definitionen des Portierungsstatus für Telefonnummern

Nachdem Sie eine Anfrage zur Portierung vorhandener Telefonnummern in Amazon Chime eingereicht haben, können Sie den Status Ihrer Portierungsanfrage in der Amazon Chime Chime-Konsole unter Anrufen, Telefonnummernverwaltung, Ausstehend einsehen.

Zu den Portierungsstatus und -definitionen gehören die folgenden:

CANCELLED

AWS Support hat den Portierungsauftrag aufgrund eines Problems mit dem Port storniert, z. B. aufgrund einer Stornierungsanfrage vom Mobilfunkanbieter oder von Ihnen. AWS Support kontaktiert Sie mit Einzelheiten.

CANCEL_REQUESTED

AWS Support bearbeitet eine Stornierung des Portierungsauftrags aufgrund eines Problems mit dem Hafen, z. B. einer Stornierungsanfrage von der Fluggesellschaft oder von Ihnen. AWS Support kontaktiert Sie mit Einzelheiten.

CHANGE_REQUESTED

AWS Support bearbeitet Ihre Änderungsanfrage und die Antwort des Transporteurs steht noch aus. Planen Sie zusätzliche Bearbeitungszeit ein.

COMPLETED

Ihr Portierungsauftrag ist abgeschlossen und Ihre Telefonnummern sind aktiviert.

EXCEPTION

AWS Support kontaktiert Sie, um weitere Informationen zu erhalten, die für die Bearbeitung der Portanfrage erforderlich sind. Planen Sie zusätzliche Bearbeitungszeit ein.

Verbindliche Auftragszusage (FOC)

Das FOC-Datum wird vom Spediteur bestätigt. AWS Support kontaktiert Sie, um das Datum zu bestätigen.

PENDING DOCUMENTS

AWS Support kontaktiert Sie, um weitere Dokumente zu erhalten, die für die Bearbeitung der Portanfrage erforderlich sind. Planen Sie zusätzliche Bearbeitungszeit ein.

SUBMITTED

Ihr Portierungsauftrag wurde übermittelt und die Antwort des Transporteurs steht noch aus.

Zuweisen von Amazon Chime Business Calling-Telefonnummern

Verwenden Sie die Inventarseite für die Verwaltung von Telefonnummern, um einzelnen Benutzern Amazon Chime Business Calling-Telefonnummern zuzuweisen.

So weisen Sie Amazon Chime Business Calling-Telefonnummern zu

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie zuweisen möchten.
4. Wählen Sie Assign (Zuweisen).
5. Wählen Sie das Konto aus, zu dem der Benutzer gehört, und klicken Sie dann auf Weiter.
6. Wählen Sie den Benutzer aus und klicken Sie dann auf Zuweisen.

Wenn du eine Telefonnummer oder die Rufnummernberechtigungen änderst, empfehlen wir, dem Benutzer seine neuen Informationen oder seine Berechtigungsinformationen zur Verfügung zu stellen. Bevor Benutzer auf ihre neuen Telefonnummern- oder Berechtigungsfunktionen zugreifen können, müssen sie sich von ihrem Amazon Chime Chime-Konto abmelden und erneut anmelden.

Aufheben der Zuweisung von Amazon Chime Business Calling-Telefonnummern

Mit dem folgenden Verfahren wird die Zuweisung von Telefonnummern von Amazon Chime Business Calling-Benutzern aufgehoben.

Um die Zuweisung von Telefonnummern aufzuheben

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, deren Zuweisung Sie aufheben möchten.
4. Wählen Sie Unassign (Zuweisung aufheben) aus.
5. Aktivieren Sie das Kontrollkästchen und wählen Sie Unassign (Zuweisung aufheben) aus.

Sie können die Details für die Nummern in Ihrem Inventar einsehen. Sie können beispielsweise sehen, ob Telefonanrufe und Textnachrichten aktiviert sind.

So zeigen Sie Details zu Telefonnummern im Verzeichnis an

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie den Tab Inventar und dann die Telefonnummer aus, die Sie sich ansehen möchten.
4. Öffnen Sie die Aktionsliste und wählen Sie Details anzeigen aus.

Namen für ausgehende Anrufe verwenden

Namen ausgehender Anrufe dienen als Anruferkennungen. Sie können einen Standardanrufnamen für eine oder mehrere Telefonnummern in Ihrem Inventar festlegen. Sie können auch eindeutige Rufnamen für einzelne Telefonnummern festlegen. Die Namen werden dann den Empfängern von ausgehenden Anrufen angezeigt, die mit diesen Telefonnummern getätigt wurden. Anrufenamen gelten für alle Produkttypen von Telefonnummern. Sie können die Namen alle sieben Tage aktualisieren.

Sie können beispielsweise den Standardanrufnamen Abteilung 5 für alle Telefonnummern in dieser Abteilung festlegen. Sie können auch den eindeutigen Namen Jane Doe für die Abteilungsleiterin festlegen.

In den folgenden Schritten wird erklärt, wie Sie Standard- und individuelle Namen für ausgehende Anrufe festlegen.

So legen Sie einen Anrufenamen fest

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Führen Sie auf der Registerkarte Inventar einen der folgenden Schritte aus: Aktivieren Sie die Kontrollkästchen neben den Telefonnummern, die Sie aktualisieren möchten.
   - Um einen Standardanrufnamen für mehrere Nummern festzulegen, aktivieren Sie die Kontrollkästchen neben diesen Nummern.
   - Um einen individuellen Rufnamen festzulegen, wählen Sie die gewünschte Nummer aus.
4. Öffnen Sie die Aktionsliste und wählen Sie Standardanrufnamen aktualisieren.

5. Geben Sie im Feld Standardanrufname einen Namen mit bis zu 15 Zeichen ein.
6. Wählen Sie Speichern.

Warten Sie 72 Stunden, bis das System den Standardanrufnamen aktualisiert hat.

Löschen von Telefonnummern

> **Important**
>
> Nur Amazon Chime Chime-Systemadministratoren können diese Schritte ausführen. Außerdem müssen Sie die Zuweisung von Telefonnummern aufheben, bevor Sie sie löschen können.

Wenn Sie eine Telefonnummer angeben, bestellen Sie sie aus einem Nummernpool, den Amazon Chime verwaltet. Wenn Sie eine Nummer löschen, wird sie wieder in den Pool verschoben. Wenn Sie eine Nummer löschen, wird sie zunächst in Ihre Löschwarteschlange verschoben, wo sie 7 Tage lang aufbewahrt wird. Während dieser Zeit kannst du die Nummer wieder in dein Inventar verschieben. Nach 7 Tagen löscht das System die Nummer automatisch aus der Warteschlange und trennt sie von Ihrem Konto. Dadurch wird die Nummer wieder in den Nummernpool aufgenommen. Wenn Sie eine Nummer zurückfordern müssen, nachdem das System sie aus der Warteschleife gelöscht hat, folgen Sie den Schritten unter. Beachten Sie jedochBereitstellen von Telefonnummern, dass die Nummer möglicherweise nicht verfügbar ist.

So löschen Sie nicht zugewiesene Telefonnummern

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie den Tab Inventar und dann die Telefonnummer (n) aus, die Sie löschen möchten.
4. Öffne die Aktionsliste und wähle Telefonnummer (n) löschen aus.
5. Markieren Sie das Kontrollkästchen und wählen Sie dann Löschen.

Gelöschte Telefonnummern werden 7 Tage lang in der Löschwarteschlange aufbewahrt, bevor sie dauerhaft aus Ihrem Inventar gelöscht werden.

Wiederherstellen gelöschter Telefonnummern

Sie können gelöschte Telefonnummern bis zu 7 Tage lang aus der Löschwarteschlange wiederherstellen, nachdem Sie sie gelöscht haben. Durch das Wiederherstellen wird die Telefonnummer wieder in das Inventory (Verzeichnis) verschoben.

So stellen Sie gelöschte Telefonnummern wieder her

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie im Navigationsbereich unter Telefonieren die Option Telefonnummernverwaltung aus.
3. Wählen Sie die Registerkarte Löschwarteschlange und wählen Sie dann die Telefonnummer (n) aus, die Sie wiederherstellen möchten.
4. Wählen Sie Move to inventory (In Verzeichnis verschieben) aus.

Verwaltung globaler Einstellungen in Amazon Chime

Sie verwenden die Amazon Chime-Konsole, um die Einstellungen für Anrufdetailaufzeichnungen zu verwalten.

Konfigurieren von Anrufdetaildatensätzen

Bevor Sie die Einstellungen für Anrufdetailaufzeichnungen für Ihr Amazon Chime Chime-Administratorkonto konfigurieren können, müssen Sie zunächst einen Amazon Simple Storage Service-Bucket erstellen. Der Amazon S3 S3-Bucket wird als Protokollziel für Ihre Anrufdetail-Datensätze verwendet. Wenn Sie Ihre Anrufdetailaufzeichnungseinstellungen konfigurieren, gewähren Sie Amazon Chime Lese- und Schreibzugriff auf den Amazon S3 S3-Bucket, um Ihre Daten zu speichern und zu verwalten. Weitere Informationen zum Erstellen eines Amazon S3 S3-Buckets finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Amazon Simple Storage Service-Benutzerhandbuch.

Sie können die Einstellungen für Anrufdetailaufzeichnungen für Amazon Chime Business Calling konfigurieren. Weitere Informationen über Amazon Chime Business Calling finden Sie unterVerwaltung von Telefonnummern in Amazon Chime.

So konfigurieren Sie Anrufdetaildatensatz-Einstellungen

1. Erstellen Sie einen Amazon S3 S3-Bucket, indem Sie den Schritten unter Erste Schritte mit Amazon Simple Storage Service im Amazon Simple Storage Service-Benutzerhandbuch folgen.
2. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
3. Wählen Sie unter Global Settings (Globale Einstellungen) die Option Call detail records (Anrufdetaildatensätze) aus.
4. Wählen Sie Business Calling Configuration.
5. Wählen Sie unter Log-Ziel den Amazon S3 S3-Bucket aus.
6. Wählen Sie Speichern.

Sie können die Protokollierung von Anrufdetaildatensätzen jederzeit beenden.

So beenden Sie die Protokollierung von Anrufdetaildatensätzen

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.

2. Wählen Sie unter Global Settings (Globale Einstellungen) die Option Call detail records (Anrufdetaildatensätze) aus.
3. Wählen Sie Disable logging (Protokollierung deaktivieren) für die entsprechende Konfiguration aus.

Amazon Chime Business Calling — detaillierte Aufzeichnungen zum Telefonieren

Wenn Sie sich für den Empfang von Anrufdetailaufzeichnungen für Amazon Chime Business Calling entscheiden, werden diese an Ihren Amazon S3 S3-Bucket gesendet. Das folgende Beispiel zeigt das allgemeine Format eines Amazon Chime Business Calling-Anrufdetaildatensatzes.

```
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
```

Das folgende Beispiel zeigt die Daten, die im Namen des Anrufdetaildatensatzes dargestellt werden.

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

Das folgende Beispiel zeigt das allgemeine Format eines Amazon Chime Business Calling-Anrufdetaildatensatzes.

```
{
    "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"
}
```

Konferenzraumkonfiguration

Amazon Chime kann in Ihre Videohardware von Cisco, Tandberg, Polycom, Lifesize, Vidyo oder anderen im Zimmer integriert werden, wenn Sie das SIP- oder H.323-Protokoll verwenden.

Um über ein VTC-Gerät im Konferenzraum, das SIP unterstützt, eine Verbindung zu Amazon Chime herzustellen, geben Sie eine der folgenden Optionen ein:

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- 10-stellige Meeting-ID, gefolgt von **`@meet.chime.in`**

`meet.chime.in`verbindet Ihr SIP-Room-Gerät mit der nächstgelegenen Amazon Chime Chime-Region. Verwenden Sie regionsspezifische DNS-Einträge für SIP-Raumsysteme für die Herstellung einer Verbindung mit einer bestimmten Region. Weitere Informationen finden Sie unter Session Initiation Protocol (SIP)-Raumsysteme.

> **Note**
>
> Wenn Ihr SIP-Raumgerät kein TLS unterstützt und TCP-Konnektivität erfordert, wenden Sie sich an den AWS-Support.

