aws

Administratorhandbuch

Amazon Chime SDK

Amazon Chime SDK: Administratorhandbuch

Table of Contents

Was ist das Amazon Chime SDK?

Das Amazon Chime SDK bietet eine Reihe von Echtzeit-Kommunikationskomponenten, mit denen Entwickler ihren Web- oder mobilen Anwendungen Messaging-, Audio-, Video- und Bildschirmfreigabefunktionen hinzufügen können. Entwickler können beispielsweise Videos zu einer Zustandsanwendung hinzufügen, sodass Patienten remote mit Patienten zu Zustandsproblemen sprechen oder benutzerdefinierte Audioansagen für die Integration in ein öffentliches Telefonnetz (PSTN) erstellen können. Durch die Verwendung des Amazon Chime SDK können Entwickler dazu beitragen, die Kosten, Komplexität und den Aufwand für die Erstellung und Wartung ihrer eigenen Infrastruktur und Services für die Kommunikation in Echtzeit zu beseitigen.

Weitere Informationen finden Sie auf der Seite AWS Amazon Chime SDK.

Preisgestaltung

Das Amazon Chime SDK bietet pay-for-use Preise ohne Vorabgebühren. Entwickler, die das SDK implementieren, können einige oder alle verfügbaren Medienmodalitäten (Audio, Video und Bildschirmfreigabe) mit einer einzigen Rate implementieren. Messaging-, Medienpipelines-, Sprachverbesserungs- und PSTN-Audiofunktionen sind ebenfalls mit - pay-for-use Preisen verfügbar. Weitere Informationen finden Sie unter Amazon Chime SDK – Preise.

Voraussetzungen

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

Ein Amazon Web Services Services-Konto erstellen

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

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.

Sicherheit im Amazon Chime SDK

Cloud-Sicherheit hat AWS 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 das Amazon Chime SDK 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 des Amazon Chime SDK anwenden können. In den folgenden Themen erfahren Sie, wie Sie das Amazon Chime SDK konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Amazon Chime SDK-Ressourcen überwachen und sichern können.

Themen

Identitäts- und Zugriffsmanagement für das Amazon Chime SDK

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 SDK-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

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

Servicebenutzer — Wenn Sie den Amazon Chime SDK-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 SDK-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 im Amazon Chime SDK nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf das Amazon Chime SDK.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Chime SDK-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf das Amazon Chime SDK. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen des Amazon Chime SDK Ihre

Mitarbeiter 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 dem Amazon Chime SDK verwenden kann, finden Sie unter. So funktioniert das Amazon Chime SDK 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 das Amazon Chime SDK zu verwalten. Beispiele für identitätsbasierte Amazon Chime SDK-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Chime SDK

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, in Kombination 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.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — 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 auf was Zugriff 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 das Amazon Chime SDK

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst 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 allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

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 `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. 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 das Amazon Chime SDK mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf das Amazon Chime SDK zu verwalten, sollten Sie sich mit den IAM-Funktionen vertraut machen, die für die Verwendung mit dem Amazon Chime SDK verfügbar sind. Einen allgemeinen Überblick darüber, wie das Amazon Chime SDK und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren.

Themen

- Identitätsbasierte Amazon Chime SDK-Richtlinien
- Ressourcen
- Beispiele

Identitätsbasierte Amazon Chime SDK-Richtlinien

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. Das Amazon Chime SDK 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.

Weitere Informationen zu Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Chime in der Service Authorization Reference.

Bedingungsschlüssel

Das Amazon Chime SDK bietet eine Reihe von dienstspezifischen Bedingungsschlüsseln. Weitere Informationen finden Sie unter Bedingungsschlüssel für Amazon Chime in der Service Authorization Reference.

Ressourcen

Das Amazon Chime SDK unterstützt die Angabe von Ressourcen-ARNs in einer Richtlinie. Weitere Informationen finden Sie unter Von Amazon Chime definierte Ressourcentypen

Beispiele

Beispiele für identitätsbasierte Amazon Chime SDK-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Chime SDK

Verschlüsselung mit Sprachanalyse verwenden

Amazon Chime SDK Voice Analytics speichert die Audiodateien, die zur Generierung der Spracheinbettung verwendet werden. Die Dateien werden mit einem symmetrischen, vom Kunden verwalteten Schlüssel verschlüsselt, den Sie erstellen, besitzen und verwalten. Da Sie die volle

Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Weitere Informationen finden Sie unter Vom Kunden verwaltete Schlüssel im AWS Key Management Service Developer Guide.

Grundlegendes zur Verschlüsselung im Ruhezustand

Standardmäßig verschlüsselt Voice Analytics alle Benutzerdaten im Ruhezustand. Wenn Sie eine neue Sprachprofil-Domain erstellen, müssen Sie einen symmetrischen, vom Kunden verwalteten Schlüssel angeben, den der Dienst zur Verschlüsselung Ihrer Daten im Ruhezustand verwendet. Sie besitzen, verwalten und kontrollieren den Schlüssel.

Der Schlüssel verschlüsselt nur die Audiodateien, die zur Registrierung von Lautsprechern für Spracheinbettungen verwendet werden.

Die Sprachanalyse greift auf den Schlüssel zu, indem Zuschüsse erstellt werden. Weitere Informationen zu Zuschüssen finden Sie im nächsten Abschnitt.

Verstehen Sie, wie Voice Analytics Zuschüsse verwendet

Für Sprachanalysen ist ein Zuschuss für die Nutzung Ihres vom Kunden verwalteten Schlüssels erforderlich. Wenn Sie eine Sprachprofil-Domain erstellen, erstellt der zugehörige Amazon Chime SDK Voice Connector in Ihrem Namen einen Zuschuss, indem er eine `CreateGrant` Anfrage an den AWS KMS sendet. Der Zuschuss ist erforderlich, um Ihren Schlüssel für die folgenden internen Operationen verwenden zu können:

- Senden von DescribeKeyAnfragen an AWS KMS, um zu überprüfen, ob die angegebene symmetrische, vom Kunden verwaltete Schlüssel-ID gültig ist.

- Senden von GenerateDataKeyAnfragen an den KMS-Schlüssel zur Erstellung von Datenschlüsseln, mit denen Objekte verschlüsselt werden können.
- Senden von DecryptAnfragen an AWS KMS zur Entschlüsselung der verschlüsselten Datenschlüssel, sodass diese zur Verschlüsselung Ihrer Daten verwendet werden können.
- Senden von RetireGrantAnfragen an AWS KMS, um die für eine Sprachprofildomäne verwendeten Zuschüsse zurückzuziehen.
- Speichern von Dateien in Amazon S3 mit serverseitiger Verschlüsselung.

Sie können den Zugriff auf den Grant jederzeit widerrufen oder dem Service den Zugriff auf Ihren Schlüssel entziehen. Wenn Sie dies tun, kann Voice Analytics nicht auf die mit dem Schlüssel verschlüsselten Daten zugreifen. Das wirkt sich auf alle Operationen aus, die von diesen Daten abhängen, und führt zu `AccessDeniedException` Fehlern und Ausfällen in den Workflows zur Lautsprechersuche.

Wichtige Richtlinie für Sprachanalysen

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine wichtige Richtlinie verfügen, mit Richtlinienerklärungen, die festlegen, wer den Schlüssel verwenden darf und wie er verwendet werden darf. Wenn Sie Ihren Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Arbeiten mit wichtigen Richtlinien im AWS Key Management Service Developer Guide.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow key access to Amazon Chime SDK voice analytics.",
            "Effect": "Allow",
            "Principal": {
                "AWS": "your_user_or_role_ARN"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": [
                        "chimevoiceconnector.region.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie unter Angabe von KMS-Schlüsseln in IAM-Richtlinienerklärungen im AWS Key Management Service Developer Guide.

Informationen zur Problembehandlung beim Schlüsselzugriff finden Sie unter Problembehandlung beim Schlüsselzugriff im AWS Key Management Service Developer Guide.

Verschlüsselungskontext verwenden

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten. AWS KMS verwendet den Verschlüsselungskontext, um authentifizierte Verschlüsselung zu unterstützen.

Wenn Sie einen Verschlüsselungskontext in eine Verschlüsselungsanforderung aufnehmen, bindet AWS KMS den Verschlüsselungskontext an die verschlüsselten Daten. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

Voice Analytics verwendet bei allen kryptografischen Vorgängen von AWS KMS denselben Verschlüsselungskontext, wobei der Schlüssel `aws:chime:voice-profile-domain:arn` und der Wert die Ressource Amazon Resource Name (ARN) ist.

Das folgende Beispiel zeigt einen typischen Verschlüsselungskontext.

```
"encryptionContext": {
    "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-west-2:111122223333:voice-profile-domain/sample-domain-id"
}
```

Sie können den Verschlüsselungskontext auch in Prüfaufzeichnungen und Protokollen verwenden, um festzustellen, wie der vom Kunden verwaltete Schlüssel verwendet wird. Der

Verschlüsselungskontext erscheint auch in Protokollen, die von CloudTrail oder CloudWatch Logs generiert wurden.

Verwenden Sie den Verschlüsselungskontext, um den Zugriff auf Ihren Schlüssel zu kontrollieren

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen verwenden, um den Zugriff auf Ihren symmetrischen, vom Kunden verwalteten Schlüssel zu kontrollieren. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

Voice Analytics verwendet eine Einschränkung des Verschlüsselungskontextes bei Zuschüssen, um den Zugriff auf die vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu kontrollieren. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Das folgende Beispiel für wichtige Richtlinienerklärungen gewährt Zugriff auf einen vom Kunden verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in der Grundsatzerklärung erfordert, dass die Zuschüsse über eine Einschränkung des Verschlüsselungskontextes verfügen, die den Verschlüsselungskontext spezifiziert.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},
{
    "Sid": "Enable CreateGrant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:chime:voice-profile-domain:arn":
 "arn:aws:chime:us-west-2:111122223333:voice-profile-domain/sample-domain-id"
```