Bei Verwendung eines Geräts, das nur H.323 unterstützt, müssen Sie eine der folgenden Optionen wählen:

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

Wenn eine Firewall den Datenverkehr zwischen dem VTC-Gerät und Amazon Chime filtert, öffnen Sie die Bereiche für die verwendeten Protokolle. Weitere Informationen finden Sie unter Netzwerkkonfiguration und Bandbreiten-Anforderungen.

Geben Sie auf dem Amazon Chime Chime-Willkommensbildschirm die 10-stellige oder 13-stellige Meeting-ID ein, um teilzunehmen. Sie finden die 13-stellige Meeting-ID im Amazon Chime Chime-Client oder in der Web-App oder wählen Sie die Einwahloption.

Beitreten zu einem moderierten Meeting

Wenn es sich um ein moderiertes Meeting handelt und Sie der Gastgeber oder dessen Stellvertreter sind, geben Sie die 13-stellige Meeting-ID ein, um dem Meeting als Moderator beizutreten. Wenn Sie Moderator sind, geben Sie den Moderator-Passcode mit dem Tastenfeld und dann das Rautezeichen (#) ein, um dem Meeting beizutreten und es zu starten. Wenn Sie kein Gastgeber, dessen Stellvertreter oder Moderator sind, werden Sie mit dem Meeting verbunden, sobald ein Moderator dem Meeting beitritt und es startet.

Moderatoren verfügen über Steuerelemente für Gastgeber, sie können also zusätzliche Meeting-Funktionen ausführen. Zu diesen Aktionen gehören das Starten und Beenden der Aufzeichnung, das Sperren und Entsperren des Meetings, das Stummschalten aller anderen Teilnehmer und das Beenden des Meetings. Weitere Informationen finden Sie im Amazon Chime Chime-Benutzerhandbuch unter Moderatorenaktionen mithilfe von Telefon- oder Videosystemen im Zimmer.

> **Note**
>
> Wenn Sie Alexa for Business verwenden, um an Ihren Amazon Chime Chime-Besprechungen teilzunehmen, können Sie nur dann als Moderator teilnehmen, wenn Ihr Gerät an ein Videosystem im Zimmer angeschlossen ist und Sie sich über die Wähltastatur des Geräts einwählen.

Kompatible VTC-Geräte

Die folgende Tabelle ist ein Teilsatz der Liste kompatibler VTC-Geräte.

Gerät	SIP	H.323	Kommentar
Cisco SX20	Ja	Ja	Audio/Video/ Bildschirm: beide Richtungen OK
Cisco DX80	Ja	Ja	Audio/Video/ Bildschirm: beide Richtungen OK

Gerät	SIP	H.323	Kommentar
Symbol "LifeSize"	Ja	Nein	Audio/Video/ Bildschirm: beide Richtungen OK
Polycom Debut	Ja	Ja	Audio/Video/ Bildschirm: beide Richtungen OK
Polycom RealPresence Desktop	Nein	Ja	Audio/Video: OK, Bildschirm: Vom Gerät OK
Polycom Trio	Ja	Ja	Audio/Video/ Bildschirm: beide Richtungen OK
Tandberg C40	Ja	Ja	Audio/Video/ Bildschirm: beide Richtungen OK

Netzwerkkonfiguration und Bandbreiten-Anforderungen

Amazon Chime benötigt die in diesem Thema beschriebenen Ziele und Ports, um verschiedene Dienste zu unterstützen. Wenn ein- oder ausgehender Datenverkehr blockiert ist, kann sich dies auf die Möglichkeit der Verwendung verschiedener Services einschließlich Audio, Video, Bildschirmfreigabe oder Chat auswirken.

Amazon Chime verwendet Amazon Elastic Compute Cloud (Amazon EC2) und andere AWS-Services auf Port TCP/443. Wenn Ihre Firewall Port TCP/443 blockiert, müssen Sie `*.amazonaws.com` auf eine Freigabeliste setzen oder IP-Adressbereiche für AWS für die folgenden Services in die Allgemeine AWS-Referenz einfügen:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Erweitern Sie die folgenden Abschnitte, um weitere Informationen zu Zielen, Ports und Bandbreite zu erhalten.

Erforderliche Ziele und Ports

Die folgenden Ziele und Ports sind für die Ausführung von Amazon Chime erforderlich.

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

Anschluss für Besprechung und Telefonie

Amazon Chime verwendet das folgende Ziel und den folgenden Port für Besprechungen und Amazon Chime Business Calling.

Bestimmungsort	Port
99.77.128.0/18	UDP/3478

H.323-Raumsysteme

Amazon Chime verwendet die folgenden Ziele und Anschlüsse für H.323-Videosysteme in Räumen.

Bestimmungsort	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	

Session Initiation Protocol (SIP)-Raumsysteme

Die folgenden Ziele und Ports werden empfohlen, wenn Sie Amazon Chime für SIP-Raumvideosysteme in Ihrer Umgebung ausführen.

AWS Region	Bestimmungsort	Ports
Global (nächste Region)	99.77.128.0/18	UDP/10000:60000

AWS Region	Bestimmungsort	Ports
	34.212.95.128/25 34.223.21.0/25 52.55.62.128/25 52.55.63.0/25	
Global	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
USA Ost (Nord-Virginia)	meet.ue1.chime.in	TCP/5061
USA West (Oregon)	meet.uw2.chime.in	TCP/5061
Asien-Pazifik (Singapur)	meet.as1.chime.in	TCP/5061
Asien-Pazifik (Sydney)	meet.as2.chime.in	TCP/5061
Asien-Pazifik (Tokio)	meet.an1.chime.in	TCP/5061
Europa (Irland)	meet.ew1.chime.in	TCP/5061
Südamerika (São Paulo)	meet.se1.chime.in	TCP/5061

Anforderungen an die Bandbreite

Amazon Chime hat die folgenden Bandbreitenanforderungen für Audio-, Video- und Screen-Sharing:

- Audio
  - Direktgespräch: 54 Kbit/s nach oben und nach unten
  - Gruppengespräch: nicht mehr als 32 Kbit/s extra nach unten für 50 Anrufer
- Video
  - Direktgespräch: 650 Kbit/s nach oben und nach unten

  - HD-Modus: 1400 Kbit/s nach oben und nach unten
  - 3–4 Personen: 450 Kbit/s nach oben und (N-1)*400 Kbit/s nach unten
  - 5–16 Personen: 184 Kbit/s nach oben und (N-1)*134 Kbit/s nach unten
  - Die Bandbreite für beide Richtungen wird je nach Netzwerkbedingungen nach unten angepasst
- Screen-Sharing
  - 1,2 Mbit/s nach oben (beim Präsentieren) und nach unten (beim Betrachten) für hohe Qualität. Dies passt sich bis zu 320 Kbit/s an, je nach Netzwerkbedingungen.
  - Remote-Kontrolle: 800 Kbit/s fest

Anzeigen von Berichten

Um leichter fundierte Entscheidungen zu treffen und die Produktivität für Ihre Organisation zu steigern, können Sie auf Nutzungs- und Feedback für Ihre Konsole zugreifen. Berichtsdaten werden täglich aktualisiert. Es kann jedoch eine Verzögerung von bis zu 48 Stunden auftreten.

So zeigen Sie Nutzungs- und Feedback-Berichte an

1. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
2. Wählen Sie Reports (Berichte), Dashboard.
3. Klicken Sie auf der Seite Usage and feedback dashboard report (Nutzungs- und Feedback-Dashboard-Bericht) auf die folgenden Daten:

> **Note**
>
> Weitere Informationen zu den verfügbaren Daten finden Sie unter Amazon Chime Report Dashboard and User Activity details.

- Datumsbereich (UTC) — Der Datumsbereich des Berichts.
- Registrierte Benutzer — Die Anzahl der Benutzer, die sich für Amazon Chime angemeldet haben.
- Aktive Benutzer — Die Anzahl der Benutzer, die entweder an einer Besprechung teilgenommen oder eine Nachricht mit Amazon Chime gesendet haben.
- Abgehaltene Besprechungen — Die Gesamtzahl der beendeten Besprechungen. Sie können eine bestimmtes Meeting auswählen, um Details anzuzeigen. Dazu gehören Konferenz-ID, Startzeit, Typ, Leiter, Dauer und Anzahl der Teilnehmer. Wählen Sie einen bestimmten Wert für Conference ID (Konferenz-ID) oder Meeting organizer (Leiter des Meetings) aus, weitere Details anzuzeigen. Dazu gehören Teilnehmer, Meeting-Teilnehmerlisten-Ereignisse, Client-Typ und Meeting-Feedback.
- Zufriedenheit mit Besprechungen — Der Prozentsatz der positiven Antworten auf die end-of-meeting Umfrage.
- Gesendete Chat-Nachrichten — Die Anzahl der Chat-Nachrichten, die Benutzer gesendet haben.

Erweiterung des Amazon Chime Chime-Desktop-Clients

Sie können die Funktionen des Amazon Chime Chime-Desktop-Clients erweitern, indem Sie Chat-Bots, Proxy-Telefonsitzungen und Webhooks hinzufügen. Chat-Bots ermöglichen es Benutzern, Aufgaben wie das Abfragen interner Systeme nach Informationen auszuführen. Proxy-Telefonsitzungen ermöglichen es Benutzern, anzurufen und Texte zu senden, ohne ihre Telefonnummern preiszugeben. Webhooks können automatisch Nachrichten an Chatrooms senden. Ein Webhook kann beispielsweise Besprechungserinnerungen zusammen mit einem Link zum Meeting an ein Team senden.

Themen

Benutzerverwaltung

Die folgenden Codefragmente können Ihnen bei der Verwaltung von Amazon Chime Chime-Benutzern helfen. Alle Beispiele in diesem Thema verwenden Java.

Themen

Laden Sie mehrere Benutzer ein

Das folgende Beispiel zeigt, wie Sie mehrere Benutzer zu einem Amazon Chime `Team` Chime-Konto einladen.

```
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);
```

Benutzerlisten werden heruntergeladen

Das folgende Beispiel zeigt, wie Sie eine Liste von Benutzern, die mit Ihrem Amazon Chime Chime-Administratorkonto verknüpft sind, im `.csv` Format herunterladen.

```
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();
```

Melden Sie mehrere Benutzer ab

Das folgende Beispiel zeigt, wie Sie mehrere Benutzer von Ihrem Amazon Chime Chime-Administratorkonto abmelden.

```
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);
}
```

Aktualisieren Sie die persönlichen PINs von Benutzern

Das folgende Beispiel zeigt, wie die persönliche Meeting-PIN für einen bestimmten Amazon Chime Chime-Benutzer zurückgesetzt wird.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

Integration von Chatbots in den Amazon Chime Desktop-Client

Sie können dasAWS Command Line Interface(AWS CLI), Amazon Chime API oderAWSSDK zur Integration von Chatbots in Amazon Chime. Mit Chatbots können Sie die Leistung von Amazon Lex nutzen,AWS Lambda, und andereAWSDienste zur Optimierung häufiger Aufgaben mit intelligenten Konversationsschnittstellen, auf die Benutzer in Amazon Chime-Chatrooms zugreifen können.

Wenn Sie ein Amazon Chime Enterprise-Kontoadministrator sind, können Sie Chatbots verwenden, um Benutzern die Ausführung folgender Aufgaben zu ermöglichen:

- Abfragen ihrer internen Systeme nach Informationen.
- Automatisieren von Aufgaben.
- Empfangen von Benachrichtigungen für kritische Probleme.
- Erstellen von Support-Tickets.

Weitere Informationen zu Amazon Chime Enterprise-KontenVerwaltung Ihrer Amazon Chime Chime-Konten.

Wenn Sie ein Amazon Chime Enterprise-Konto verwalten, können Sie bis zu 10 Chatbots für die Integration mit Amazon Chime erstellen. Chatbots können nur in Chatrooms verwendet werden, die von Mitgliedern Ihres Kontos erstellt wurden. Nur Chatroom-Administratoren können Chatbots zu einem Chatroom hinzufügen. Nachdem ein Chatbot zu einem Chatroom hinzugefügt wurde, können Mitglieder des Chatrooms mithilfe von Befehlen, die vom Bot-Ersteller bereitgestellt werden, mit dem Bot interagieren. Führen Sie den folgenden Abschnitt aus diesem Thema aus.

Linux- und MacOS-Benutzer können einen benutzerdefinierten Beispiel-Chatbot erstellen. Weitere Informationen finden Sie unterErstellen Sie benutzerdefinierte Chatbots für Amazon Chime.

Inhalt

Verwenden von Chatbots mit Amazon Chime

Wenn Sie ein Amazon Chime Enterprise-Konto verwalten, können Sie bis zu 10 Chatbots für die Integration mit Amazon Chime erstellen. Chatbots können nur in Chatrooms verwendet werden, die von Mitgliedern Ihres Kontos erstellt wurden. Nur Chatroom-Administratoren können Chatbots zu einem Chatroom hinzufügen. Nachdem ein Chatbot zu einem Chatroom hinzugefügt wurde, können Mitglieder des Chatrooms mithilfe von Befehlen, die vom Bot-Ersteller bereitgestellt werden, mit dem Bot interagieren. Weitere Informationen finden Sie unterChatbots verwendenin derAmazon Chime Chime-Benutzerhandbuch.

Sie können auch den Amazon Chime Chime-API-Vorgang verwenden, um Chatbots für Ihr Amazon Chime Chime-Konto zu aktivieren oder zu beenden. Weitere Informationen finden Sie unter Chatbots aktualisieren.

> **Note**
>
> Sie können keine Chatbots löschen. Um zu verhindern, dass ein Chatbot in Ihrem Konto verwendet wird, verwenden Sie Amazon ChimeUpdateBotAPI-Betrieb inAmazon Chime API-Referenz. Wenn Sie einen Chatbot beenden, können Chatroom-Administratoren ihn aus einem Chatroom entfernen, aber sie können ihn nicht zu einem Chatroom hinzufügen.

Benutzer, die einen gestoppten Chatbot in einem Chatroom per @mention aufrufen, erhalten eine Fehlermeldung.

Voraussetzungen

Führen Sie die folgenden Voraussetzungen aus, bevor Sie das Verfahren für die Integration von Chatbots aus

- Erstellen Sie einen Chatbot.
- Erstellen Sie den ausgehenden Endpunkt für Amazon Chime, um Ereignisse an Ihren Bot zu senden. Wählen Sie einen ARN der AWS Lambda-Funktion oder einen HTTPS-Endpunkt. Weitere Informationen zu Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

Bewährte Methoden für DNS für HTTPS-Endgeräte

Wir empfehlen die folgenden bewährten Methoden beim Zuweisen von DNS für Ihren HTTPS-Endpunkt:

- Verwenden Sie eine DNS-Subdomäne, die dem Bot-Endpunkt zugeordnet ist.
- Verwenden Sie nur A-Records, die auf den Bot-Endpunkt verweisen.
- Schützen Sie Ihre DNS-Server und Ihr DNS-Registrar-Konto, um Domain-Hijjacking zu verhindern.
- Verwenden Sie öffentlich gültige TLS-Zwischenzertifikate, die dem Bot-Endpunkt zugewiesen sind.
- Überprüfen Sie die Bot-Nachrichtensignatur kryptografisch, bevor Sie auf eine Bot-Nachricht reagieren.

Nachdem Sie Ihren Chatbot erstellt haben, verwenden Sie denAWS Command Line Interface(AWS CLI) oder den Amazon Chime Chime-API-Vorgang, um die in den folgenden Abschnitten beschriebenen Aufgaben auszuführen.

Aufgaben

- Schritt 1: Integrieren Sie einen Chatbot in Amazon Chime
- Schritt 2: Führen Sie den ausstellbaren Amazon Chime aus
- Schritt 3: Fügen Sie den Chatbot zu einem Amazon Chime Chime-Chatroom hinzu
- Chatbot-Anfragen authentifizieren

- Chatbots aktualisieren

Schritt 1: Integrieren Sie einen Chatbot in Amazon Chime

Nachdem Sie das abgeschlossen habenVoraussetzungen, integrieren Sie Ihren Chatbot in Amazon Chime mithilfe derAWS CLIoder Amazon Chime API.

> **Note**
>
> Diese Verfahren erstellen einen Namen und eine E-Mail-Adresse für Ihren Chatbot. Chatbot-Namen und E-Mail-Adressen können nach der Erstellung nicht geändert werden.

AWS CLI

Um einen Chatbot mit dem zu integrierenAWS CLI

1. Um Ihren Chatbot in Amazon Chime zu integrieren, verwenden Sie dencreate-botBefehl in derAWS CLI.

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

   a. Geben Sie einen Chatbot-Anzeigenamen mit bis zu 55 alphanumerischen Zeichen oder Sonderzeichen (z. B. +, -,%) ein.

   b. Führen Sie den registrierten Domainnamen für Ihr Amazon Chime Enterprise-Konto aus.

2. Amazon Chime gibt eine Antwort aus, die die Bot-ID enthält.

   ```
   "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. Kopieren und speichern Sie die Bot-ID und die Bot-E-Mail-Adresse, um sie in den folgenden Verfahren zu verwenden.

Amazon Chime API

So integrieren Sie einen Chatbot mithilfe der Amazon Chime Chime-API

1. Um Ihren Chatbot in Amazon Chime zu integrieren, verwenden Sie denCreateBotAPI-Betrieb inAmazon Chime API-Referenz.
   a. Geben Sie einen Chatbot-Anzeigenamen mit bis zu 55 alphanumerischen Zeichen oder Sonderzeichen (z. B. +, -,%) ein.
   b. Führen Sie den registrierten Domainnamen für Ihr Amazon Chime Enterprise-Konto aus.
2. Amazon Chime gibt eine Antwort aus, die die Bot-ID enthält. Kopieren und speichern Sie die Bot-ID und die E-Mail-Adresse. Die Bot-E-Mail-Adresse sieht so aus:*exampleBot*-chimebot@*example.com*.

AWS-SDK für Java

Der folgende Beispielcode zeigt, wie Sie einen Chatbot mithilfe der integrierenAWSSDK for Java.

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

chime.createBot(createBotRequest);
```

Amazon Chime gibt eine Antwort aus, die die Bot-ID enthält. Kopieren und speichern Sie die Bot-ID und die E-Mail-Adresse. Die Bot-E-Mail-Adresse sieht so aus:*exampleBot*-chimebot@*example.com*.

Schritt 2: Führen Sie den ausstellbaren Amazon Chime aus

Nachdem Sie eine Chatbot-ID für Ihr Amazon Chime Enterprise-Konto erstellt haben, konfigurieren Sie Ihren ausgehenden Endpunkt, damit Amazon Chime Nachrichten an Ihren Bot sendet. Der

ausgehende Endpunkt kann ein seinAWS LambdaFunktion ARN oder ein HTTPS-Endpunkt, den Sie als Teil der erstellt habenVoraussetzungen. Weitere Informationen zu Lambda finden Sie im AWS Lambda Entwicklerhandbuch.

> **Note**
>
> Wenn der ausgehende HTTPS-Endpunkt für Ihren Bot nicht konfiguriert oder leer ist, können Chatroom-Administratoren den Bot nicht zu einem Chatroom hinzufügen. Außerdem können Chatroom-Benutzer nicht mit dem Bot interagieren.

AWS CLI

Um einen ausgehenden Endpunkt für Ihren Chatbot zu konfigurieren, verwenden Sie denput-events-configurationBefehl imAWS CLI. Konfigurieren Sie einen Lambda-Funktions-ARN oder einen ausgehenden HTTPS-Endpunkt.

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 antwortet mit der Bot-ID und dem HTTPS-Endpunkt.

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

Amazon Chime API

Verwenden Sie Amazon Chime, um den ausgehenden Endpunkt für Ihren Chatbot zu konfigurierenPutEventsConfigurationAPI-Betrieb inAmazon Chime API-Referenz. Konfigurieren Sie entweder einen Lambda-Funktions-ARN oder einen ausgehenden HTTPS-Endpunkt.

- Wenn Sie eine Lambda-Funktion ARN konfigurieren— Amazon Chime ruft Lambda auf, um dem Amazon Chime Chime-Administrator die Erlaubnis zu erteilenAWSKonto, um die bereitgestellte Quue für die Lambda-Funktion aufzurufen. Führen Sie einen Probelauf aus, um zu überprüfen, ob Amazon Chime die Berechtigung zum Aufrufen der Funktion hat. Wenn das Hinzufügen von Berechtigungen fehlschlägt oder wenn der Probelaufruf fehlschlägt, dann`PutEventsConfiguration`Die Anfrage gibt einen HTTP 4xx-Fehler zurück.
- Wenn Sie einen ausgehenden HTTPS-Endpunkt konfigurieren— Amazon Chime verifiziert Ihren Endpunkt, indem es eine HTTP-Post-Anfrage mit einer Challenge-JSON-Payload an den ausgehenden HTTPS-Endpunkt sendet, den Sie im vorherigen Schritt angegeben haben. Ihr ausgehender HTTPS-Endpunkt muss reagieren, indem er den Challenge-Parameter im JSON-Format zurückgibt. Die folgenden Beispiele zeigen die Anforderung und eine gültige Antwort.

  Request

```
HTTPS POST

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

  Response

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

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

Falls der Challenge-Handshake fehlschlägt, gibt die `PutEventsConfiguration`-Anforderung einen HTTP 4xx-Fehler zurück.

AWS-SDK für Java

Der folgende Beispielcode zeigt, wie Sie einen Endpunkt mit dem konfigurierenAWSSDK for 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):
```

Schritt 3: Fügen Sie den Chatbot zu einem Amazon Chime Chime-Chatroom hinzu

Nur ein Chatroom-Administrator kann einen Chatbot zu einem Chatroom hinzufügen. Sie verwenden die Chatbot-E-Mail-Adresse, die in erstellt wurdeSchritt 1.

So fügen Sie einem Chatroom ein Chatbot hinzu

1. Öffnen Sie den Amazon Chime Chime-Desktop-Client oder die Webanwendung.
2. Wählen Sie das Zahnradsymbol in der oberen rechten Ecke ausVerwalte Webhooks und Bots.
3. Wählen Sie Add Bot.
4. Füre-mail-adresse, geben Sie die Bot-E-Mail-Adresse ein.
5. Wählen Sie Add (Hinzufügen) aus.

Der Bot-Name erscheint in der Teilnehmerliste des Chatroom. Wenn zusätzliche Aktionen erforderlich sind, um einen Chatbot zu einem Chatroom hinzuzufügen, teilen Sie die Aktionen dem Chatroom-Administrator mit.

Nachdem der Chatbot dem Chatroom hinzugefügt wurde, geben Sie die Chatbot-Befehle an Ihre Chatroom-Benutzer weiter. Eine Möglichkeit, dies zu tun, besteht darin, Ihren Chatbot so zu programmieren, dass er Befehlshilfe an den Chatroom sendet, wenn er die Einladung zum Chatroom erhält. AWS empfiehlt außerdem, einen Hilfebefehl zu erstellen, den Ihre Chatbot-Benutzer verwenden können.

Chatbot-Anfragen authentifizieren

Sie können Anfragen authentifizieren, die von einem Amazon Chime Chime-Chatroom an Ihren Chatbot gesendet wurden. Berechnen Sie dazu eine Signatur auf der Grundlage der Anfrage. Überprüfen Sie dann, ob die berechnete Signatur mit der Signatur im Anforderungsheader übereinstimmt. Amazon Chime verwendet den HMAC SHA256-Hash, um die Signatur zu generieren.

Wenn Ihr Chatbot für Amazon Chime mit einem ausgehenden HTTPS-Endpunkt konfiguriert ist, verwenden Sie die folgenden Authentifizierungsschritte.

Um eine signierte Anfrage von Amazon Chime für einen Chatbot zu validieren, für den ein ausgehender HTTPS-Endpunkt konfiguriert ist

1. Rufen Sie den Chime-Signature-Header aus der HTTP-Anforderung ab.
2. Rufen Sie den Chime-Request-Timestamp-Header und den Text der Anforderung ab. Verwenden Sie anschließend einen vertikalen Strich als Trennzeichen zwischen den beiden Elementen, um eine Zeichenfolge zu erstellen.
3. Verwenden Sie denSecurityTokenaus CreateBot Antwort als Anfangsschlüssel vonHMAC_SHA_256, und hashen Sie die Zeichenfolge, die Sie in Schritt 2 erstellt haben.
4. Kodieren Sie den gehashten Byte mit Base64-Encoder zu einer Signatur-Zeichenfolge.
5. Vergleichen Sie diese berechnete Signatur mit derjenigen im Chime-Signature-Header.