```
        }
    }
}
```

Überwachen von Verschlüsselungsschlüsseln

Amazon Chime SDK Voice Connectors senden Anfragen an AWS KMS, und Sie können diese Anfragen in CloudTrail oder CloudWatch Protokollen verfolgen.

CreateGrant

Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, um eine Sprachprofil-Domain-Ressource zu erstellen, sendet der zugehörige Voice Connector in Ihrem Namen eine `CreateGrant` Anfrage, um auf den KMS-Schlüssel in Ihrem AWS Konto zuzugreifen. Der Zuschuss, den der Voice Connector gewährt, ist spezifisch für die Ressource, die dem vom Kunden verwalteten Schlüssel zugeordnet ist. Der Voice Connector verwendet den `RetireGrant` Vorgang auch, um einen Zuschuss zu entfernen, wenn Sie eine Ressource löschen.

Im folgenden Beispiel wird ein `CreateGrant` Vorgang aufgezeichnet.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
```

```
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
       "constraints": {
            "encryptionContextSubset": {
                "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
            }
        },
        "retiringPrincipal": "chimevoiceconnector.region.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt",
            "DescribeKey",
            "RetireGrant"
        ],
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "granteePrincipal": "chimevoiceconnector.region.amazonaws.com",
        "retiringPrincipal": "chimevoiceconnector.region.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

GenerateDataSchlüssel

Wenn Sie eine Sprachprofil-Domain erstellen und der Domain einen vom Kunden verwalteten Schlüssel zuweisen, erstellt der zugehörige Voice Connector einen eindeutigen Datenschlüssel, um die Audiodaten der einzelnen Sprecher bei der Registrierung zu verschlüsseln. Der Voice Connector sendet eine `GenerateDataKey` Anfrage an AWS KMS, in der der Schlüssel für die Ressource angegeben wird.

Das folgende Beispiel zeichnet einen `GenerateDataKey` Vorgang auf.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

Wenn bei einem Stimmprofil in einer Sprachprofildomäne aufgrund eines neueren Spracherkennungsmodells die Sprachausgabe aktualisiert werden muss, ruft der zugehörige Voice Connector den `Decrypt` Vorgang auf, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf die verschlüsselten Daten zu verwenden.

Im folgenden Beispiel wird ein `Decrypt` Vorgang aufgezeichnet.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-10-12T23:59:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "keyId": "arn:aws:kms:us-
west-2:111122223333:key/44444444-3333-2222-1111-EXAMPLE11111",
            "encryptionContext": {
                "aws:chime:voice-profile-domain:arn": "arn:aws:chime:us-
west-2:111122223333:voice-profile-domain/sample-domain-id"
            },
            "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
        },
        "responseElements": null,
```

```
        "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
        "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
        "readOnly": true,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "sharedEventID": "35d58aa1-26b2-427a-908f-025bf71241f6",
        "eventCategory": "Management"
    }
```

DescribeKey

Voice Connectors verwenden den `DescribeKey` Vorgang, um zu überprüfen, ob der mit einer Sprachprofildomäne verknüpfte Schlüssel im Konto und in der Region vorhanden ist.

Im folgenden Beispiel wird ein `DescribeKey` Vorgang aufgezeichnet.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
```

```
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

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 die Verwendung des Kontextschlüssels „`aws:SourceAccount`Global Condition“ in Ihren Ressourcenrichtlinien. Diese Schlüssel schränken die Berechtigungen ein, die das Amazon Chime SDK 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 für Amazon Chime SDK

Das Amazon Chime SDK unterstützt ressourcenbasierte Richtlinien für die folgenden Ressourcentypen.

Autorisierung basierend auf Amazon Chime SDK-Tags

Das Amazon Chime SDK unterstützt Tagging für diese Ressourcentypen.

IAM-Rollen im Amazon Chime SDK

Eine IAM-Rolle ist eine Entität in Ihrem AWS -Konto mit spezifischen Berechtigungen.

Temporäre Anmeldeinformationen mit dem Amazon Chime SDK 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 GetFederationTokenaufrufen.

Das Amazon Chime SDK unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, 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.

Das Amazon Chime SDK unterstützt serviceverknüpfte Rollen. Einzelheiten zum Erstellen oder Verwalten dieser Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für das Amazon Chime SDK

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.

Das Amazon Chime SDK unterstützt keine Servicerollen.

Beispiele für identitätsbasierte Richtlinien für Amazon Chime SDK

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, Amazon Chime SDK-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 sind sehr leistungsfähig. Sie bestimmen, ob jemand Amazon Chime SDK-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 — Um schnell mit der Nutzung des Amazon Chime SDK zu beginnen, verwenden Sie AWS verwaltete Richtlinien, um Ihren Mitarbeitern die erforderlichen Berechtigungen zu erteilen. Diese Richtlinien sind bereits in Ihrem Konto verfügbar

und werden von AWS. Weitere Informationen finden Sie unter Erste Schritte zur Nutzung von Berechtigungen mit AWS verwalteten Richtlinien im IAM-Benutzerhandbuch.

- Gewähren von geringsten Rechten – Gewähren Sie beim Erstellen benutzerdefinierter Richtlinien nur die Berechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Beginnen Sie mit einem Mindestsatz von Berechtigungen und gewähren Sie zusätzliche Berechtigungen wie erforderlich. Dies ist sicherer, als mit Berechtigungen zu beginnen, die zu weit gefasst sind, und dann später zu versuchen, sie zu begrenzen. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.
- Aktivieren von MFA für sensible Vorgänge – Sie sollten die Verwendung der Multi-Faktor-Authentifizierung (MFA) von IAM-Benutzern fordern, um beim Zugriff auf sensible Ressourcen oder API-Operationen zusätzliche Sicherheit zu erhalten. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.
- Verwenden von Richtlinienbedingungen für zusätzliche Sicherheit – Definieren Sie die Bedingungen, unter denen Ihre identitätsbasierten Richtlinien den Zugriff auf eine Ressource zulassen, soweit praktikabel. Beispielsweise können Sie Bedingungen schreiben, die eine Reihe von zulässigen IP-Adressen festlegen, von denen eine Anforderung stammen muss. Sie können auch Bedingungen schreiben, die Anforderungen nur innerhalb eines bestimmten Datums- oder Zeitbereichs zulassen oder die Verwendung von SSL oder MFA fordern. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

AWS verwaltete Amazon Chime SDK-Richtlinie

Sie verwenden die AWS verwalteten AktionenAmazonChimeVoiceConnectorServiceLinkedRolePolicy, um Benutzern Zugriff auf Amazon Chime SDK zu gewähren. Weitere Informationen finden Sie unter Beispiele für IAM-Rollen im Amazon Chime SDK Developer Guide und Actions, resources, and condition keys for Amazon Chime in der Service Authorization Reference.

```
// Policy ARN: arn:aws:iam::aws:policy/AmazonChimeSDK
// Description: Provides access to Amazon Chime SDK operations
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:CreateMediaCapturePipeline",
                "chime:CreateMediaConcatenationPipeline",
```

```
                "chime:CreateMediaLiveConnectorPipeline",
                "chime:CreateMeeting",
                "chime:CreateMeetingWithAttendees",
                "chime:DeleteMediaCapturePipeline",
                "chime:DeleteMediaPipeline",
                "chime:DeleteMeeting",
                "chime:GetMeeting",
                "chime:ListMeetings",
                "chime:CreateAttendee",
                "chime:BatchCreateAttendee",
                "chime:DeleteAttendee",
                "chime:GetAttendee",
                "chime:GetMediaCapturePipeline",
                "chime:GetMediaPipeline",
                "chime:ListAttendees",
                "chime:ListAttendeeTags",
                "chime:ListMediaCapturePipelines",
                "chime:ListMediaPipelines",
                "chime:ListMeetingTags",
                "chime:ListTagsForResource",
                "chime:StartMeetingTranscription",
                "chime:StopMeetingTranscription",
                "chime:TagAttendee",
                "chime:TagMeeting",
                "chime:TagResource",
                "chime:UntagAttendee",
                "chime:UntagMeeting",
                "chime:UntagResource"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Das `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` ermöglicht Amazon Chime SDK Voice Connectors, Medien zu Amazon Kinesis Video Streams zu streamen, Streaming-Benachrichtigungen bereitzustellen und Sprache mithilfe von Amazon Polly zu synthetisieren. Diese Richtlinie gewährt dem Amazon Chime SDK Voice Connector-Service die Erlaubnis, auf die Amazon

Kinesis Video Streams des Kunden zuzugreifen, Benachrichtigungsereignisse an Amazon Simple Notification Service (SNS) und Amazon Simple Queue Service (SQS) zu senden und Amazon Polly zur Sprachsynthese zu verwenden, wenn die Amazon Chime SDK Sprachanwendungen und -aktionen verwendet werden. `Speak` `SpeakAndGetDigits`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["chime:GetVoiceConnector*"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:GetDataEndpoint",
                "kinesisvideo:PutMedia",
                "kinesisvideo:UpdateDataRetention",
                "kinesisvideo:DescribeStream",
                "kinesisvideo:CreateStream"
            ],
            "Resource": ["arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"]
        },
        {
            "Effect": "Allow",
            "Action": ["kinesisvideo:ListStreams"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": ["SNS:Publish"],
            "Resource": ["arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"]
        },
        {
            "Effect": "Allow",
            "Action": ["sqs:SendMessage"],
            "Resource": ["arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"]
        },
        {
            "Effect": "Allow",
            "Action": ["polly:SynthesizeSpeech"],
            "Resource": ["*"]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "chime:CreateMediaInsightsPipeline",
                "chime:GetMediaInsightsPipelineConfiguration"
            ],
            "Resource": ["*"]
        }
    ]
}
```

Weitere Informationen finden Sie unter Verwenden der Richtlinie für verknüpfte Rollen mit dem Amazon Chime SDK Voice Connector-Service.

AWS verwaltete Richtlinie: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Sie können die `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` nicht an Ihre IAM-Entitäten anhängen.

Diese Richtlinie ermöglicht es Kinesis Video Streams, Daten zu Amazon Chime SDK-Meetings zu streamen und Metriken zu veröffentlichen. CloudWatch Außerdem können Amazon Chime SDK-Medien-Pipelines in Ihrem Namen auf Amazon Chime SDK-Meetings zugreifen. Weitere Informationen finden Sie unter Rollen mit Amazon Chime SDK-Medien-Pipelines verwenden in diesem Handbuch.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `cloudwatch`— Erteilt die Erlaubnis zur Eingabe von Metriken. CloudWatch
- `kinesisvideo`— Erteilt Berechtigungen zum Abrufen von Datenendpunkten, zum Speichern von Medien, zum Aktualisieren von Datenaufbewahrungsintervallen, zum Beschreiben von Datenströmen, zum Erstellen von Datenströmen und zum Auflisten von Datenströmen.
- `chime`— Erteilt Berechtigungen zum Abrufen von Besprechungen, zum Erstellen von Teilnehmern und zum Löschen von Teilnehmern.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutMetricsForChimeSDKNamespace",
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/ChimeSDK"
                }
            }
        },
        {
            "Sid": "AllowKinesisVideoStreamsAccess",
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:GetDataEndpoint",
                "kinesisvideo:PutMedia",
                "kinesisvideo:UpdateDataRetention",
                "kinesisvideo:DescribeStream",
                "kinesisvideo:CreateStream"
            ],
            "Resource": [
                "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
            ]
        },
        {
            "Sid": "AllowKinesisVideoStreamsListAccess",
            "Effect": "Allow",
            "Action": [
                "kinesisvideo:ListStreams"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AllowChimeMeetingAccess",
            "Effect": "Allow",
            "Action": [
                "chime:GetMeeting",
                "chime:CreateAttendee",
                "chime:DeleteAttendee"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Chime Chime-Updates für AWS verwaltete Richtlinien