Das folgende Codebeispiel demonstriert das Generieren einer Signatur mit 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;
            }
    }
```

Der ausgehende HTTPS-Endpunkt muss auf die Amazon Chime Chime-Anfrage antworten mit`200 0`Kinnerhalb von 2 Sekunden. Andernfalls schlägt die Anforderung fehl. Wenn der ausgehende HTTPS-Endpunkt nach 2 Sekunden nicht verfügbar ist, möglicherweise aufgrund eines Verbindungs- oder Lese-Timeouts, oder wenn Amazon Chime einen 5xx-Antwortcode erhält, wiederholt Amazon Chime die Anfrage zweimal. Die erste Wiederholung wird 200 Millisekunden nach dem Fehlschlagen der ersten Anforderung gesendet. Die zweite Wiederholung wird 400 Millisekunden nach dem Fehlschlagen der vorherigen Wiederholung gesendet. Wenn der ausgehende HTTPS-Endpunkt nach der zweiten Wiederholung immer noch nicht verfügbar ist, schlägt die Anforderung fehl.

> **Note**
>
> Der Chime-Request-Timestamp ändert sich jedes Mal, wenn die Anforderung wiederholt wird.

Wenn Ihr Chatbot für Amazon Chime mithilfe einer Lambda-Funktion ARN konfiguriert ist, verwenden Sie die folgenden Authentifizierungsschritte.

Um eine signierte Anfrage von Amazon Chime für einen Chatbot mit konfiguriertem Lambda-Funktions-ARN zu validieren

1. Holen Sie sich dieGlockenspiel-SignaturundChime-Request-Zeitstempelaus der Lambda-AnfrageClientContext, im Base64-codierten JSON-Format.

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

2. Rufen Sie den Text der Anforderung aus der Anforderungsnutzlast ab.
3. Verwenden Sie denSecurityTokenaus`CreateBot`Antwort als Anfangsschlüssel vonHMAC_SHA_256, und hashen Sie die Zeichenfolge, die Sie erstellt haben.
4. Kodieren Sie den gehashten Byte mit Base64-Encoder zu einer Signatur-Zeichenfolge.

5. Vergleichen Sie diese berechnete Signatur mit derjenigen im Chime-Signature-Header.

Wenn ein`com.amazonaws.SdkClientException`tritt während des Lambda-Aufrufs auf, Amazon Chime wiederholt die Anfrage zweimal.

Chatbots aktualisieren

Als Amazon Chime Chime-Kontoadministrator können Sie die Amazon Chime Chime-API mit dem verwendenAWSSDK oderAWS CLIum Ihre Chatbot-Details einzusehen. Sie können auch die Verwendung Ihrer Chatbots in Ihrem Konto aktivieren oder verhindern. Sie können auch Sicherheitstoken für Ihren Chatbot neu generieren.

Führen Sie die folgenden Nachrichten ausAmazon Chime API-Referenz:

- GetBot— Ruft Ihre Chatbot-Details ab, z. B. die Bot-E-Mail-Adresse und den Bot-Typ.
- UpdateBot— Aktiviert oder verhindert die Verwendung eines Chatbots in Ihrem Konto.
- RegenerateSecurityToken— Regeneriert das Sicherheitstoken für Ihren Chatbot.

Sie können das auch ändern`PutEventsConfiguration`für deinen Chatbot. Wenn Ihr Chatbot beispielsweise ursprünglich für die Verwendung eines ausgehenden HTTPS-Endpunkts konfiguriert wurde, können Sie die vorherige Ereigniskonfiguration löschen und eine neue Ereigniskonfiguration für einen Lambda-Funktions-ARN ARN.

Führen Sie die folgenden Nachrichten ausAmazon Chime API-Referenz:

- DeleteEventsConfiguration
- PutEventsConfiguration

Amazon Chime Chime-Ereignisse, die an Chatbots gesendet wurden

Die folgenden Ereignisse werden von Amazon Chime an Ihren Chatbot gesendet:

- Laden Sie ein— Wird gesendet, wenn Ihr Chatbot zu einem Amazon Chime Chime-Chatroom hinzugefügt wird
- Erwähnen— Wird gesendet, wenn ein Nutzer in einem Chatroom deinen Chatbot @mentions
- Entfernen— Wird gesendet, wenn Ihr Chatbot aus einem Amazon Chime Chime-Chatroom entfernt wird

Die folgenden Beispiele zeigen die JSON-Nutzdaten, die für jedes dieser Ereignisse an Ihren Chatbot gesendet wurden.

Example : Veranstaltung einladen

```
            {
              "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 : Veranstaltung erwähnen

```
            {
                "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**
>
> Die `InboundHttpsEndpoint`-URL für ein Mention-Ereignis läuft in zwei Minuten ab, nachdem sie gesendet wird.

Example : Ereignis entfernen

```
            {
                "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"
            }
```

Webhooks für Amazon Chime erstellen

Webhooks ermöglichen es Webanwendungen, in Echtzeit miteinander zu kommunizieren. Normalerweise senden Webhooks Benachrichtigungen, wenn eine Aktion stattfindet. Angenommen, Sie betreiben eine Online-Shopping-Website. Webhooks können Sie benachrichtigen, wenn ein Kunde Artikel in einen Warenkorb legt, eine Bestellung bezahlt oder einen Kommentar sendet. Webhooks benötigen nicht so viel Programmierung wie herkömmliche Anwendungen und verbrauchen nicht so viel Rechenleistung. Ohne einen Webhook muss ein Programm häufig Daten

abfragen, um sie in Echtzeit zu erhalten. Mit einem Webhook veröffentlicht die sendende Anwendung die Daten sofort.

Eingehende Webhooks, die Sie erstellen, können programmgesteuert Nachrichten an Amazon Chime-Chatrooms senden. Ein Webhook kann beispielsweise ein Kundenservice-Team über die Erstellung eines neuen Tickets mit hoher Priorität informieren und einen Link zu dem Ticket im Chatroom hinzufügen.

Webhooks-Nachrichten können mit Markdown formatiert werden und Emojis enthalten. HTTP-Links und E-Mail-Adressen werden als aktive Links wiedergegeben. Die Nachrichten können auch die Anmerkungen "@All" und "@Present" enthalten, um alle Mitglieder bzw. anwesende Mitglieder eines Chatrooms aufmerksam zu machen. Um einen Chatroom-Teilnehmer direkt anzusprechen (@mention), verwenden Sie sein Alias oder seine vollständige E-Mail-Adresse. Beispiel: `@alias` oder `@alias@domain.com`.

Webhooks können nur Teil eines Chatrooms sein und nicht geteilt werden. Amazon Chime-Chatroom-Administratoren können bis zu 10 Webhooks für jeden Chatraum hinzufügen.

Nachdem Sie einen Webhook erstellt haben, können Sie ihn in einen Amazon Chime-Chatroom integrieren, wie im folgenden Verfahren gezeigt.

Um einen Webhook in einen Chatroom zu integrieren

1. Holen Sie sich die Webhook-URL vom Chatroom-Administrator. Weitere Informationen finden Sie unterHinzufügen von Webhooks zu einem Chatroomin derAmazon Chime-Benutzerhandbuch.
2. Verwenden Sie die Webhook-URL in dem Skript oder der Anwendung, die Sie erstellt haben, um Nachrichten an den Chatroom zu senden:

   a. Die URL akzeptiert eine HTTP-POST-Anforderung.

   b. Amazon Chime-Webhooks akzeptieren eine JSON-Payload mit einem einzigen SchlüsselInhalt. Es folgt ein curl-Bespielbefehl mit einer Beispielnutzlast:

   ```
   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"}'
   ```

   Das Folgende ist ein BeispielPowerShellBefehl für Windows-Benutzer:

```
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"}'
```

Nachdem das externe Programm die HTTP-POST-Anforderung an die Webhook-URL gesendet hat, validiert der Server, dass der Webhook gültig ist und ihm ein Chatroom zugewiesen ist. Der Webhook wird in der Chatroom-Liste mit einem Webhook-Symbol neben dem Namen angezeigt. Chatroom-Nachrichten, die vom Webhook gesendet werden, erscheinen im Chatroom unter dem Webhook-Namen gefolgt von (Webhook).

> **Note**
>
> CORS ist derzeit nicht für Webhooks aktiviert.

Behebung von Webhook-Fehlern

Im Folgenden finden Sie eine Liste von Fehlern bezüglich Webhook:

- Das eingehende Webhook-Ratenlimit für jeden Webhook ist 1 TPS pro Chatroom. Eine Drosselung der Ergebnisse führt zu einem HTTP 429-Fehler.
- Die von einem Webhook-Host geposteten Nachrichten dürfen maximal 4 KB betragen. Eine größere Nachrichtennutzlast führt zu einem HTTP 413-Fehler.
- Von einem Webhook mit @All- und @Present-Anmerkungen gesendete Nachrichten eignen sich nur für Chatrooms mit 50 oder weniger Mitgliedern. Bei mehr als 50 Mitgliedern führt dies zu einem HTTP 400-Fehler.
- Wenn die Webhook-URL neu generiert wird, führt die Verwendung des alten URL zu einem HTTP 404-Fehler.
- Wenn der Webhook in einem Raum gelöscht wird, führt die Verwendung der alten URL zu einem HTTP 404-Fehler.
- Ungültige Webhook-URLs ergeben HTTP 403-Fehler.
- Wenn der Service nicht verfügbar ist, erhält der Benutzer in der Antwort einen HTTP 503-Fehler.

Administrativer Support für Amazon Chime

> **Note**
>
> Hilfe zu Ihrem Amazon-Einkaufskonto erhalten Sie unter Kundenservice auf amazon.com.

Wenn Sie den Support für Amazon Chime kontaktieren möchten, wählen Sie eine der folgenden Optionen:

- Wenn Sie ein AWS Support-Konto haben, gehen Sie zum Support Center und reichen Sie ein Ticket ein.
- Öffnen Sie andernfalls das AWS Management Consoleund wählen Sie Amazon Chime, Support, Anfrage senden aus.

Geben Sie so viele der folgenden Informationen wie möglich an:

- Eine ausführliche Beschreibung des Problems.
- Den Zeitpunkt, zu dem das Problem aufgetreten ist, einschließlich Ihrer Zeitzone.
- Ihre Amazon Chime Chime-Version. So finden Sie Ihre Versionsnummer:
  - Wählen Sie in Windows Hilfe, Über Amazon Chime.
  - Wählen Sie in macOS Amazon Chime, Info zu Amazon Chime.
  - Wählen Sie unter iOS und Android Einstellungen, Info.
- Die Referenz-ID des Protokolls. So finden Sie diese ID:
  - Wählen Sie unter Windows und macOS Hilfe, Diagnoseprotokolle senden.
  - Wählen Sie unter iOS und Android Einstellungen, Diagnoseprotokolle senden.
- Wenn das Problem in Zusammenhang mit einem Meeting auftritt, die Meeting-ID.

Sicherheit in Amazon Chime

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Chime gelten, finden Sie unter AWS-Services in Umfang nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon Chime anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon Chime konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS AWS-Services nutzen können, die Ihnen helfen, Ihre Amazon Chime Chime-Ressourcen zu überwachen und zu sichern.

Themen

- Protokollieren und überwachen in Amazon Chime
- Konformitätsprüfung für Amazon Chime
- Resilienz in Amazon Chime
- Infrastruktursicherheit in Amazon Chime
- Grundlegendes zu automatischen Updates von Amazon Chime

Identitäts- und Zugriffsmanagement für Amazon Chime

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Chime Chime-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon Chime ausführen.

Servicebenutzer — Wenn Sie den Amazon Chime Chime-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Amazon Chime Chime-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Amazon Chime nicht zugreifen können, finden Sie weitere Informationen unterProblembehandlung Amazon Chime Chime-Identität und Zugriff.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Chime-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon Chime. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Chime Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um

die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon Chime verwenden kann, finden Sie unter. So funktioniert Amazon Chime mit IAM

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon Chime zu verwalten. Beispiele für identitätsbasierte Amazon Chime Chime-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien von Amazon Chime

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -

Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

AWS verwaltete Richtlinien für Amazon Chime

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken häufige Anwendungsfälle ab und sind in Ihrem AWS -Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die AWS verwaltete ReadOnlyAccess-Richtlinie bietet beispielsweise Lesezugriff auf alle AWS Dienste und Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon Chime mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Chime zu verwalten, sollten Sie wissen, welche IAM-Funktionen für Amazon Chime verfügbar sind. Einen allgemeinen Überblick darüber, wie Amazon Chime und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Themen

- Identitätsbasierte Richtlinien von Amazon Chime
- Ressourcen
- Beispiele

Identitätsbasierte Richtlinien von Amazon Chime

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Amazon Chime unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bedingungsschlüssel

Amazon Chime stellt keine servicespezifischen Zustandsschlüssel zur Verfügung. Eine Liste aller globalen AWS -Bedingungsschlüssel finden Sie unter Globale AWS -Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Ressourcen

Amazon Chime unterstützt die Angabe von Ressourcen-ARNs in einer Richtlinie nicht.

Beispiele

Beispiele für identitätsbasierte Richtlinien von Amazon Chime finden Sie unter. Beispiele für identitätsbasierte Richtlinien von Amazon Chime

Serviceübergreifende Confused-Deputy-Prävention

Das Problem mit dem verwirrten Stellvertreter ist ein Problem der Informationssicherheit, das auftritt, wenn eine Entität, die nicht berechtigt ist, eine Aktion auszuführen, eine Entität mit mehr Rechten zur Ausführung der Aktion aufruft. Auf diese Weise können böswillige Akteure Befehle ausführen oder Ressourcen ändern, zu deren Ausführung oder Zugriff sie sonst nicht berechtigt wären. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Das Problem des verwirrten Stellvertreters.

In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Szenario mit verwirrtem Stellvertreter führen. Ein dienstübergreifender Identitätswechsel tritt auf, wenn ein Dienst (der anrufende Dienst) einen anderen Dienst (den angerufenen Dienst) anruft. Ein böswilliger Akteur kann den anrufenden Dienst verwenden, um Ressourcen in einem anderen Dienst zu ändern, indem er Berechtigungen verwendet, über die er normalerweise nicht verfügen würde.

AWS bietet Dienstprinzipalen verwalteten Zugriff auf Ressourcen in Ihrem Konto, um Sie beim Schutz Ihrer Ressourcen zu unterstützen. Wir empfehlen, den `aws:SourceAccount` globalen Condition-Kontextschlüssel in Ihren Ressourcenrichtlinien zu verwenden. Diese Schlüssel schränken die Berechtigungen ein, die Amazon Chime einem anderen Service für diese Ressource gewährt.

Das folgende Beispiel zeigt eine S3-Bucket-Richtlinie, die den `aws:SourceAccount` globalen Bedingungskontextschlüssel im konfigurierten `CallDetailRecords` S3-Bucket verwendet, um das Problem mit dem verwirrten Stellvertreter zu verhindern.