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

Änderung	Beschreibung	Datum
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` zusätzlichen Berechtigungen, die es Amazon Chime SDK-Meetings ermöglichen, Metriken CloudWatch zur Verwendung in Service-Dashboards zu veröffentlichen. Weitere Informationen finden Sie unter Rollen mit Amazon Chime SDK-Medien-Pipelines verwenden.	8. Dezember 2023
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` zusätzlichen Berechtigungen, die es Kinesis Video Streams ermöglichen, Audio-, Video- und Screenshare-Daten an Amazon Chime SDK-Meetings zu streamen. Weitere Informationen finden Sie unter Rollen	20. August 2023

Änderung	Beschreibung	Datum
	mit Amazon Chime SDK-Medien-Pipelines verwenden.	
AmazonChimeVoiceConnectorServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` hinzugefügten Berechtigungen, die den Zugriff auf die GetMediaInsightsPipelineConfiguration API ermöglichen. Amazon Chime Voice Connectors benötigen diese Berechtigungen, um Media Insights-Pipeline-Konfigurationen zu erhalten. Weitere Informationen finden Sie unter Konfiguration von Voice Connectors für die Verwendung von Anrufanalysen.	14. April 2023

Änderung	Beschreibung	Datum
Neue und aktualisierte Rollen, die mit dem Service verknüpft sind	Entwickler können die verknüpfte Rolle mit dem AmazonChime SDKEvents -Dienst verwenden, um auf Streaming-Dienste wie Kinesis Firehose zuzugreifen. Weitere Informationen finden Sie unter Verwenden der serviceverknüpften Rolle. AmazonChimeSDKEvents Wir haben den AmazonChimeVoiceConnectorServiceLinkedRolePolicyNamen auch zu Using service linked roles hinzugefügt. Weitere Informationen finden Sie unter Verwenden von AmazonChimeVoiceConnectorServiceLinkedRolePolicy.	27. März 2023
Beispiele für identitätsbasierte Amazon Chime SDK-Richtlinien — Aktualisierung einer bestehenden Richtlinie.	Die AWS verwaltete Amazon Chime SDK-Richtlinie fügte Berechtigungen hinzu, die es Ihnen ermöglichen, Amazon Chime SDK Media Pipeline-APIs zum Erstellen, Lesen und Löschen von Medien-Pipelines zu verwenden.	5. Januar 2023

Änderung	Beschreibung	Datum
Die AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy— neue verwaltete Richtlinie wurde hinzugefügt.	Das Amazon Chime SDK hat eine servicebezogene Rolle hinzugefügt, die es Ihnen ermöglicht, Medienerfassungspipelines in Amazon Chime SDK-Meetings zu verwenden.	27. April 2022
Von AWS verwaltete Richtlinie: AmazonChimeVoiceConnectorServiceLinkedRolePolicy — Aktualisierung einer bestehenden Richtlinie.	Amazon Chime SDK Voice Connectors hat 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

Änderung	Beschreibung	Datum
AmazonChimeVoiceConnectorServiceLinkedRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Amazon Chime SDK Voice Connector hat Berechtigungen hinzugefügt, die den Zugriff auf Amazon Kinesis Video Streams und das Senden von Benachrichtigungsereignissen an Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Query Service (Amazon SQS) ermöglichen. Diese Berechtigungen sind erforderlich, damit Amazon Chime SDK Voice Connectors Medien auf Amazon Kinesis Video Streams streamen und Streaming-Benachrichtigungen bereitstellen kann.	20. Dezember 2021
Änderung der bestehenden Richtlinie. IAM-Benutzer oder -Rollen mit der Chime SDK-Richtlinie erstellen.	Das Amazon Chime SDK hat neue Aktionen hinzugefügt, um die erweiterte Validierung zu unterstützen. Eine Reihe von Aktionen wurde hinzugefügt, um das Auflisten und Markieren von Teilnehmern und Meeting-Ressourcen sowie das Starten und Beenden der Meeting-Transkription zu ermöglichen.	23. September 2021
Das Amazon Chime SDK hat begonnen, Änderungen zu verfolgen	Das Amazon Chime SDK hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	23. September 2021

Fehlerbehebung bei Identität und Zugriff auf das Amazon Chime SDK

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

Themen

Ich bin nicht berechtigt, eine Aktion im Amazon Chime SDK 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 zur Ausführung von iam:PassRole autorisiert.

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat. Bitten Sie diese Person, Ihre Richtlinien zu aktualisieren, damit Sie eine Rolle an das Amazon Chime SDK übergeben können.

Einige AWS Dienste 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, den Service zu verwenden, um eine Aktion im Amazon Chime SDK auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Service-Rolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

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

In diesem Fall bittet Mary ihren Administrator um die Aktualisierung ihrer Richtlinien, um die Aktion `iam:PassRole` ausführen zu können.

Verwenden von serviceverknüpften Rollen für das Amazon Chime SDK

Das Amazon Chime SDK verwendet AWS Identity and Access Management (IAM) service-verknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit dem Amazon Chime SDK verknüpft ist. Servicebezogene Rollen sind vom Amazon Chime SDK vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle macht die Einrichtung des Amazon Chime SDK effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Das Amazon Chime SDK definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur das Amazon Chime SDK 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. Dadurch werden Ihre Amazon Chime SDK-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen 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 serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

Verwenden der Richtlinie für verknüpfte Rollen mit dem Amazon Chime SDK Voice Connector-Service

Die Informationen in den folgenden Abschnitten erläutern, wie Sie:

- Verwenden Sie die Richtlinie für verknüpfte Rollen mit dem Amazon Chime SDK Voice Connector-Service, um Amazon Chime SDK Voice Connector-Medien an Kinesis zu streamen.
- Synthetisieren Sie Sprache mit Amazon Polly und den Speak- und SpeakAndGetDigitsAktionen.

Themen

Servicebezogene Rollenberechtigungen für Amazon Chime SDK Voice Connectors

Amazon Chime SDK Voice Connectors verwenden die dienstbezogene Rolle mit dem Namen AWSServiceRoleForAmazonChimeVoiceConnector— Ermöglicht Amazon Chime SDK Voice Connectors, AWS Dienste in Ihrem Namen anzurufen. Weitere Informationen zum Starten des Medienstreamings für Ihren Amazon Chime SDK Voice Connector finden Sie unterAmazon Chime SDK Voice Connector-Medien an Kinesis streamen.

Die AWSServiceRoleForAmazonChimeVoiceConnector dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `voiceconnector.chime.amazonaws.com`

Das AmazonChimeVoiceConnectorServiceLinkedRolePolicyermöglicht dem Amazon Chime SDK, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `chime:GetVoiceConnector*` für `all AWS resources`
- Aktion: `kinesisvideo:*` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeVoiceConnector-*`
- Aktion: `polly:SynthesizeSpeech` für `all AWS resources`
- Aktion: `chime:CreateMediaInsightsPipeline` für `all AWS resources`
- Aktion: `chime:GetMediaInsightsPipelineConfiguration` für `all AWS resources`
- Aktion: `kinesisvideo:CreateStream` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:PutMedia` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:UpdateDataRetention` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:DescribeStream` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:GetDataEndpoint` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:ListStreams` für `arn:aws:kinesisvideo:us-east-1:111122223333:stream/*`

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

Eine serviceverknüpfte Rolle für Amazon Chime SDK Voice Connectors erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Kinesis Media Streaming für Ihren Amazon Chime SDK Voice Connector starten oder eine Amazon Chime SDK SIP-

Medienanwendung in der AWS Management Console, der oder der AWS API erstellen oder aktualisieren, erstellt Amazon Chime die serviceverknüpfte Rolle für Sie. AWS CLI

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

Bearbeiten einer serviceverknüpften Rolle für Amazon Chime SDK Voice Connectors

Das Amazon Chime SDK ermöglicht es Ihnen nicht, die AWSServiceRoleForAmazonChimeVoiceConnector 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 serviceverknüpften Rolle für Amazon Chime SDK Voice Connectors

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften 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 der Amazon Chime SDK-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Amazon Chime SDK-Ressourcen zu löschen, die von der AWSServiceRoleForAmazonChimeVoiceConnector (Konsole) verwendet werden

- Beenden Sie das Medienstreaming für alle Amazon Chime SDK Voice Connectors in Ihrem Amazon Chime SDK-Konto.

  a. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.

  b. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.

  c. Wählen Sie den Namen des Amazon Chime SDK Voice Connectors.

  d. Wählen Sie den Tab Streaming.

  e. Wählen Sie unter An Kinesis Video Streams senden die Option Stopp aus.

  f. Wählen Sie Speichern.

Um Amazon Chime SDK-Ressourcen zu löschen, die von der AWSServiceRoleForAmazonChimeVoiceConnector (AWS CLI) verwendet werden

- Verwenden Sie den `delete-voice-connector-streaming-configuration` Befehl in der AWS CLI, um das Medienstreaming für alle Amazon Chime SDK Voice Connectors in Ihrem Konto zu beenden.

```
aws chime delete-voice-connector-streaming-configuration --voice-connector-
id abcdef1ghij2klmno3pqr4
```

Um Amazon Chime SDK-Ressourcen zu löschen, die von der AWSServiceRoleForAmazonChimeVoiceConnector (API) verwendet werden

- Verwenden Sie die DeleteVoiceConnectorStreamingConfigurationAPI, um das Medienstreaming für alle Amazon Chime SDK Voice Connectors in Ihrem Konto zu beenden.

Manuelles Löschen der -serviceverknüpften Rolle

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

Unterstützte Regionen für serviceverknüpfte Amazon Chime SDK-Rollen

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

Verwenden von Rollen mit Live-Transkription

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

Themen

- Serviceverknüpfte Rollenberechtigungen für Amazon Chime SDK Live Transcription
- Erstellen einer serviceverknüpften Rolle für Amazon Chime SDK Live Transcription
- Bearbeiten einer serviceverknüpften Rolle für Amazon Chime SDK Live Transcription
- Löschen einer serviceverknüpften Rolle für Amazon Chime SDK Live Transcription
- Unterstützte Regionen für serviceverknüpfte Amazon Chime-Rollen

Serviceverknüpfte Rollenberechtigungen für Amazon Chime SDK Live Transcription

Amazon Chime SDK Live Transcription verwendet eine serviceverknüpfte Rolle namens AWSServiceRoleForAmazonChimeTranscription – Ermöglicht dem Amazon Chime SDK den Zugriff auf Amazon Transcribe und Amazon Transcribe Medical in Ihrem Namen.

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

- `transcription.chime.amazonaws.com`

Die Rollenberechtigungsrichtlinie erlaubt es dem Amazon Chime SDK, die folgenden Aktionen für die 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 serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Amazon Chime SDK Live Transcription

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

> **Note**
>
> Sie müssen über administrative IAM-Berechtigungen verfügen, um diese Schritte ausführen zu können. Wenn Sie dies nicht tun, wenden Sie sich an einen Systemadministrator.

So erstellen Sie die Rolle

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen und dann Rolle erstellen aus.
3. Wählen Sie den Rollentyp AWS Service und dann Chime Transcription aus.

   Die IAM-Richtlinie wird angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben der Richtlinie und wählen Sie dann Weiter: Tags aus.
5. Wählen Sie Weiter: Prüfen aus.
6. Bearbeiten Sie die Beschreibung nach Bedarf und wählen Sie dann Rolle erstellen aus.

Sie können auch die AWS CLI oder die -AWSAPI 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 serviceverknüpfte Rolle im IAM-Leitfaden. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für Amazon Chime SDK Live Transcription

Mit dem Amazon Chime SDK können Sie die AWSServiceRoleForAmazonChimeTranscription serviceverknüpfte Rolle nicht 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 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 Amazon Chime SDK Live Transcription

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften 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 serviceverknüpfte 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-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Amazon Chime-Rollen

Das Amazon Chime SDK 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.

Rollen mit Amazon Chime SDK-Medien-Pipelines verwenden

In den folgenden Abschnitten wird erklärt, wie Sie eine serviceverknüpfte Rolle für Amazon Chime SDK Media Pipelines erstellen und verwalten.

Themen

- Servicebezogene Rollenberechtigungen für Amazon Chime SDK-Medien-Pipelines
- Eine serviceverknüpfte Rolle für Amazon Chime SDK-Medien-Pipelines erstellen
- Bearbeiten einer serviceverknüpften Rolle für Amazon Chime SDK-Medien-Pipelines
- Löschen einer serviceverknüpften Rolle für Amazon Chime SDK-Medien-Pipelines

- Unterstützte Regionen für serviceverknüpfte Rollen im Amazon Chime SDK Media Pipelines

Servicebezogene Rollenberechtigungen für Amazon Chime SDK-Medien-Pipelines

Das Amazon Chime SDK verwendet die serviceverknüpfte Rolle mit dem Namen `AWSServiceRoleForAmazonChimeSDKMediaPipelines` — Erlaubt Amazon Chime SDK-Medien-Pipelines, in Ihrem Namen auf AWS Dienste zuzugreifen.

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

- `mediapipelines.chime.amazonaws.com`

Die Rolle ermöglicht es dem Amazon Chime SDK, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `cloudwatch:PutMetricData` für `all AWS resources`
- Aktion: `chime:CreateAttendee` für `all AWS resources`
- Aktion: `chime:DeleteAttendee` für `all AWS resources`
- Aktion: `chime:GetMeeting` für `all AWS resources`
- Aktion: `kinesisvideo:CreateStream` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:PutMedia` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:UpdateDataRetention` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:DescribeStream` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:GetDataEndpoint` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/ChimeMediaPipelines-*`
- Aktion: `kinesisvideo:ListStreams` für `arn:aws:kinesisvideo:*:`*`111122223333`*`:stream/*`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann.

Weitere Informationen zur Konfiguration von Berechtigungen finden Sie unter Servicebezogene Rollenberechtigungen im IAM-Benutzerhandbuch.

Weitere Informationen zu den `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` finden Sie AWS verwaltete Richtlinie: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy weiter oben in diesem Handbuch.

Eine serviceverknüpfte Rolle für Amazon Chime SDK-Medien-Pipelines erstellen

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. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie den Rollentyp AWS Service, dann Chime und dann Chime SDK Media Pipelines aus.
4. Wählen Sie Weiter.
5. Wählen Sie Weiter.
6. Bearbeiten Sie die Beschreibung nach Bedarf und wählen Sie dann Rolle erstellen.

Sie können auch die AWS CLI oder die AWS API verwenden, um eine serviceverknüpfte Rolle mit dem Namen `mediapipelines.chime.amazonaws.com` zu erstellen.

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

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

Bearbeiten einer serviceverknüpften Rolle für Amazon Chime SDK-Medien-Pipelines

Das Amazon Chime SDK erlaubt es 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 serviceverknüpften Rolle für Amazon Chime SDK-Medien-Pipelines

Wenn Sie eine Funktion oder einen Dienst nicht verwenden müssen, für den eine dienstbezogene Rolle erforderlich ist, empfehlen wir, diese Rolle zu löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird.

So löschen Sie die serviceverknüpfte Rolle mit IAM

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

Unterstützte Regionen für serviceverknüpfte Rollen im Amazon Chime SDK Media Pipelines

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

Verwenden der serviceverknüpften Rolle AmazonChimeSDKEvents

Das Amazon Chime SDK verwendet eine serviceverknüpfte Rolle namens `AmazonChimeSDKEvents`. Die Rolle gewährt Zugriff auf die AWS Services und Ressourcen, die vom Amazon Chime SDK verwendet oder verwaltet werden, z. B. den Kinesis Firehose, der für das Daten-Streaming verwendet wird.

Die `AmazonChimeSDKEvents` serviceverknüpfte Rolle ermöglicht es dem Amazon Chime SDK, `kinesis:PutRecord` und `kinesis:PutRecordBatch` auf Streams mit diesem Format abzuschließen: `arn:aws:firehose:::deliverystream/AmazonChimeSDKEvents-*`.

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität wie ein Benutzer, eine Gruppe oder eine Rolle eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpfte -Rolle

Die serviceverknüpfte Rolle ist Teil der CloudFormation Vorlage Chime SDK Events im Quick-Create-Link.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall Amazon Chime SDK Events zu erstellen. Erstellen Sie in der AWS-CLI oder der AWS-API eine serviceverknüpfte Rolle mit dem Servicenamen `events.chime.amazonaws.com`. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch. Wenn Sie diese Rolle löschen, können Sie diesen Vorgang wiederholen, um sie erneut zu erstellen.

Bearbeiten der serviceverknüpften Rolle

Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie ihre Beschreibung nur bearbeiten und dies mit IAM tun. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

Löschen der serviceverknüpften -Rolle

Als bewährte Methode sollten Sie die `Amazon Chime SDKEvents` Rolle löschen, wenn Sie ein Feature oder einen Service nicht mehr benötigen, die bzw. der dies erfordert. Andernfalls haben Sie eine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

Um die Rolle manuell zu löschen, löschen Sie zunächst die Ressourcen, die die Rolle verwendet. In den folgenden Schritten wird erläutert, wie beide Aufgaben ausgeführt werden.

Löschen von Rollenressourcen

Sie löschen Ressourcen, indem Sie den Kinesis Firehose löschen, der zum Streamen von Daten verwendet wird.

> **Note**
>
> Das Löschen kann fehlschlagen, wenn Sie versuchen, Ressourcen zu löschen, während die Rolle sie verwendet. Wenn ein Löschvorgang fehlschlägt, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die Rollenressourcen

- Deaktivieren Sie den Kinesis Firehose, indem Sie die folgende API aufrufen.

```
aws firehose delete-delivery-stream --delivery-stream-name delivery_stream_name
```

So löschen Sie die serviceverknüpfte Rolle

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

Protokollierung und Überwachung im Amazon Chime SDK

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung des Amazon Chime SDK und Ihrer anderen AWS Lösungen. AWS bietet die folgenden Tools, um das Amazon Chime SDK zu überwachen, Probleme zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht in Echtzeit Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen AWS. Sie können Kennzahlen 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. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Rechnen. Auf diese Weise können Sie Regeln schreiben, die auf bestimmte

Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen, wenn diese Ereignisse eintreten. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs 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 CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden. Der Service gibt die Protokolldateien in einen Amazon S3-Bucket aus, den Sie zuvor angegeben haben. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

Überwachung des Amazon Chime SDK mit Amazon CloudWatch

Sie können das Amazon Chime SDK CloudWatch zur Überwachung verwenden. CloudWatch sammelt Rohdaten und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes verschaffen können. 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 CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Metriken für das Amazon Chime SDK

Das Amazon Chime SDK sendet die folgenden Metriken an CloudWatch Das Amazon Chime SDK sendet die Metriken einmal pro Minute für die Dauer eines Anrufs und sendet alle hier aufgeführten Metriken.

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

> **Note**
>
> Das SDK sendet für die Dauer eines Anrufs einmal pro Minute Werte für Paketverluste. Die Verlustwerte summieren sich für die Dauer des Anrufs. Wenn beispielsweise um 11:01 Uhr ein Paketverlust auftritt, wird dieser Verlustwert auf die verbleibenden Minuten des Anrufs übertragen. Am Ende des Anrufs erhalten Sie eine einzige Kennzahl für den Paketverlust.

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. Einheiten: Anzahl

Metrik	Beschreibung
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 Statuscodes der 1xx-Ebene. Einheiten: Anzahl
Sip2xxCodes	Die Anzahl der SIP-Nachrichten mit Statuscodes der 2xx-Ebene. Einheiten: Anzahl
Sip3xxCodes	Die Anzahl der SIP-Nachrichten mit Statuscodes der 3xx-Ebene. Einheiten: Anzahl
Sip4xxCodes	Die Anzahl der SIP-Nachrichten mit Statuscodes der 4xx-Ebene. Einheiten: Anzahl

Metrik	Beschreibung
`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 SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`CustomerToVcRtpBytes`	Die Anzahl der Byte, die vom Kunden in RTP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`CustomerToVcRtcpPackets`	Die Anzahl der RTCP-Pakete, die vom Kunden an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
`CustomerToVcRtcpBytes`	Die Anzahl der Byte, die vom Kunden in RTCP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl

Metrik	Beschreibung
`CustomerToVcPacketsLost`	Die Anzahl der Pakete, die bei der Übertragung vom Kunden zur Amazon Chime SDK Voice Connector-Infrastruktur verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ. Einheiten: Anzahl
`CustomerToVcJitter`	Der durchschnittliche Jitter für Pakete, die vom Kunden an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet werden. Einheiten: Mikrosekunden
`VcToCustomerRtpPackets`	Die Anzahl der RTP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an den Kunden gesendet wurden. Einheiten: Anzahl
`VcToCustomerRtpBytes`	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTP-Paketen an den Kunden gesendet wurden. Einheiten: Anzahl
`VcToCustomerRtcpPackets`	Die Anzahl der RTCP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an den Kunden gesendet wurden. Einheiten: Anzahl

Metrik	Beschreibung
VcToCustomerRtcpBytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTCP-Paketen an den Kunden gesendet wurden. Einheiten: Anzahl
VcToCustomerPacketsLost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime SDK Voice Connector -Infrastruktur zum Kunden verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ. Einheiten: Anzahl
VcToCustomerJitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an den Kunden gesendet werden. Einheiten: Mikrosekunden
RTTBetweenVcAndCustomer	Die durchschnittliche Hin- und Rückflugzeit zwischen dem Kunden und der Amazon Chime SDK Voice Connector-Infrastruktur. Einheiten: Mikrosekunden
MOSBetweenVcAndCustomer	Der geschätzte Mean Opinion Score (MOS) im Zusammenhang mit Sprachstreams zwischen dem Kunden und der Amazon Chime SDK Voice Connector-Infrastruktur. Einheiten: Ergebnis zwischen 1,0 bis 4,4. Eine höhere Punktzahl weist auf eine besser wahrgenommene Audioqualität hin.