```
{
    "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"
                }
            }
        }
    ]
}
```

Ressourcenbasierte Richtlinien von Amazon Chime

Amazon Chime unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung basierend auf Amazon Chime Chime-Tags

Amazon Chime unterstützt weder das Markieren von Ressourcen noch die Steuerung des Zugriffs auf der Grundlage von Tags.

Amazon Chime IAM-Rollen

Eine IAM-Rolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit Amazon Chime verwenden

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder GetFederationToken aufrufen.

Amazon Chime unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit Diensten verknüpfte Rollen ermöglichen es AWS Diensten, auf Ressourcen in anderen Diensten zuzugreifen, die Aktionen in Ihrem Namen ausführen. Mit Diensten verknüpfte Rollen werden in Ihrem IAM-Konto angezeigt, und die Dienste sind Eigentümer der Rollen. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Amazon Chime unterstützt serviceverknüpfte Rollen. Einzelheiten zum Erstellen oder Verwalten von serviceverknüpften Amazon Chime Chime-Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Amazon Chime

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Amazon Chime unterstützt keine Servicerollen.

Beispiele für identitätsbasierte Richtlinien von Amazon Chime

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, Amazon Chime Chime-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Chime Chime-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden

Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon Chime Chime-Konsole

Um auf die Amazon Chime Chime-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon Chime Chime-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten weiterhin die Amazon Chime Chime-Konsole verwenden können, fügen Sie den Entitäten auch die folgende AWS verwaltete AmazonChimeReadOnlyRichtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

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

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Erlauben Sie Benutzern vollen Zugriff auf Amazon Chime

Die folgende AWS verwaltete AmazonChimeFullAccessRichtlinie gewährt einem IAM-Benutzer vollen Zugriff auf Amazon Chime Chime-Ressourcen. Die Richtlinie gewährt dem Benutzer Zugriff auf alle Amazon Chime-Operationen sowie auf andere Vorgänge, die Amazon Chime in Ihrem Namen ausführen muss.

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

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet die Erlaubnis, diese Aktion auf der Konsole oder programmgesteuert mithilfe der API oder durchzuführen. AWS CLI 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": "*"
        }
    ]
}
```