Metrik	Beschreibung
RemoteToVcRtpPackets	Die Anzahl der RTP-Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
RemoteToVcRtpBytes	Die Anzahl der Byte, die vom Remote-En de in RTP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
RemoteToVcRtcpPackets	Die Anzahl der RTCP-Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
RemoteToVcRtcpBytes	Die Anzahl der Byte, die vom Remote-En de in RTCP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden. Einheiten: Anzahl
RemoteToVcPacketsLost	Die Anzahl der Pakete, die bei der Übertragu ng vom Remote-Ende zur Amazon Chime SDK Voice Connector-Infrastruktur verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ. Einheiten: Anzahl

Metrik	Beschreibung
RemoteToVcJitter	Der durchschnittliche Jitter für Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet werden. Einheiten: Mikrosekunden
VcToRemoteRtpPackets	Die Anzahl der RTP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden. Einheiten: Anzahl
VcToRemoteRtpBytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTP-Paketen an das Remote-Ende gesendet wurden. Einheiten: Anzahl
VcToRemoteRtcpPackets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an das Remote-Ende gesendet wurden. Einheiten: Anzahl
VcToRemoteRtcpBytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTCP-Paketen an das Remote-Ende gesendet wurden. Einheiten: Anzahl

Metrik	Beschreibung
VcToRemotePacketsLost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime SDK Voice Connector -Infrastruktur zum Remote-Ende verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ. Einheiten: Anzahl
VcToRemoteJitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an das Remote-Ende gesendet werden. Einheiten: Mikrosekunden
RTTBetweenVcAndRemote	Die durchschnittliche Hin- und Rücklaufzeit zwischen dem Remote-Ende und der Amazon Chime SDK Voice Connector-Infrastruktur. Einheiten: Mikrosekunden
MOSBetweenVcAndRemote	Der geschätzte Mean Opinion Score (MOS) im Zusammenhang mit Sprachstreams zwischen dem Remote-End und der Amazon Chime SDK 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 das Amazon Chime SDK

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

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

CloudWatch Protokolle für das Amazon Chime SDK

Sie können Ihre Amazon Chime SDK Voice Connectors so konfigurieren, dass Messwerte an CloudWatch Logs gesendet werden. Wenn Sie dies tun, können Sie auch Metrikprotokolle in Medienqualität für diese Voice Connectors erhalten.

Das Amazon Chime SDK sendet einmal pro Minute detaillierte Metriken. Das Amazon Chime SDK sendet sie für alle Anrufe, die mit den konfigurierten Voice Connectors getätigt wurden, und sendet sie an eine CloudWatch Logs-Protokollgruppe, die wir für Sie erstellen.

Der Name der Protokollgruppe verwendet dieses Format:`/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`.

Weitere Informationen zur Konfiguration von Voice Connectors zum Senden von Messdaten finden Sie unterBearbeiten der Amazon Chime SDK Voice Connector-Einstellungen.

> **Note**
>
> Die Messwerte für den Paketverlust sammeln sich für die Dauer eines Anrufs an. Wenn beispielsweise um 11:01 Uhr ein Paketverlust auftritt, wird dieser Verlustwert auf die verbleibenden Minuten des Anrufs übertragen. Am Ende des Anrufs erhalten Sie eine einzige Kennzahl für den Paketverlust.

Das Amazon Chime SDK enthält die folgenden Felder in den Protokollen im JSON-Format.

Feld	Beschreibung
voice_connector_id	Die Amazon Chime SDK 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.
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. Mit CloudWatch Logs Insights verwenden. 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 SDK Voice Connector-Infrastruktur gesendet wurden.
cust2vc_rtp_bytes	Die Anzahl der Byte, die vom Kunden in RTP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.

Feld	Beschreibung
cust2vc_rtcp_packets	Die Anzahl der RTCP-Pakete, die vom Kunden an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.
cust2vc_rtcp_bytes	Die Anzahl der Byte, die vom Kunden in RTCP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.
cust2vc_packets_lost	Die Anzahl der Pakete, die bei der Übertragung vom Kunden zur Amazon Chime SDK Voice Connector-Infrastruktur verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ.
cust2vc_jitter	Der durchschnittliche Jitter für Pakete, die vom Kunden an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet werden.
vc2cust_rtp_packets	Die Anzahl der RTP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an den Kunden gesendet wurden.
vc2cust_rtp_bytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTP-Paketen an den Kunden gesendet wurden.
vc2cust_rtcp_packets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an den Kunden gesendet wurden.
vc2cust_rtcp_bytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTCP-Paketen an den Kunden gesendet wurden.

Feld	Beschreibung
vc2cust_packets_lost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime SDK Voice Connector -Infrastruktur zum Kunden verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ.
vc2cust_jitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime SDK 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 SDK Voice Connector-Infrastruktur.
mos_btwn_vc_and_cust	Der geschätzte Mean Opinion Score (MOS) im Zusammenhang mit Sprachstreams zwischen dem Kunden und der Amazon Chime SDK Voice Connector-Infrastruktur.
rem2vc_rtp_packets	Die Anzahl der RTP-Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.
rem2vc_rtp_bytes	Die Anzahl der Byte, die vom Remote-En de in RTP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.
rem2vc_rtcp_packets	Die Anzahl der RTCP-Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.

Feld	Beschreibung
rem2vc_rtcp_bytes	Die Anzahl der Byte, die vom Remote-En de in RTCP-Paketen an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet wurden.
rem2vc_packets_lost	Die Anzahl der Pakete, die bei der Übertragu ng vom Remote-Ende zur Amazon Chime SDK Voice Connector-Infrastruktur verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ.
rem2vc_jitter	Der durchschnittliche Jitter für Pakete, die vom Remote-Ende an die Amazon Chime SDK Voice Connector-Infrastruktur gesendet werden.
vc2rem_rtp_packets	Die Anzahl der RTP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastr uktur an das Remote-Ende gesendet wurden.
vc2rem_rtp_bytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTP-Paketen an das Remote-Ende gesendet wurden.
vc2rem_rtcp_packets	Die Anzahl der RTCP-Pakete, die von der Amazon Chime SDK Voice Connector-Infrastr uktur an das Remote-Ende gesendet wurden.
vc2rem_rtcp_bytes	Die Anzahl der Byte, die von der Amazon Chime SDK Voice Connector-Infrastruktur in RTCP-Paketen an das Remote-Ende gesendet wurden.

Feld	Beschreibung
vc2rem_packets_lost	Die Anzahl der Pakete, die bei der Übertragung von der Amazon Chime SDK Voice Connector -Infrastruktur zum Remote-Ende verloren gegangen sind. Werte werden jede Minute gesendet, bis der Anruf endet. Die Anzahl der Werte ist kumulativ.
vc2rem_jitter	Der durchschnittliche Jitter für Pakete, die von der Amazon Chime SDK Voice Connector-Infrastruktur an das Remote-Ende gesendet werden.
rtt_btwn_vc_and_rem	Die durchschnittliche Hin- und Rücklaufzeit zwischen dem Remote-Ende und der Amazon Chime SDK Voice Connector-Infrastruktur.
mos_btwn_vc_and_rem	Der geschätzte Mean Opinion Score (MOS) im Zusammenhang mit Sprachstreams zwischen dem Remote-End und der Amazon Chime SDK Voice Connector-Infrastruktur.

SIP-Nachrichtenprotokolle

Sie können sich dafür entscheiden, SIP-Nachrichtenprotokolle für Ihren Amazon Chime SDK Voice Connector zu erhalten. Wenn Sie dies tun, erfasst das Amazon Chime SDK eingehende und ausgehende SIP-Nachrichten und sendet sie an eine CloudWatch Logs-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 SDK Voice Connector-ID.
aws_region	Die AWS Region, die mit dem Ereignis verknüpft ist.

Feld	Beschreibung
event_timestamp	Der Zeitpunkt, zu dem die Nachricht erfasst wird, in Millisekunden seit der UNIX-Epoche (Mitternacht am 1. Januar 1970) in UTC.
call_id	Die Amazon Chime SDK Voice Connector-Anruf-ID.
sip_message	Die vollständige SIP-Nachricht, die erfasst wird.

Automatisieren des Amazon Chime SDK mit EventBridge

EventBridge Mit Amazon können Sie Ihre AWS Services automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen reagieren. Weitere Informationen zu den Besprechungsereignissen finden Sie unter Besprechungsereignisse im Amazon Chime SDK Developer Guide.

Wenn das Amazon Chime SDK Ereignisse generiert, sendet es sie EventBridge zur bestmöglichen Zustellung an. Das bedeutet, dass das Amazon Chime SDK versucht, alle Ereignisse an zu senden EventBridge, aber in seltenen Fällen kann es vorkommen, dass ein Ereignis nicht zugestellt wird. Weitere Informationen finden Sie unter Events from AWS services im EventBridge Amazon-Benutzerhandbuch.

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

Automatisieren von Amazon Chime SDK Voice Connectors mit EventBridge

Zu den Aktionen, die für Amazon Chime SDK Voice Connectors automatisch ausgelöst werden können, gehören:

- Eine Funktion aufrufen AWS Lambda
- Eine Amazon Elastic Container Service-Aufgabe starten

- Weiterleiten des Ereignisses an Amazon Kinesis Video Streams
- Aktivierung einer Zustandsmaschine AWS Step Functions
- Benachrichtigen eines Amazon SNS-Themas oder einer Amazon SQS-Warteschlange

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

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

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Amazon Chime SDK Voice Connector Streaming-Ereignisse

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

Das Amazon Chime SDK Voice Connector-Streaming wird gestartet

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

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@abcdef1ghij2klmno3pqr4M.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-1:123456M:stream/
ChimeVoiceConnector-abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

Das Streaming mit dem Amazon Chime SDK Voice Connector wird beendet

Amazon Chime SDK Voice Connectors senden dieses Ereignis, wenn das Medienstreaming zu 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 für Amazon Chime SDK Voice Connector

Amazon Chime SDK Voice Connectors senden dieses Ereignis, wenn das Medienstreaming zu 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 Streaming mit dem Amazon Chime SDK Voice Connector schlägt fehl

Amazon Chime SDK 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"
  }
}
```

Wird AWS CloudTrail zum Protokollieren von API-Aufrufen verwendet

Das Amazon Chime SDK ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die ein Benutzer, eine Rolle oder AWS ein Service im Amazon Chime SDK ausgeführt hat. CloudTrail erfasst alle API-Aufrufe für das Amazon Chime SDK als Ereignisse, einschließlich Aufrufe von der Amazon Chime SDK-Konsole und Codeaufrufen an die Amazon Chime SDK-APIs.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für das Amazon Chime SDK. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole auf der Seite mit dem Ereignisverlauf anzeigen. Zu den Informationen gehören jede Anfrage, die IP-Adressen, von denen aus die Anfragen gestellt wurden, und wer die Anfrage gestellt hat.

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn die Amazon Chime Chime-Verwaltungskonsole einen API-Aufruf tätigt, CloudTrail zeichnet sie diese Aktivität in einem Ereignis auf. Um die Ereignisse zu sehen, starten Sie die CloudTrail Konsole und gehen Sie zum Ereignisverlauf. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Erstellen eines Trails

In den folgenden Themen wird erklärt, wie Sie mit der CloudTrail Konsole einen Trail erstellen. Wenn Sie in der Konsole einen Trail erstellen, protokolliert der Trail standardmäßig Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket.

Folgen Sie diesen Themen in der angegebenen Reihenfolge.

1. Übersicht zum Erstellen eines Trails
2. CloudTrail unterstützte Dienste und Integrationen
3. Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
4. Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Daten, die durch eine Spur erfasst wurden

CloudTrail protokolliert alle Amazon Chime SDK-Aktionen. Informationen zu den Aktionen finden Sie in der Amazon Chime SDK API-Referenz. Aufrufe der CreateAttendeeAktion generieren beispielsweise Einträge in den CloudTrail Protokolldateien. Jedes Ereignis enthält Informationen darüber, wer die Anfrage generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

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

Weitere Informationen finden Sie unter dem CloudTrailUserIdentity-Element.

Grundlegendes zu den Amazon Chime SDK-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen

oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge erscheinen.

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

Wenn Sie Active Directory für Ihr Amazon Chime SDK-Konto konfiguriert haben, finden Sie weitere Informationen unter Protokollieren von AWS Verzeichnisdienst-API-Aufrufen mithilfe von CloudTrail. Hier wird beschrieben, wie Sie nach Problemen suchen, die sich auf die Anmeldefähigkeit Ihrer Amazon Chime SDK-Benutzer auswirken könnten.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für das Amazon Chime SDK:


```
{"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 das Amazon Chime SDK

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 im Amazon Chime SDK

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 das Amazon Chime SDK verschiedene Funktionen, um Ihre Datenstabilität und Backup-Anforderungen zu erfüllen. Weitere Informationen finden Sie unter Amazon Chime SDK Voice Connector-Gruppen verwalten und Amazon Chime SDK Voice Connector-Medien an Kinesis streamen.

Infrastruktursicherheit im Amazon Chime SDK

Als verwalteter Service ist es 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.

Erste Schritte

Die Informationen in den folgenden Themen erläutern die ersten Schritte mit den administrativen Aufgaben des Amazon Chime SDK.

Themen

Einrichten von Telefonnummern für Ihr Amazon Chime SDK-Konto

Die folgenden Telefonoptionen sind für Administratorkonten des Amazon Chime SDK verfügbar:

Amazon Chime SDK Voice Connector

Stellt Session Initiation Protocol (SIP)-Trunking-Services für ein vorhandenes Telefonsystem bereit. Portieren Sie vorhandene Telefonnummern oder stellen Sie neue Telefonnummern in der Amazon Chime SDK-Konsole bereit. Dazu gehören Notfallnummern. Weitere Informationen finden Sie unter Amazon Chime SDK Voice Connectors verwalten und Einrichten von Notrufen.

Amazon Chime SDK – SIP-Medienanwendungen

Mit Amazon Chime SDK können Sie einfacher und schneller benutzerdefinierte Signalisierungs- und Medienanweisungen erstellen, die Sie normalerweise auf Ihrem Private Branch Phone Exchange (PBX) aufbauen würden. Weitere Informationen finden Sie unter Verwaltung von SIP-Medienanwendungen

Verwaltung von Telefonnummern im Amazon Chime SDK

In den Themen in diesem Abschnitt wird erklärt, wie Telefonnummern für die Verwendung mit dem Amazon Chime SDK verwaltet werden.

Sie können Nummern auf folgende Weise abrufen:

- Stellen Sie Nummern bereit, indem Sie sie aus einem vom Amazon Chime SDK bereitgestellten Nummernpool bestellen. Sie können dies nur in Ländern tun, in denen es keine Identifizierungsanforderungen gibt.
- Portieren Sie bestehende Nummern von einem anderen Mobilfunkanbieter in das Amazon Chime SDK.
- Internationale Telefonnummern bestellen.

Die Bereitstellungs- und Portierungsprozesse fügen die Nummern Ihrem Inventar hinzu. Anschließend verwenden Sie die Nummern mit Amazon Chime SDK Voice Connectors, Amazon Chime SDK Voice Connector-Gruppen oder Amazon Chime SDK SIP-Medienanwendungen.

> **Note**
>
> Sie können gebührenfreie Nummern für die Verwendung mit Amazon Chime SDK Voice Connectors und Amazon Chime SIP-Medienanwendungen portieren. Amazon Chime Business Calling unterstützt keine gebührenfreien Nummern. Weitere Informationen finden Sie Portieren von Telefonnummern weiter unten in diesem Handbuch.

Um eine Telefonnummer mit einer Amazon Chime SDK Voice Connector- oder Amazon Chime SDK Voice Connector-Gruppe zu verwenden, verwenden Sie die Amazon Chime SDK-Konsole, um die Nummer zuzuweisen. Informationen zu Voice Connectors finden Sie unter. Amazon Chime SDK Voice Connectors verwalten Informationen zum Zuweisen von Nummern zu Voice Connectors finden Sie unterZuweisen von Nummern zu einer Voice Connector- oder Voice Connector-Gruppe.

> **Note**
>
> Sie verwenden Voice Connectors auch, um Notrufe von Amazon Chime aus zu aktivieren. Das Amazon Chime SDK bietet jedoch keine Notrufdienste außerhalb der USA an. Um die

Notrufdienste zu ändern, die das Amazon Chime SDK für die Vereinigten Staaten bereitstellt, können Sie eine Notruf-Routing-Nummer von einem Drittanbieter für Notrufe anfordern, diese Nummer an das Amazon Chime SDK weitergeben und die Nummer dann einem Amazon Chime SDK Voice Connector zuweisen. Weitere Informationen finden Sie unter Einrichten von Notfall-Routing-Nummern von Drittanbietern.

Um eine Telefonnummer mit einer SIP-Medienanwendung zu verwenden, fügen Sie sie der SIP-Regel hinzu, die der Anwendung zugeordnet ist. Weitere Informationen zu SIP-Medienanwendungen finden Sie unterVerwenden von SIP-Medienanwendungen. Weitere Informationen zum Hinzufügen von Telefonnummern zu SIP-Regeln finden Sie unterErstellen einer SIP-Regel.

Note

Für Amazon Chime SDK Voice Connectors und Amazon Chime SDK SIP-Medienanwendungen gelten Bandbreitenanforderungen. Weitere Informationen finden Sie unter Anforderungen an die Bandbreite.

Inhalt

Bereitstellen von Telefonnummern

Sie verwenden die Amazon Chime SDK-Konsole, um Telefonnummern für Ihr Amazon Chime SDK-Konto bereitzustellen. Wählen Sie aus den folgenden Ansätzen:

- Amazon Chime SDK Voice Connectors — Integration in ein vorhandenes Telefonsystem. Weitere Informationen finden Sie unter Amazon Chime SDK Voice Connectors verwalten.

- Amazon Chime SDK SIP-Medienanwendungen — Integrieren Sie Amazon Chime SDK-Besprechungen und interaktive Sprachantwortdienste wie Amazon Lex. Weitere Informationen finden Sie unter Verwaltung von SIP-Medienanwendungen.

Sie stellen Telefonnummern aus einem Pool von Nummern bereit, die vom Amazon Chime SDK bereitgestellt werden. Wenn die Bereitstellung abgeschlossen ist, werden die Telefonnummern in Ihrem Inventar angezeigt, und Sie können sie einzelnen Benutzern zuweisen.

> **Important**
>
> Sie befolgen diese Schritte nur für Länder, für die keine Identifizierungsanforderungen gelten. Informationen zur Bereitstellung von Telefonnummern in Ländern mit Identifizierungsanforderungen finden Sie unterInternationale Telefonnummern anfordern.

So stellen Sie Telefonnummern bereit

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie den Tab Bestellungen und anschließend Telefonnummern bereitstellen aus.
4. Wählen Sie im Dialogfeld „Telefonnummern bereitstellen“ die Option „Voice Connector“ oder „SIP Media Application Dial-In“ und anschließend „Weiter“.

   > **Note**
   >
   > Der einer Telefonnummer zugewiesene Produkttyp wirkt sich auf Ihre Abrechnung aus. Wenn Sie einen Standardanrufnamen festlegen, weist das System ihn neu bereitgestellten Telefonnummern in den USA zu. Bei ausgehenden Anrufen mit SIP-Medienanwendungen muss die Anrufer-ID außerdem mit einer Nummer in Ihrem Inventar übereinstimmen. Alternativ muss sie mit der ursprünglichen Anrufer-ID eines eingehenden Anrufs übereinstimmen, der von der zugehörigen Lambda-Funktion zurückgesendet wurde. Die Funktion könnte beispielsweise die Aktion verwenden. `CallAndBridge` Weitere Informationen finden Sie Namen für ausgehende Anrufe

festlegen in diesem Handbuch und CallAndBridgeim Amazon Chime SDK Developer Guide.

5. Gehen Sie auf der Seite Rufnummern bereitstellen wie folgt vor:
   - Öffnen Sie die Liste „Anwendungstyp auswählen“ und wählen Sie eine der Optionen, Voice Connector oder SIP Media Application Dial-in.

     Ihre Auswahl wirkt sich auf die Länder aus, die Sie in Schritt 6 sehen.
   - (Optional) Geben Sie unter Details zur Telefonnummer (n) im Feld Name einen aussagekräftigen Namen für die Telefonnummer ein, z. B. eine Kostenstelle oder einen Bürostandort.

     Dieses Feld unterscheidet sich von den Namen ausgehender Anrufe. Weitere Informationen zu den Namen ausgehender Anrufe finden Sie Namen für ausgehende Anrufe festlegen in diesem Handbuch.
6. Öffnen Sie unter Rufnummernsuche die Länderliste, wählen Sie ein Land aus und führen Sie dann einen der folgenden Schritte aus:
   - Für Nummern außerhalb der USA:
     a. Öffnen Sie die Typliste und wählen Sie eine Option aus.

        Je nach Land, das Sie auswählen, ist einer der Typen möglicherweise nicht verfügbar. Sie können beispielsweise nur lokale Nummern für Kanada und gebührenfreie Nummern für Italien auswählen.
     b. Wählen Sie die Schaltfläche Suchen.
   - Für US-Nummern:
     a. Öffnen Sie die Typliste und wählen Sie eine Option aus.
     b. Öffnen Sie die Gebietsliste und wählen Sie Standort oder Vorwahl.
        - Wenn Sie Standort wählen, öffnen Sie die Liste Bundesland und wählen Sie ein Bundesland aus. Geben Sie dann eine Stadt ein und klicken Sie auf die Schaltfläche Suchen.