Benutzern den Zugriff auf Benutzerverwaltungsaktionen erlauben

Verwenden Sie die AWS verwaltete AmazonChimeUserManagementRichtlinie, um Benutzern Zugriff auf Benutzerverwaltungsaktionen in der Amazon Chime Chime-Konsole zu gewähren.

```
{
    "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 verwaltete Richtlinie: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Das `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` ermöglicht Amazon Chime Voice Connectors, Medien auf Amazon Kinesis Video Streams zu streamen, Streaming-Benachrichtigungen bereitzustellen und Sprache mithilfe von Amazon Polly zu synthetisieren. Diese Richtlinie gewährt dem Amazon Chime Voice Connector-Service die Erlaubnis, auf die Amazon Kinesis Video Streams von Kunden zuzugreifen, Benachrichtigungsereignisse an den Amazon Simple Notification Service und Amazon Simple Queue Service zu senden und Amazon Polly zur Sprachsynthese zu verwenden, wenn die Sprachanwendungen und -aktionen des Amazon Chime SDK verwendet werden. `Speak` `SpeakAndGetDigits` Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon Chime SDK im Amazon Chime SDK-Administratorhandbuch.

Amazon Chime Chime-Updates für AWS verwaltete Richtlinien

In der folgenden Tabelle sind die Aktualisierungen der Amazon Chime IAM-Richtlinie aufgeführt und beschrieben.

Änderung	Beschreibung	Datum
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Aktualisierung auf eine bestehende Richtlinie	Amazon Chime Voice Connectors hat neue Berechtigungen hinzugefügt, mit denen Sie Amazon Polly zur Sprachsynthese verwenden können. Diese Berechtigungen sind erforderlich, um die `SpeakAndGetDigits` Aktionen `Speak` und in Amazon Chime SDK Voice Applications verwenden zu können.	15. März 2022
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Aktualisierung auf eine bestehende Richtlinie	Amazon Chime Voice Connector hat neue Berechtigungen hinzugefügt, um den Zugriff auf Amazon Kinesis Video Streams zu ermöglichen und Benachrichtigungsereignisse an SNS und SQS zu senden. Diese Berechtigungen sind erforderlich, damit Amazon Chime Voice Connectors Medien auf Amazon Kinesis Video Streams streamen und Streaming-Benachrichtigungen bereitstellen kann.	20. Dezember 2021

Änderung	Beschreibung	Datum
Änderung der bestehenden Richtlinie. IAM-Benutzer oder -Rollen mit der Chime SDK-Richtlinie erstellen.	Amazon Chime hat neue Aktionen hinzugefügt, um die erweiterte Validierung zu unterstützen. Eine Reihe von Aktionen wurde hinzugefügt, um das Auflisten und Markieren von Teilnehmern und Besprechungsressourcen sowie das Starten und Beenden der Besprechungstranskription zu ermöglichen.	23. September 2021
Amazon Chime hat begonnen, Änderungen zu verfolgen	Amazon Chime hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	23. September 2021

Problembehandlung Amazon Chime Chime-Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Chime und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon Chime durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon Chime Chime-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon Chime durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `chime:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `chime:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon Chime übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Chime auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon Chime Chime-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon Chime diese Funktionen unterstützt, finden Sie unterSo funktioniert Amazon Chime mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in IAM.

Verwenden von serviceverknüpften Rollen für Amazon Chime

Amazon Chime verwendetAWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Amazon Chime verknüpft ist. Serviceverknüpfte Rollen werden von Amazon Chime vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen andererAWS -Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle macht die Einrichtung von Amazon Chime effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Chime definiert die Berechtigungen seiner serviceverknüpfte Rollen, und sofern nicht anders definiert, kann nur Amazon Chime seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und

Berechtigungsrichtlinie. Die Berechtigungsrichtlinie kann an keine andere IAM-Entität angefügt werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Amazon Chime Chime-Ressourcen, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entfernen können.

Weitere Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Themen

Verwenden von Rollen mit gemeinsam genutzten Alexa for Business Business-Geräten

Die Informationen in den folgenden Abschnitten erläutern, wie Sie serviceverknüpfte Rollen verwenden und Amazon Chime Zugriff auf die Alexa for Business Business-Ressourcen in IhremAWS Konto gewähren.

Themen

Serviceverknüpfte Rollenberechtigungen für Amazon Chime

Amazon Chime verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForAmazonChime—Ermöglicht den Zugriff aufAWS -Services und Ressourcen, die von Amazon Chime Alexa for Business verwaltet werden.

Die AWSServiceRoleForAmazonChime serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `chime.amazonaws.com`

Die Rollenberechtigungsrichtlinie erlaubt Amazon Chime, die folgende Aktion auf der angegebenen Ressource durchzuführen:

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

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpfte Rolle für Amazon Chime

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Alexa for Business für ein gemeinsam genutzten Gerät in Amazon Chime in derAWS Management Console, demAWS CLI, oder derAWS -API aktivieren, erstellt Amazon Chime die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall Amazon Chime zu erstellen. Erstellen Sie in der AWS CLI oder der AWS-API eine servicegebundene Rolle mit dem Servicenamen `chime.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpfte Rolle für Amazon Chime

Amazon Chime erlaubt Ihnen nicht, die AWSServiceRoleForAmazonChime serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpfte Rolle für Amazon Chime

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine

ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

> **Note**
>
> Wenn Amazon Chime die Rolle verwendet, während Sie die Ressourcen löschen möchten, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die von der AWSServiceRoleForAmazonChime (Konsole) verwendeten Amazon Chime Chime-Ressourcen

- Schalten Sie Alexa for Business für alle gemeinsam genutzten Geräte in Ihrem Amazon Chime Chime-Konto aus.

  a. Öffnen Sie die Amazon Chime Chime-Konsole unter https://chime.aws.amazon.com/.
  b. Wählen Sie Benutzer, Freigegebene Geräte aus.
  c. Wählen Sie ein Gerät aus.
  d. Wählen Sie Actions (Aktionen).
  e. Wählen Sie „Alexa for Business deaktivieren“.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForAmazonChime serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützten Regionen für Amazon Chime serviceverknüpfte Rollen

Amazon Chime unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter Amazon Chime Chime-Endpunkte und -Kontingente.

Rollen mit Live-Transkription verwenden

Die Informationen in den folgenden Abschnitten erklären, wie Sie eine serviceverknüpfte Rolle für die Live-Transkription von Amazon Chime Chime-Live-Transkription erstellen und verwalten. Weitere Informationen zum Live-Transkriptionsdienst finden Sie unter Verwenden der Live-Transkription des Amazon Chime SDK.

Themen

Service-Linked Role for for for for for for for Amazon Chime for for for for for for for for for for

Amazon Chime Live Transcription verwendet eine serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForAmazonChimeTranscription— Ermöglicht Amazon Chime, in Ihrem Namen auf Amazon Transcribe und Amazon Transcribe Medical zuzugreifen.

Die AWSServiceRoleForAmazonChimeTranscription serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `transcription.chime.amazonaws.com`

Die Richtlinie für Rollenberechtigungen erlaubt Amazon Chime, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `transcribe:StartStreamTranscription` für `all AWS resources`
- Aktion: `transcribe:StartMedicalStreamTranscription` für `all AWS resources`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für die Amazon Chime Live-Transkription

Sie verwenden die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall Chime Transcription zu erstellen.

> **Note**
>
> Sie benötigen IAM-Administratorrechte, um diese Schritte ausführen zu können. Wenn Sie dies nicht tun, wenden Sie sich an einen Systemadministrator.

So erstellen Sie die Rolle

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM-Konsole Roles aus und wählen Sie im Navigationsbereich der IAM-Konsole Roles aus.
3. Wählen Sie den Rollentyp AWS Service, wählen Sie dann Chime und dann Chime Transcription.
4. Wählen Sie Next (Weiter).
5. Wählen Sie Next (Weiter).
6. Bearbeiten Sie die Beschreibung nach Bedarf und wählen Sie dann Rolle erstellen.

Sie können auch dieAWS CLIAWS -API verwenden, um eine serviceverknüpfte Rolle mit dem Namen transcription.chime.amazonaws.com zu erstellen.

Führen Sie in der CLI diesen Befehl aus:`aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

Weitere Informationen finden Sie unter Erstellen einer servicegebundenen Rolle im IAM-Leitfaden. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für die -Rolle für die -Rolle für die Live-Transkription

Amazon Chime erlaubt es Ihnen nicht, die AWSServiceRoleForAmazonChimeTranscription serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr

geändert werden. Sie können IAM verwenden, um die Beschreibung der Rolle zu bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für die Amazon Chime für die -Rolle für

Wenn Sie eine Funktion oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForAmazonChimeTranscription serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen Amazon Chime Service-Linked Roles

Amazon Chime unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter Amazon Chime-Endpunkte und Kontingente und Verwenden von Amazon Chime SDK-Medienregionen.

Verwenden von Rollen mit Amazon Chime SDK-Medienpipelines

Die Informationen in den folgenden Abschnitten erklären, wie Sie eine serviceverknüpfte Rolle für Amazon Chime SDK Media Pipelines erstellen und verwalten.

Themen

- Serviceverknüpfte Rollenberechtigungen für Amazon Chime SDK-Medienpipelines
- Erstellen einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines
- Bearbeiten einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines
- Löschen einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines
- Unterstützten Regionen für Amazon Chime SDK-Medien-Pipelines serviceverknüpfte Rollen

Serviceverknüpfte Rollenberechtigungen für Amazon Chime SDK-Medienpipelines

Amazon Chime verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForAmazonChimeSDKMediaPipelines— Ermöglicht Amazon Chime SDK-Medienpipelines, in Ihrem Namen auf Amazon Chime SDK-Besprechungen zuzugreifen.

Die AWSServiceRoleForAmazonChimeSDKMediaPipelines serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `mediapipelines.chime.amazonaws.com`

Die Rolle erlaubt Amazon Chime, die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

- Aktion: `chime:CreateAttendee` für `all AWS resources`
- Aktion: `chime:DeleteAttendee` für `all AWS resources`
- Aktion: `chime:GetMeeting` für `all AWS resources`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines

Sie verwenden die IAM-Konsole, um eine serviceverknüpfte Rolle mit dem Amazon Chime SDK Media Pipelines* -Anwendungsfall zu erstellen.

> **Note**
>
> Sie benötigen IAM-Administratorrechte, um diese Schritte ausführen zu können. Wenn Sie dies nicht tun, wenden Sie sich an einen Systemadministrator.

So erstellen Sie die Rolle

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Roles und wählen Sie dann Create role.
3. Wählen Sie den Rollentyp AWSService, dann Chime und dann Chime SDK Media Pipelines.
4. Wählen Sie Next (Weiter).
5. Wählen Sie Next (Weiter).
6. Bearbeiten Sie die Beschreibung nach Bedarf und wählen Sie dann Rolle erstellen.

Sie können auch dieAWS CLI oderAWS -API verwenden, um eine serviceverknüpfte Rolle namens mediapipelines.chime.amazonaws.com zu erstellen.

Führen Sie in derAWS CLI diesen Befehl aus:`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Weitere Informationen finden Sie unter Erstellen einer servicegebundenen Rolle im IAM-Leitfaden. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines

Amazon Chime erlaubt Ihnen nicht, die AWSServiceRoleForAmazonChimeSDKMediaPipelines serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpfte Rolle für Amazon Chime SDK-Medienpipelines

Wenn Sie eine Funktion oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForAmazonChimeSDKMediaPipelines serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützten Regionen für Amazon Chime SDK-Medien-Pipelines serviceverknüpfte Rollen

Amazon Chime SDK unterstützt die Verwendung von serviceverknüpften Rollen in allenAWS Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter Amazon Chime Chime-Endpunkte und -Kontingente.

Protokollieren und überwachen in Amazon Chime

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Chime und Ihrer anderenAWS -Lösungen aufrechtzuerhalten. AWSstellt die folgenden Tools zur Verfügung, um

Amazon Chime zu überwachen, Probleme zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht in Echtzeit IhreAWS -Ressourcen und die in ausgeführten AnwendungenAWS. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Beispielsweise können Sie mit die CPU-Auslastung oder andere Metriken Ihrer Amazon EC2-Instances CloudWatch erfassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im Amazon CloudWatch Benutzerhandbuch.
- Amazon EventBridge liefert nahezu in Echtzeit einen Strom von Systemereignissen, die Änderungen inAWS -Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Computing. Damit können Sie Regeln schreiben, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen AWS-Services auslösen, wenn diese Ereignisse auftreten. Weitere Informationen finden Sie im Amazon EventBridge Benutzerhandbuch.
- Amazon Amazon CloudWatch Logs ermöglicht Ihnen die Überwachung, Speicherung und den Zugriff auf Ihre Protokolldateien von Amazon EC2-Instances und anderen Quellen. CloudTrail CloudWatch Protokolle können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die vom oder für das AWS-Konto getätigt wurden. Der Service gibt die Protokolldateien in einen Amazon S3-Bucket aus, den Sie zuvor angegeben haben. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen

Amazon Chime mit Amazon überwachen CloudWatch

Sie können Amazon Chime überwachen CloudWatch, das Rohdaten erfasst und in lesbare Metriken nahezu in Echtzeit verarbeitet. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im Amazon CloudWatch Benutzerhandbuch.

CloudWatch Metriken für Amazon Chime

Amazon Chime sendet die folgenden Metriken an CloudWatch.

Der`AWS/ChimeVoiceConnector` Namespace enthält die folgenden Metriken für Telefonnummern, die IhremAWS Konto und Amazon Chime Voice Connectors zugewiesen sind.

Metrik	Beschreibung
`InboundCallAttempts`	Die Anzahl der versuchten eingehenden Anrufe. Einheiten: Anzahl
`InboundCallFailures`	Die Anzahl der Fehler bei eingehenden Anrufen. Einheiten: Anzahl
`InboundCallsAnswered`	Die Anzahl der eingehenden Anrufe, die beantwortet werden. Einheiten: Anzahl
`InboundCallsActive`	Die Anzahl der eingehenden Anrufe, die derzeit aktiv sind. Einheiten: Anzahl
`OutboundCallAttempts`	Die Anzahl der versuchten ausgehenden Anrufe.

Metrik	Beschreibung
	Einheiten: Anzahl
`OutboundCallFailures`	Die Anzahl der Fehler bei ausgehenden Anrufen. Einheiten: Anzahl
`OutboundCallsAnswered`	Die Anzahl der ausgehenden Anrufe, die beantwortet werden. Einheiten: Anzahl
`OutboundCallsActive`	Die Anzahl der ausgehenden Anrufe, die derzeit aktiv sind. Einheiten: Anzahl
`Throttles`	Gibt an, wie oft Ihr Konto gedrosselt wird, wenn Sie versuchen, einen Anruf zu tätigen. Einheiten: Anzahl
`Sip1xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscod es der 1xx-Ebene. Einheiten: Anzahl
`Sip2xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscod es der 2xx-Ebene. Einheiten: Anzahl
`Sip3xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscod es der 3xx-Ebene. Einheiten: Anzahl

Metrik	Beschreibung
`Sip4xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscodes der 4xx-Ebene. Einheiten: Anzahl
`Sip5xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscodes der 5xx-Ebene. Einheiten: Anzahl
`Sip6xxCodes`	Die Anzahl der SIP-Nachrichten mit Statuscodes der 6xx-Ebene. Einheiten: Anzahl
`CustomerToVcRtpPackets`	Die Anzahl der RTP-Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`CustomerToVcRtpBytes`	Die Anzahl der vom Kunden gesendeten Bytes. Einheiten: Anzahl
`CustomerToVcRtcpPackets`	Die Anzahl der RTCP-Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`CustomerToVcRtcpBytes`	Die Anzahl der vom Kunden gesendeten Bytes. Einheiten: Anzahl

Metrik	Beschreibung
CustomerToVcPacketsLost	Die Anzahl der Pakete, die bei der Übertragung vom Kunden zur Amazon Chime Voice Connector-Infrastruktur verloren gegangen sind. Einheiten: Anzahl
CustomerToVcJitter	Der durchschnittliche Jitter für Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet werden. Einheiten: Mikrosekunden
VcToCustomerRtpPackets	Die Anzahl der RTP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet wurden. Einheiten: Anzahl
VcToCustomerRtpBytes	Die Anzahl der Bytes Amazon Chime die in RTP-Paketen gesendet werden. Einheiten: Anzahl
VcToCustomerRtcpPackets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet wurden. Einheiten: Anzahl
VcToCustomerRtcpBytes	Die Anzahl der Bytes Amazon Chime in RTCP-Paketen gesendet werden. Einheiten: Anzahl

Metrik	Beschreibung
VcToCustomerPacketsLost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime Voice Connector-Infrastruktur zum Kunden verloren gegangen sind. Einheiten: Anzahl
VcToCustomerJitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet werden. Einheiten: Mikrosekunden
RTTBetweenVcAndCustomer	Die durchschnittliche Hin- und Rückflugzeit zwischen dem Kunden und der Amazon Chime Voice Connector-Infrastruktur. Einheiten: Mikrosekunden
MOSBetweenVcAndCustomer	Der geschätzte Mean Opinion Score (MOS) für Sprachstreams zwischen dem Kunden und der Amazon Chime Voice Connector-Infrastruktur. Einheiten: Ergebnis zwischen 1,0 bis 4,4. Eine höhere Punktzahl weist auf eine besser wahrgenommene Audioqualität hin.
RemoteToVcRtpPackets	Die Anzahl der RTP-Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
RemoteToVcRtpBytes	Die Anzahl der vom Remote-Ende gesendeten Bytes. Einheiten: Anzahl

Metrik	Beschreibung
`RemoteToVcRtcpPackets`	Die Anzahl der RTCP-Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`RemoteToVcRtcpBytes`	Die Anzahl der vom Remote-Ende gesendeten Bytes. Einheiten: Anzahl
`RemoteToVcPacketsLost`	Die Anzahl der Pakete, die bei der Übertragung vom Remote-Ende zur Amazon Chime Voice Connector-Infrastruktur verloren gegangen sind. Einheiten: Anzahl
`RemoteToVcJitter`	Der durchschnittliche Jitter für Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet werden. Einheiten: Mikrosekunden
`VcToRemoteRtpPackets`	Die Anzahl der RTP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden. Einheiten: Anzahl
`VcToRemoteRtpBytes`	Die Anzahl der Bytes Amazon Chime werden in RTP-Paketen gesendet. Einheiten: Anzahl

Metrik	Beschreibung
VcToRemoteRtcpPackets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden. Einheiten: Anzahl
VcToRemoteRtcpBytes	Die Anzahl der Bytes Amazon Chime die in RTCP-Paketen gesendet werden. Einheiten: Anzahl
VcToRemotePacketsLost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime Voice Connector-Infrastruktur zum Remote-Ende verloren gegangen sind. Einheiten: Anzahl
VcToRemoteJitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet werden. Einheiten: Mikrosekunden
RTTBetweenVcAndRemote	Die durchschnittliche Hin- und Rückflugzeit zwischen dem Remote-Ende und der Amazon Chime Voice Connector-Infrastruktur. Einheiten: Mikrosekunden
MOSBetweenVcAndRemote	Der geschätzte Mean Opinion Score (MOS) für Sprachstreams zwischen dem Remote-Ende und der Amazon Chime Voice Connector-Infrastruktur. Einheiten: Einheiten: Ergebnis zwischen 1,0 bis 4,4. Eine höhere Punktzahl weist auf eine besser wahrgenommene Audioqualität hin.

CloudWatch Abmessungen für Amazon Chime

Die CloudWatch Dimensionen, die Sie mit Amazon Chime verwenden können, sind wie folgt aufgeführt.

Dimension	Beschreibung
`VoiceConnectorId`	Die ID des Amazon Chime Voice Connectors, für den Messwerte angezeigt werden sollen.
`Region`	Die AWS-Region, die dem Ereignis zugeordnet ist.

CloudWatch Protokolle für Amazon Chime

Sie können Amazon Chime Voice Connector-Metriken an CloudWatch Logs senden. Weitere Informationen finden Sie unter Bearbeiten der Amazon Chime Voice Connector-Einstellungen im Amazon Chime SDK-Administrationshandbuch.

Metrikprotokolle der Medienqualität

Sie können sich dafür entscheiden, Metrikprotokolle in Medienqualität für Ihren Amazon Chime Voice Connector zu erhalten. Wenn Sie dies tun, sendet Amazon Chime detaillierte Metriken pro Minute für all Ihre Amazon Chime Voice Connector-Anrufe an eine CloudWatch Protokollgruppe, die für Sie erstellt wurde. Der Name der Protokollgruppe lautet `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. Die folgenden Felder sind in den Protokollen im JSON-Format enthalten.

Feld	Beschreibung
voice_connector_id	Die Amazon Chime Voice Connector-ID, die den Anruf weiterleitet.
event_timestamp	Die Zeitpunkt, zu dem die Metriken emittiert werden, angegeben in Millisekunden seit der UNIX-Epoche (Mitternacht am 1. Januar 1970) in UTC.
call_id	Entspricht der Transaktions-ID.

Feld	Beschreibung
from_sip_user	Der einleitende Benutzer des Anrufs.
from_country	Das einleitende Land des Anrufs.
to_sip_user	Der empfangende Benutzer des Anrufs.
to_country	Das empfangende Land des Anrufs.
Endpoint_id	Ein undurchsichtiger Bezeichner, der den anderen Endpunkt des Anrufs angibt. Verwenden Sie es mit CloudWatch Logs Insights. Weitere Informationen finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.
aws_region	Die AWS-Region für den Anruf.
cust2vc_rtp_packets	Die Anzahl der RTP-Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden.
cust2vc_rtp_bytes	Die Anzahl der vom Kunden gesendeten Bytes.
cust2vc_rtcp_packets	Die Anzahl der RTCP-Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden.
cust2vc_rtcp_bytes	Die Anzahl der vom Kunden gesendeten Bytes.
cust2vc_packets_lost	Die Anzahl der Pakete, die bei der Übertragung vom Kunden zur Amazon Chime Voice Connector-Infrastruktur verloren gegangen sind.

Feld	Beschreibung
cust2vc_jitter	Der durchschnittliche Jitter für Pakete, die vom Kunden an die Amazon Chime Voice Connector-Infrastruktur gesendet werden.
vc2cust_rtp_packets	Die Anzahl der RTP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet wurden.
vc2cust_rtp_bytes	Die Anzahl der Bytes Amazon Chime die in RTP-Paketen gesendet werden.
vc2cust_rtcp_packets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet wurden.
vc2cust_rtcp_bytes	Die Anzahl der Bytes Amazon Chime in RTCP-Paketen gesendet werden.
vc2cust_packets_lost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime Voice Connector-Infrastruktur zum Kunden verloren gegangen sind.
vc2cust_jitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an den Kunden gesendet werden.
rtt_btwn_vc_und_cust	Die durchschnittliche Hin- und Rückflugzeit zwischen dem Kunden und der Amazon Chime Voice Connector-Infrastruktur.
mos_btwn_vc_and_cust	Der geschätzte Mean Opinion Score (MOS) für Sprachstreams zwischen dem Kunden und der Amazon Chime Voice Connector-Infrastruktur.

Feld	Beschreibung
rem2vc_rtp_packets	Die Anzahl der RTP-Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden.
rem2vc_rtp_bytes	Die Anzahl der vom Remote-Ende gesendeten Bytes.
rem2vc_rtcp_packets	Die Anzahl der RTCP-Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet wurden.
rem2vc_rtcp_bytes	Die Anzahl der vom Remote-Ende gesendeten Bytes.
rem2vc_packets_lost	Die Anzahl der Pakete, die bei der Übertragung vom Remote-Ende zur Amazon Chime Voice Connector-Infrastruktur verloren gegangen sind.
rem2vc_jitter	Der durchschnittliche Jitter für Pakete, die vom Remote-Ende an die Amazon Chime Voice Connector-Infrastruktur gesendet werden.
vc2rem_rtp_packets	Die Anzahl der RTP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden.
vc2rem_rtp_bytes	Die Anzahl der Bytes Amazon Chime werden in RTP-Paketen gesendet.
vc2rem_rtcp_packets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden.
vc2rem_rtcp_bytes	Die Anzahl der Bytes Amazon Chime die in RTCP-Paketen gesendet werden.

Feld	Beschreibung
vc2rem_packets_lost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime Voice Connector-Infrastruktur zum Remote-Ende verloren gegangen sind.
vc2rem_jitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime Voice Connector-Infrastruktur an das Remote-Ende gesendet werden.
rtt_btwn_vc_and_rem	Die durchschnittliche Hin- und Rückflugzeit zwischen dem Remote-Ende und der Amazon Chime Voice Connector-Infrastruktur.
mos_btwn_vc_and_rem	Der geschätzte Mean Opinion Score (MOS) für Sprachstreams zwischen dem Remote-Ende und der Amazon Chime Voice Connector-Infrastruktur.

SIP-Nachrichtenprotokolle

Sie können sich dafür entscheiden, SIP-Nachrichtenprotokolle für Ihren Amazon Chime Voice Connector zu erhalten. Wenn Sie dies tun, erfasst Amazon Chime eingehende und ausgehende SIP-Nachrichten und sendet sie an eine CloudWatch Protokollgruppe, die für Sie erstellt wurde. Der Name der Protokollgruppe lautet `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. Die folgenden Felder sind in den Protokollen im JSON-Format enthalten.

Feld	Beschreibung
voice_connector_id	Die Amazon Chime Voice Connector ID.
aws_region	Die AWS-Region, die dem Ereignis zugeordnet ist.
event_timestamp	Der Zeitpunkt, zu dem die Nachricht erfasst wird, in Millisekunden seit der UNIX-Epoche (Mitternacht am 1. Januar 1970) in UTC.

Feld	Beschreibung
call_id	Die Amazon Chime Voice Connector.
sip_message	Die vollständige SIP-Nachricht, die erfasst wird.

Automatisierung von Amazon Chime mit EventBridge

EventBridge Mit Amazon können Sie IhreAWS -Services automatisieren und automatisch auf Systemereignisse reagieren, z. B. bei Problemen mit der Anwendungsverfügbarkeit oder Ressourcenänderungen. Weitere Informationen zu den Besprechungsereignissen finden Sie unter Besprechungsereignisse im Amazon Chime Developer Guide.

Wenn Amazon Chime Ereignisse generiert, werden sie an EventBridge die Best-Effort-Zustellung gesendet. Das bedeutet, Amazon Chime versucht, alle Ereignisse an einen Initiator zu senden EventBridge, aber in seltenen Fällen wird ein Ereignis möglicherweise nicht zugestellt. Weitere Informationen finden Sie unter Events fromAWS services im EventBridge Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie Daten verschlüsseln müssen, müssen Sie Amazon S3-Managed Keys verwenden. Wir unterstützen keine serverseitige Verschlüsselung mit Kundenmasterschlüsseln, die imAWS Key Management Service gespeichert sind.

Automatisieren von Amazon Chime Voice Connectors mit EventBridge

Zu den Aktionen, die automatisch Amazon Chime können, gehören folgende:

- Aufrufen einer AWS Lambda-Funktion
- Starten einer Amazon Elastic Container Service Aufgabe
- Weiterleiten Amazon Kinesis Video Streams
- Aktivieren eines AWS Step Functions-Zustandsautomaten
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

Einige Beispiele für die Verwendung EventBridge mit Amazon Chime Voice Connectors sind:

- Aktivierung einer Lambda-Funktion, um Audio für einen Anruf herunterzuladen, nachdem der Anruf beendet wurde.
- Starten einer Amazon ECS-Aufgabe, um die Transkription in Echtzeit zu aktivieren, nachdem ein Anruf gestartet wurde.

Weitere Informationen finden Sie im Amazon EventBridge Benutzerhandbuch.

Amazon Chime Voice Connector

Amazon Chime Voice Connectors unterstützen das Senden von Ereignissen an den EventBridge Zeitpunkt, an dem die in diesem Abschnitt beschriebenen Ereignisse eintreten.

Amazon Chime Voice Connector wird gestartet

Amazon Chime Voice Connectors senden dieses Ereignis, wenn das Medienstreaming an Kinesis Video Streams gestartet wird.

Example Ereignisdaten

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.