> **Note**
>
> Wenn bei der Suche keine Zahlen zurückgegeben werden, löschen Sie das Feld Stadt und suchen Sie erneut.

- Wenn Sie Ortsvorwahl wählen, geben Sie eine Vorwahl in das Feld Ortsvorwahl ein und klicken Sie auf die Schaltfläche Suchen.

7. Wählen Sie aus der daraufhin angezeigten Liste eine oder mehrere Telefonnummern aus.
8. (Optional) Geben Sie unter Details zur Telefonnummer (n) einen Namen für die Nummer (n) ein. Wenn Sie in den vorherigen Schritten mehrere Nummern ausgewählt haben, gilt der Name für alle Nummern.
9. Wählen Sie „Rufnummernbestellung erstellen“.

Die Telefonnummern werden während der Bereitstellung auf den Tabs Bestellungen und Ausstehend angezeigt. Wenn die Bereitstellung abgeschlossen ist, werden die Nummern auf der Registerkarte Inventar angezeigt.

Internationale Telefonnummern anfordern

In den Schritten in diesem Abschnitt wird erklärt, wie Sie internationale Telefonnummern für die Verwendung mit dem Amazon Chime SDK anfordern. Sie können nur internationale Nummern mit dem Produkttyp SIP Media Application Dial-In verwenden.

Um internationale Rufnummern erwerben zu können, müssen Sie aufgrund der in vielen Ländern geltenden Vorschriften über die folgenden Artikel verfügen:

- Eine lokale Adresse
- Nachweis Ihrer Identität durch das Amazon Chime SDK oder unsere Transporteure

Warten Sie 2—6 Wochen, bis das Amazon Chime SDK Ihre Anfrage bearbeitet hat. Weitere Informationen zu den Dokumentationsanforderungen für verschiedene Länder finden Sie unter. the section called “Länderanforderungen für Telefonnummern”

So fordern Sie internationale Telefonnummern in Ländern an, in denen Ausweispflichten gelten

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
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. Falls es noch nicht ausgewählt ist, wähle Konto und Abrechnung aus.
4. Wählen Sie für Service Chime SDK (Number Management).
5. Wählen Sie als Kategorie die Option Telefonnummernanfragen und dann Nächster Schritt: Zusätzliche Informationen aus.
6. Geben Sie als Betreff Provisioning International Numbers ein.
7. Geben Sie für Problem oder Beschreibung Folgendes ein:

   - Einzelperson oder Unternehmen
   - Name (Einzelperson oder Firmenname)
   - Art der Nummer (lokal oder gebührenfrei)
   - Land
   - Anzahl der Telefonnummern
8. Geben Sie unter E-Mail die E-Mail-Adresse ein, die mit Ihrem Amazon Chime Chime-Administratorkonto verknüpft ist, und wählen Sie dann Anfrage senden aus.

   AWS Der Support beantwortet Ihre Support-Anfrage per E-Mail und teilt Ihnen mit, ob die Telefonnummern bereitgestellt werden können. Sobald die Nummern bereitgestellt wurden, können Sie sie in der Amazon Chime SDK-Konsole anzeigen. Wählen Sie unter Telefonnummern die Option Telefonnummernverwaltung aus. Ihre Nummern werden auf der Inventarseite angezeigt.
9. Verwenden Sie SIP-Regeln, um die Telefonnummern der entsprechenden SIP-Medienanwendung zuzuweisen.

Einreichen der erforderlichen Dokumente

Nachdem Sie die angeforderten Telefonnummern erhalten haben, reichen Sie alle erforderlichen Dokumente ein. In den folgenden Schritten wird erklärt, wie.

> **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 SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
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. Aktivieren Sie unter Objekte das Kontrollkästchen „Lesen“ und wählen Sie dann „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.

Einschränkungen für ausgehende Anrufe

China

Chinesische Fluggesellschaften blockieren zunehmend internationale Strecken nach China. Das Amazon Chime SDK unterstützt weiterhin unsere Bestandskunden, aber alle Kunden, die China anrufen dürfen, müssen die folgenden Bedingungen erfüllen:

Zulassungskriterien

Nicht unterstützte Anwendungsfälle

- Anrufe von kurzer Dauer und Warnmeldungen von weniger als 15 Sekunden.
- Hohe Anzahl von Anrufen, insbesondere über einen kurzen Zeitraum, unter Verwendung derselben ausgehenden Anrufer-ID (mehr als 5 Anrufe pro Minute).
- Jede Form von Kaltakquise.
- Alle Anrufe an ungültige Telefonnummern. Alle angerufenen Nummern müssen als korrekt bestätigt werden.
- Wiederholte Anrufe mit denselben FROM- und/oder TO-Nummern.
- Versuche, China von einer beliebigen Nummer aus anzurufen, für die keine Vorabgenehmigung erteilt wurde.

Unterstützte Anwendungsfälle

- Direkte Anrufe an bekannte Geschäftseinheiten, z. B. ein Hotel oder eine IT-Supportabteilung.
- Rufen Sie Benutzer an, die versuchen, mit Ihrem Unternehmen in Kontakt zu treten, z. B. bei Praktika an Universitäten oder beim Kauf von Produkten.

Für die Einrichtung erforderliche Daten

Gehen Sie wie folgt vor, um die Erlaubnis zum Anrufen chinesischer Telefonnummern (+86) zu erhalten:

- Geben Sie eine genaue und vollständige Liste der Telefonnummern an, unter denen China angerufen wurde.
  - Bei der Nummer muss es sich um eine vom Amazon Chime SDK bereitgestellte DID handeln. Andere Nummern sind nicht zulässig.
  - Nummern dürfen nicht von Hongkong, Macau, Taiwan, China oder Singapur bereitgestellte DIDs sein.

  > **Note**
  >
  > Die obige Liste kann sich jederzeit ändern.

- Für jede Nummer müssen Sie eine Ankündigung aufzeichnen, in der der Name Ihres Unternehmens angegeben ist, sodass jeder, der die Nummer anruft, die Aufzeichnung hören kann und weiß, welches Unternehmen den Anruf tätigt.
- Sie müssen eine detaillierte Beschreibung Ihres Anwendungsfalls für Anrufe nach China vorlegen AWS und bestätigen, dass Sie die in diesem Thema beschriebenen Zulassungskriterien erfüllen.

Folgen eines Verstoßes gegen die Kriterien

Das Amazon Chime SDK verfolgt eine Null-Toleranz-Richtlinie für Anrufe nach China. Amazon sperrt Ihr Amazon Chime SDK-Konto, wenn Sie den Service für einen der oben aufgeführten eingeschränkten Anwendungsfälle nutzen. Ihre Amazon Chime SDK-Administratoren müssen diese Richtlinie anderen Mitgliedern Ihrer Organisation mitteilen, damit auch sie über diese Einschränkungen informiert sind. Die Unkenntnis der Regeln ist kein akzeptabler Grund für einen Verstoß.

Servicegewährleistung

Wenn chinesische Fluggesellschaften wichtige internationale Strecken ohne vorherige Warnung blockieren und die Möglichkeit beeinträchtigen, nach China zu telefonieren, treten die Ausschlüsse im Amazon Chime SDK Service Level Agreement in Kraft.

Länderanforderungen für Telefonnummern

Außerhalb der USA erfordern Vorschriften häufig eine lokale Adresse und bestimmte Identifikationsdokumente, um eine Telefonnummer zu erwerben und zu verwenden. Bei der Adresse kann es sich um eine geschäftliche oder private Adresse handeln. In den folgenden Tabellen sind

die Länder aufgeführt, die identifiziert werden müssen. Wenn Sie internationale Telefonnummern anfordern oder bestehende Telefonnummern portieren, arbeitet der Amazon Chime SDK-Support mit Ihnen zusammen, um die erforderlichen Dokumente einzureichen.

> **Note**
>
> Stellen Sie sicher, dass Sie die Identitäten und Adressen der Endbenutzer angeben, die Ihre Telefonnummern verwenden.

Themen

Australien

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Australien aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
Amazon-Chime-SDK-SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse • Nachweis des Standorts Geschäftsadressen müssen dieselbe geografische Zone wie ihre entsprechenden Telefonnummern haben.
	Gebührenfrei	Ja	• Geschäftsadresse Internationale Adressen werden akzeptiert.

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Österreich

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Österreich aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
Einwahl für SIP-Medienanwendungen	Local	Ja	• Geschäftsadresse • Nachweis von Telekommunikationsdiensten wie einer Rechnung eines Netzwerkbetreibers mit einer anderen Telefonnummer im selben Bereich. -ODER- Eine Rechnung eines Internetanbieters für den Internetzugriff mit einer festen IP-Adresse im rechten Bereich. Geschäftsadressen müssen dieselbe geografische Zone wie ihre entsprechenden Telefonnummern haben.

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
	Nationale Vorwahlen: +43 720	Ja	• Geschäftsadresse Die Adresse muss sich im Land befinden.
	Gebührenfrei	Ja	• Geschäftsadresse Fremdadresse akzeptabel

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Kanada

In den folgenden Tabellen werden die Anforderungen für die Bestellung und Portierung von Telefonnummern in Kanada aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Nein	N/A
Gebührenfrei	Nein	N/A	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Dänemark

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Italien aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Nein	N/A
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Finnland

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Finnland aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse • Nachweis des Standorts Geschäftsadressen müssen sich in denselben geografischen Regionen wie ihre entsprechenden Telefonnummern befinden.

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
	Nationale Präfixe +358 075	Nein	N/A
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Deutschland

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Deutschland aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse • Eine Kopie Ihrer Unternehmensregistrierung

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
			oder eine Kopie Ihrer -ID, wenn Sie eine Person sind • Adressnachweis, z. B. eine Rechnung eines Energieunternehmens Geschäftsadressen müssen dieselbe geografische Zone wie ihre entsprechenden Telefonnummern haben.
	Nationale Vorwahlen: +49 32	Ja	• Geschäftsadresse • Eine Kopie Ihrer Unternehmensregistrierung oder eine Kopie Ihrer -ID, wenn Sie eine Person sind • Adressnachweis, z. B. eine Rechnung eines Energieunternehmens Die Adresse muss sich im Land befinden.

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
	Gebührenfrei	Ja	• Geschäftsadresse • Adressnachweis, z. B. eine Rechnung eines Energieunternehmens Die Adresse muss sich im Land befinden. Sie müssen die Nummer zuerst direkt von der lokalen Aufsichtsbehörde abrufen. Details zum Vorgang werden bei Anforderungsstellung bereitgestellt.