```
{
    "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"
    }
}
```

Amazon Chime Voice Connector wird beendet

Amazon Chime Voice Connectors senden dieses Ereignis, wenn das Medienstreaming an Kinesis Video Streams endet.

Example Ereignisdaten

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "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"
    }
}
```

Streaming-Updates

Amazon Chime Voice Connectors senden dieses Ereignis, wenn das Medienstreaming an Kinesis Video Streams aktualisiert wird.

Example Ereignisdaten

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "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"
    }
}
```

Das Amazon Chime Voice Connector schlägt fehl

Amazon Chime Voice Connectors senden dieses Ereignis, wenn das Medienstreaming zu Kinesis Video Streams fehlschlägt.

Example Ereignisdaten

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
  "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"
  }
}
```

Protokollieren von Amazon Chime API-Aufrufen mitAWS CloudTrail

Amazon Chime ist in einen Service integriertAWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS -Service in Amazon Chime durchgeführten Aktionen bietet. CloudTrail erfasst alle API-Aufrufe für Amazon Chime als Ereignisse, einschließlich Aufrufen von der Amazon Chime Konsole und von Code-Aufrufen an die Amazon Chime APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignissen für Amazon Chime, aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an Amazon Chime gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

Informationen zu Amazon Chime in CloudTrail

CloudTrail wird beim Erstellen IhresAWS -Kontos aktiviert. Wenn API-Aufrufe von der Amazon Chime-Verwaltungskonsole gestellt werden, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderenAWS -Service-Ereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung der Ereignisse in IhremAWS Konto, einschließlich Ereignissen für Amazon Chime, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von -Protokolldateien in einem Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt

dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail von CloudTrail -Protokolldateien aus mehreren Konten

Alle Amazon Chime-Aktionen werden von der Amazon Chime API-Referenz protokolliert CloudTrail und sind dort dokumentiert. Beispielsweise generieren Aufrufe der`ResetPersonalPIN` Abschnitte`CreateAccount`,`InviteUsers` und Einträge in den CloudTrail Protokolldateien. Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen von ausgeführt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Erläuterungen der Amazon Chime Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Einträge für Amazon Chime werden durch die Ereignisquelle chime.amazonaws.com identifiziert.

Wenn Sie Active Directory für Ihr Amazon Chime-Konto konfiguriert haben, finden Sie weitere Informationen unter Protokollieren von AWS Directory Service Service-API-Aufrufen mithilfe

CloudTrail. Hier wird beschrieben, wie Sie auf Probleme achten können, die sich auf die Anmeldefähigkeit Ihrer Amazon Chime-Benutzer auswirken könnten.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag für 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"
```

```
    }
```

Konformitätsprüfung für Amazon Chime

Externe Prüfer bewerten die Sicherheit und Konformität von AWS Services im Rahmen mehrerer AWS Compliance-Programme wie SOC, PCI, FedRAMP und HIPAA.

Informationen darüber, ob ein in den Geltungsbereich bestimmter Compliance-Programme AWS-Service fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-ProgrammAWS-Services . Wählen Sie aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National

Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.

- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in Amazon Chime

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Amazon Chime verschiedene Funktionen zur Unterstützung Ihrer Datenstabilität und Backup-Anforderungen. Weitere Informationen finden Sie unter Amazon Chime Voice Connector-Gruppen verwalten und Amazon Chime Voice Connector-Medien an Kinesis streamen im Amazon Chime SDK-Administrationshandbuch.

Infrastruktursicherheit in Amazon Chime

Als verwalteter Service ist Amazon Chime durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Grundlegendes zu automatischen Updates von Amazon Chime

Amazon Chime bietet verschiedene Möglichkeiten, seine Clients zu aktualisieren. Die Methode variiert, je nachdem, ob Ihre Benutzer Amazon Chime in einem Browser, auf Ihrem Desktop oder auf einem Mobilgerät ausführen.

Die Amazon Chime Chime-Webanwendung — https://app.chime.aws — wird immer mit den neuesten Funktionen und Sicherheitsupdates geladen.

Der Amazon Chime Chime-Desktop-Client sucht immer dann nach Updates, wenn ein Benutzer „Beenden“ oder „Abmelden“ wählt. Dies gilt für Windows- und MacOS-Computer. Wenn Benutzer den Client ausführen, sucht er alle drei Stunden nach Updates. Benutzer können auch nach Updates suchen, indem sie im Windows-Hilfemenü oder im macOS Amazon Chime-Menü die Option Nach Updates suchen wählen.

Wenn der Desktop-Client ein Update erkennt, fordert Amazon Chime die Benutzer auf, es zu installieren, sofern sie sich nicht in einem laufenden Meeting befinden. Benutzer nehmen an einem laufenden Meeting teil, wenn:

- Sie nehmen an einer Besprechung teil.
- Sie wurden zu einem Treffen eingeladen, das noch nicht abgeschlossen ist.

Amazon Chime fordert sie auf, die neueste Version zu installieren, und gibt ihnen einen 15-Sekunden-Countdown, damit sie die Installation verschieben können. Wählen Sie Später testen, um das Update zu verschieben.

Wenn Benutzer ein Update verschieben und sie nicht an einem laufenden Meeting teilnehmen, sucht der Client nach drei Stunden nach dem Update und fordert sie erneut auf, es zu installieren. Die Installation beginnt, wenn der Countdown endet.

> **Note**
>
> Auf einem macOS-Computer müssen Benutzer „Jetzt neu starten“ wählen, um mit dem Update zu beginnen.

Auf einem Mobilgerät — Die mobilen Amazon Chime Chime-Anwendungen verwenden die vom App Store und Google Play bereitgestellten Aktualisierungsoptionen, um die neueste Version des Amazon Chime Chime-Clients bereitzustellen. Sie können Updates auch über Ihr Mobilgeräte-Managementsystem verteilen. In diesem Thema wird davon ausgegangen, dass Sie wissen, wie.

Dokumentenverlauf für Amazon Chime

In der folgenden Tabelle werden wichtige Änderungen am Amazon Chime Chime-Administratorhandbuch beschrieben, die im März 2018 beginnen. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Amazon Chime SDK-Administrationshandbuch veröffentlicht	Die Amazon Chime SDK-Themen sind jetzt im Amazon Chime SDK Administration Guide veröffentlicht. Weitere Informationen finden Sie im Amazon Chime SDK Administration Guide.	24. März 2022
Aktualisierungen der IAM-Richtlinien	Änderungen an IAM-Richtlinien, die von verwaltet werden, AWS werden jetzt in diesem Administratorhandbuch nachverfolgt. Sehen Sie sich Beispiele für identitätsbasierte Richtlinien von Amazon Chime an.	23. September 2021
Serviceverknüpfte Rollen	Administratoren können jetzt servicebezogene Rollen für Amazon Live Transcription erstellen und Ereignismeldungen anzeigen, wenn ein Amazon Chime Chime-Live-Transkriptionsvorgang beginnt und endet. Weitere Informationen finden Sie unter Rollen mit Live-Transkription verwenden und Amazon Chime mit Ereigniss	12. August 2021

	en automatisieren. CloudWatch	
SIP-Medienanwendungen und Regeln	Administratoren können SIP-Medienanwendungen und Regeln für die Verwendung mit Amazon Chime Voice Connector und AWS Lambda Funktionen erstellen. Weitere Informationen finden Sie unter Verwaltung von SIP-Anwendungen und -Regeln im Amazon Chime Chime-Administratorhandbuch.	18. November 2020
Notruf-Routing-Nummern für Amazon Chime Voice Connector	Amazon Chime-Administratoren können Notruf-Routing-Nummern für einen Amazon Chime Voice Connector einrichten. Weitere Informationen finden Sie unter Einrichten von Notruf-Routing-Nummern für Ihren Amazon Chime Voice Connector im Amazon Chime Chime-Administratorhandbuch.	1. Juli 2020

Amazon Chime auf Dolby Voice Huddle	Amazon Chime bietet ein systemeigenes Meeting-Erlebnis oder ein First-Party-Meeting-Erlebnis auf Dolby Voice Huddle Audio- und Videokonferenzhardware. Weitere Informationen finden Sie unter Einrichten von Amazon Chime auf Dolby-Hardware im Amazon Chime Chime-Administratorhandbuch.	3. Juni 2020
Richtlinien zur Aufbewahrung von Chats festlegen	Amazon Chime Chime-Administratoren können Richtlinien zur Chat-Aufbewahrung für ihre Enterprise-Konten festlegen. Weitere Informationen finden Sie unter Verwaltung von Chat-Aufbewahrungsrichtlinien im Amazon Chime Chime-Administratorhandbuch.	21. Mai 2020
Chat-Nachrichten entfernen	Wenn Sie programmieren können, können Sie zwei Amazon Chime Chime-APIs verwenden, um Nachrichten aus den Chatrooms und Konversationen in Ihrem Konto zu entfernen. Weitere Informationen finden Sie unter Löschen einzelner Nachrichten im Amazon Chime Chime-Administratorhandbuch.	18. Mai 2020

CloudWatch Kennzahlen zur Medienqualität für Amazon Chime Voice Connector	Amazon Chime unterstützt das Senden von Medienqualitätsmetriken für Ihren Amazon Chime Voice Connector an. CloudWatch Weitere Informationen finden Sie unter Amazon Chime Monitoring with CloudWatch im Amazon Chime Chime-Administratorhandbuch.	23. Januar 2020
Amazon Chime Meetings-App für Slack	Amazon Chime unterstützt die Amazon Chime Meetings-App für Slack. Weitere Informationen finden Sie unter Einrichtung der Amazon Chime Meetings-App für Slack im Amazon Chime Chime-Administratorhandbuch.	4. Dezember 2019
Einstellungen für die Meeting-Region	Amazon Chime unterstützt die Bearbeitung von Besprechungen in der optimalen AWS Region für alle Teilnehmer. Weitere Informationen finden Sie unter Einstellungen für die Meeting-Region im Amazon Chime Chime-Administratorhandbuch.	3. Dezember 2019

Kompatibilität mit SIP-basierter Medienaufzeichnung (SIPREC)	Amazon Chime Voice Connectors unterstützen das Streamen von Medien von einer SIPREC-kompatiblen Sprachinfrastruktur zu Kinesis Video Streams. Weitere Informationen finden Sie unter Kompatibilität mit SIP-basierter Medienaufzeichnung (SIPREC) im Amazon Chime Chime-Administratorhandbuch.	25. November 2019
Amazon Chime auf Dolby Voice Room	Wenn Sie möchten, dass Benutzer bequem an Besprechungen teilnehmen können, bietet Amazon Chime ein systemeigenes Meeting-Erlebnis oder ein First-Party-Meeting-Erlebnis auf Dolby Voice Room-Audio- und Videokonferenzhardware. Weitere Informationen finden Sie unter Einrichten von Amazon Chime in Dolby Voice Room im Amazon Chime Chime-Administratorhandbuch.	29. Oktober 2019

Namen ausgehender Anrufe aktualisieren	Legen Sie einen Standardanrufnamen fest, der Empfängern von ausgehenden Anrufen angezeigt wird, die mit Telefonnummern in Ihrem Amazon Chime-Inventar getätigt wurden. Weitere Informationen finden Sie unter Aktualisieren der Namen ausgehender Anrufe im Amazon Chime Chime-Administratorhandbuch.	24. Oktober 2019
Medien zu Amazon Kinesis streamen	Streamen Sie Telefonanruf-Audio von Amazon Chime Voice Connectors zu Kinesis Video Streams für Analysen, maschinelles Lernen und andere Verarbeitungsvorgänge. Weitere Informationen finden Sie unter Streaming von Amazon Chime Voice Connector-Medien an Kinesis und Verwenden der serviceverknüpften Rolle Amazon Chime Voice Connector im Amazon Chime Chime-Administratorhandbuch.	24. Oktober 2019

Überwachung von Amazon Chime mit Amazon CloudWatch	Überwachen Sie Amazon Chime mithilfe von Amazon Chime CloudWatch, das Rohdaten sammelt und zu lesbaren Metriken nahezu in Echtzeit verarbeitet. Weitere Informationen finden Sie unter Amazon Chime Monitoring with CloudWatch im Amazon Chime Chime-Administratorhandbuch.	24. Oktober 2019
Amazon Chime Voice Connector-Gruppen	Erstellen Sie eine Amazon Chime Voice Connector-Gruppe, die Amazon Chime Voice Connectors enthält, die in verschiedenen AWS Regionen erstellt wurden. Auf diese Weise können eingehende Anrufe über Regionen hinweg ein Failover durchführen, wodurch ein fehlertoleranter Mechanismus für Fallback bei Verfügbarkeitsereignissen erstellt wird. Weitere Informationen finden Sie unter Arbeiten mit Amazon Chime Voice Connector-Gruppen im Amazon Chime Chime-Administratorhandbuch.	24. Oktober 2019

Aktualisierungen der Netzwerkkonfiguration	Amazon Chime vereinfacht seine Firewall-Anforderungen. Weitere Informationen finden Sie unter Netzwerkkonfiguration und Bandbreitenanforderungen im Amazon Chime Chime-Administratorhandbuch.	6. September 2019
Moderierte Besprechungen	Amazon Chime unterstützt moderierte Besprechungen. Weitere Informationen finden Sie unter Teilnehmen an einem moderierten Meeting im Amazon Chime Chime-Administratorhandbuch.	25. Juli 2019
Konformitätsprüfung für Amazon Chime	Amazon Chime ist ein HIPAA-fähiger Service. Weitere Informationen finden Sie unter Konformitätsprüfung für Amazon Chime im Amazon Chime Chime-Administratorhandbuch.	11. Juni 2019
Portierung gebührenfreier Telefonnummern	Amazon Chime unterstützt die Portierung gebührenfreier US-Telefonnummern zur Verwendung mit Amazon Chime Voice Connectors. Weitere Informationen finden Sie unter Portierung vorhandener Telefonnummern im Amazon Chime Chime-Administratorhandbuch.	28. Mai 2019

Verwaltung von Telefonnummern in Amazon Chime	Verwenden Sie Amazon Chime Business Calling, um Amazon Chime Chime-Benutzern Telefonnummern bereitzustellen und zuzuweisen. Integrieren Sie einen Amazon Chime Voice Connector in ein vorhandenes Telefonsystem. Weitere Informationen finden Sie unter Verwaltung von Telefonnummern in Amazon Chime im Amazon Chime Chime-Administratorhandbuch.	18. März 2019
Amazon Chime Chime-Zusatzmodul für Outlook	Amazon Chime bietet zwei Add-Ins für Microsoft Outlook: das Amazon Chime Add-In für Outlook unter Windows und das Amazon Chime Add-In für Outlook. Mit diesen Add-ins werden die gleichen Zeitplanungsfunktionen verfügbar, sie unterstützen jedoch Benutzer unterschiedlicher Typen. Weitere Informationen finden Sie unter Deployment the Add-In for Outlook im Amazon Chime Chime-Administratorhandbuch.	12. März 2019
Verschiedene Updates	Verschiedene Updates zum Layout und zur Organisation der Themen.	11. Februar 2019

Amazon Chime Chime-Funktion „Mich anrufen“	Administratoren können die Amazon Chime-Call-Me-Funktion in ihren Meetings-Einstellungen aktivieren. Weitere Informationen finden Sie unter Verwaltung der Meeting-Einstellungen im Amazon Chime Chime-Administratorhandbuch.	22. August 2018
Connect zu Okta SSO her	Wenn Sie über ein Enterprise-Konto verfügen, können Sie zum Authentifizieren und Zuweisen von Benutzerberechtigungen eine Verbindung mit Okta-SSO herstellen. Weitere Informationen finden Sie unter Connect to Okta SSO im Amazon Chime Chime-Administratorhandbuch.	1. August 2018
Benutzeranhänge anfordern	Empfangen Sie Anlagen, die von Benutzern in Amazon Chime hochgeladen wurden. Weitere Informationen finden Sie unter Benutzeranhänge anfordern im Amazon Chime Chime-Administratorhandbuch.	23. April 2018
Zusätzliche Berichtsdaten anzeigen	Anzeigen zusätzlicher Berichtsdaten. Weitere Informationen finden Sie unter Berichte anzeigen im Amazon Chime Chime-Administratorhandbuch.	30. März 2018

Weisen Sie Benutzern Pro- oder Basic-Berechtigungen zu	Zuweisen von Pro- oder Basic-Berechtigungen. Weitere Informationen finden Sie unter Benutzerzugriff und Benutzerberechtigungen verwalten im Amazon Chime Chime-Administratorhandbuch.	29. März 2018