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA) • Geschäftsadresse • Eine Kopie Ihrer Unternehmensregistrierung • Kopie der ID des Unternehmensmitarbeiters

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
		Geschäftsadressen müssen dieselbe geografische Zone wie ihre entsprechenden Telefonnummern haben.
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA) • Nummernzertifikat von NRAs Sie müssen die Nummer zuerst direkt von der lokalen Aufsichtsbehörde abrufen. Details zum Prozess werden bereitgestellt, wenn Sie die Anforderung stellen

Irland

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Irland aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse Geschäftsadressen müssen sich in denselben geografis

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
			chen Regionen wie die entsprechenden Telefonnummern befinden.
	Universaler Zugriff und VOIP-Präfixe: +353 0818, +353 076	Ja	• Geschäftsadresse Die Adresse muss sich im Land befinden.
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Italien

In den folgenden Tabellen werden die Anforderungen für die Bestellung und Portierung von Telefonnummern in Italien aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse • Nachweis des Standorts • Kopie der Geschäftsregistrierung • Reisepass- oder Endbenutzer-ID Geschäftsadressen müssen sich in denselben geografischen Regionen wie die entsprechenden Telefonnummern befinden.
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA) • Kopie des Reisepasses oder der ID des Unternehmensmitarbeiters

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
		• Kopie der lokalen Unternehmensregistrierung oder Adressnachweis für eine Person
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Neuseeland

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Neuseeland aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Nein	N/A
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP-Medienanwendungs-Dial-In	Local	Nicht unterstützt
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Nigeria

In den folgenden Tabellen sind die Anforderungen für die Bestellung von Telefonnummern in Nigeria aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse Fremdadresse akzeptabel.

Puerto Rico

In den folgenden Tabellen werden die Anforderungen für die Bestellung und Portierung von Telefonnummern in Rico aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
Geschäftsanrufe Amazon Chime SDK Voice Connector	Local	Nein	N/A
Gebührenfrei	Nein	N/A	N/A

Südkorea

In den folgenden Tabellen sind die Anforderungen für die Bestellung von Telefonnummern in Korea aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP-Medienanwendungs-Dial-In	Gebührenfrei	Ja	• Geschäftsadresse • Nachweis des Standorts Die Adresse muss sich im Land befinden.

Schweden

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Schweden aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP Medienanwendungs-Dial-In	Local	Nein	N/A
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
		• Letter of Authorization (LOA)

Schweiz

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in der Türkei aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP Medienanwendungs-Dial-In	Local	Ja	• Geschäftsadresse • Nachweis des Standorts • Eine Kopie der Unternehmensregistrierung oder eine Kopie Ihrer -ID, wenn Sie eine Person sind Geschäftsadressen müssen dieselbe geografische Zone wie ihre entsprechenden Telefonnummern haben.
	Geschäftsnummernpräfixe: +41 051, +41 058	Ja	• Geschäftsadresse

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
			Die Adresse muss sich im Land befinden.
	Gebührenfrei	Ja	• Geschäftsadresse • Eine Kopie der Unternehmensregistrierung oder eine Kopie Ihrer -ID, wenn Sie eine Person sind Fremdadresse akzeptabel

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA) • Geschäftsadresse Fremdadressen sind akzeptabel
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
		• Geschäftsadresse • Zertifikat von NRAs Die Adresse muss sich innerhalb des Landes befinden.

Großbritannien und Nordirland

In den folgenden Tabellen sind die Anforderungen für die Bestellung und Portierung von Telefonnummern in Großbritannien aufgeführt und beschrieben.

Bestellung von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	ID-Anforderungen	Zulässige ID-Typen
SIP Medienanwendungs-Dial-In	Local	Nein	N/A
	Gebührenfrei	Nein	N/A

Portieren von Telefonnummern

Unterstützte Produkttypen	Zahlentypen	Erforderliche ID
SIP Medienanwendungs-Dial-In	Local	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)
	Gebührenfrei	• Letzte Rechnung des aktuellen Anbieters • Letter of Authorization (LOA)

Portieren von Telefonnummern

> **Important**
>
> Ab Freitag, dem 01. März 2024, wurden Anfragen zur Portierung von Amazon Chime SDK-Telefonnummern in den Bereich Konto und Abrechnung der AWS Support Center-Konsole verschoben. Um einen neuen Support-Fall für die Portierung von Telefonnummern zu erstellen, wählen Sie Konto und Abrechnung, öffnen Sie das Drop-down-Menü Services und wählen Sie Chime (Nummernverwaltung).

Neben der Bereitstellung von Telefonnummern können Sie auch Nummern von Ihrem Telefonanbieter in Ihr Amazon Chime SDK-Inventar importieren. Dazu gehören gebührenfreie Nummern. Sie können portierte Nummern mit Amazon Chime SDK Voice Connectors und Amazon Chime SDK SIP-Medienanwendungen verwenden.

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

Themen

Voraussetzungen für die Portierung von Nummern

Für die Portierung von Nummern müssen Sie über folgende Voraussetzungen verfügen:

- Eine Vollmacht (LOA). Sie benötigen eine LOA für US-amerikanische und internationale Telefonnummern. Laden Sie das Formular Letter of Agency (LOA) herunter und füllen Sie es aus. Wenn Sie mehrere Telefonnummern von verschiedenen Telefonnetzbetreibern portieren möchten, müssen Sie für jeden Telefonnetzbetreiber eine LOA (Autorisierung) ausfertigen.

> **Note**
>
> In einer Reihe von Ländern gelten Dokumentationspflichten für die Portierung von Telefonnummern. Weitere Informationen finden Sie unter Länderanforderungen für Telefonnummern in diesem Handbuch.

- Bevor Sie Telefonnummern für Amazon Chime SDK Voice Connectors portieren können, müssen Sie einen Voice Connector erstellen. Weitere Informationen finden Sie unter Einen Amazon Chime SDK Voice Connector erstellen.

Portierung von Telefonnummern in das Amazon Chime SDK

Sie erstellen eine Support-Anfrage, um bestehende Telefonnummern in das Amazon Chime SDK zu portieren.

Um bestehende Telefonnummern in das Amazon Chime SDK zu portieren

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
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 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 Ihr BTN portieren möchten, geben Sie eine der folgenden Optionen an:
  - 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 der oben aufgeführten Optionen 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 SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
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. Aktivieren Sie unter Objekte das Kontrollkästchen „Lesen“ und wählen Sie dann „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

Um die Amazon Chime SDK-Konsole zu verwenden, um den Status Ihrer Portierungsanfragen einzusehen.

Um den Status einzusehen

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

Portierte Nummern zuweisen

Nachdem Ihr bestehender Telefonnetzbetreiber bestätigt hat, dass das LOA korrekt ist, überprüft und genehmigt er die angeforderte Portierung. Anschließend geben sie das Datum und die Uhrzeit des Portierens an (Firm Order AWS Support Commit, FOC).

Um Nummern zuzuweisen

- • Weisen Sie Ihren Voice Connectors Amazon Chime SDK Voice Connector-Nummern zu.
  • Verwenden Sie für Einwahlnummern für Amazon Chime SDK SIP Media Application SIP-Regeln, um Nummern zuzuweisen. Weitere Informationen zu SIP-Regeln finden Sie unter SIP-Regeln erstellen.

  Die Telefonnummern werden erst nach der Festlegung des Datums des Firm Order Commit (FOC, verbindliche Auftragszusage) zur Verwendung aktiviert, wie in den folgenden Schritten dargelegt wird. Weitere Informationen finden Sie unter Verwalten des Telefonnummernverzeichnisses und Einen Amazon Chime SDK Voice Connector erstellen.

AWS Support kontaktiert Sie mit dem FOC, um zu bestätigen, dass Datum und Uhrzeit für Sie geeignet sind.

> **Note**
>
> Die Telefonnummern können erst dann Anrufe tätigen oder entgegennehmen, wenn Sie sie zugewiesen haben.

Am FOC-Datum sind die portierten Telefonnummern für die Verwendung mit dem Amazon Chime SDK aktiviert.

Portieren von Telefonnummern aus dem Amazon Chime SDK

Sie können US- und Nicht-US-Nummern aus dem Amazon Chime SDK portieren. Sie folgen für jeden Nummerntyp einem anderen Prozess. Erweitern Sie die folgenden Abschnitte nach Bedarf, um mehr zu erfahren.

Portierung von US-Nummern

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 Voice Connector-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) Beantragung einer PIN zum Schutz Ihrer Nummer

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 SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.

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.

Portierung internationaler Nummern

In den folgenden Schritten wird erklärt, wie internationale Nummern aus dem Amazon Chime SDK portiert werden.

Um Telefonnummern zu portieren

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
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 alle relevanten Daten ein.

AWS Support antwortet mit den entsprechenden nächsten Schritten. Sie erhalten Antworten auf der Grundlage Ihrer ausgewählten Kontaktmethoden und aller E-Mail-Adressen, die Sie für zusätzliche Kontakte eingegeben haben.

Wenn der Portierungsvorgang abgeschlossen ist und die Telefonnummern auf Ihren neuen Mobilfunkanbieter portiert wurden, heben Sie die Zuweisung der Telefonnummern auf und löschen Sie sie aus Ihrem Amazon Chime SDK-Inventar. Weitere Informationen finden Sie unter Aufheben der Zuweisung von Voice Connector-Telefonnummern und Löschen von Telefonnummern.

Definitionen des Portierungsstatus für Telefonnummern

Nachdem Sie eine Anfrage zur Portierung vorhandener Telefonnummern in das Amazon Chime SDK eingereicht haben, können Sie den Status Ihrer Portierungsanfrage in der Amazon Chime SDK-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 für weitere Informationen, die zur 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.

Verwalten des Telefonnummernverzeichnisses

In den folgenden Abschnitten wird erklärt, wie Sie die Telefonnummern bereitstellen und verwalten, die mit Amazon Chime SDK Voice Connectors, Amazon Chime SDK Voice Connector-Gruppen und SIP-Medienanwendungen verwendet werden.

Wenn Sie die Amazon Chime Business Calling-Telefonnummer oder die Rufnummernberechtigungen eines Benutzers ändern, empfehlen wir, dem Benutzer seine neue Telefonnummer oder seine neuen Berechtigungsinformationen mitzuteilen. Bevor Benutzer auf ihre neuen Telefonnummern- oder Berechtigungsfunktionen zugreifen können, müssen sie sich von ihrem Amazon Chime Chime-Konto abmelden und erneut anmelden.

Themen

Zuweisen von Nummern zu einer Voice Connector- oder Voice Connector-Gruppe

In den folgenden Schritten wird erklärt, wie Sie Amazon Chime SDK Voice Connectors und Voice Connector-Gruppen Telefonnummern zuweisen. Durch die Zuweisung von Nummern können Sie Anrufe tätigen.

Sie können Voice Connectors und Voice Connector-Gruppen einzelne Nummern oder Rufnummerngruppen zuweisen. In den folgenden Schritten wird erklärt, wie das geht.

Um einzelne Telefonnummern zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie zuweisen möchten, und klicken Sie dann auf Bearbeiten.
4. (Optional) Geben Sie im Feld Anrufname einen Namen für die Telefonnummer ein.
5. Stellen Sie sicher, dass unter Produkttyp Voice Connector ausgewählt ist
6. Wählen Sie unter Zuweisungstyp die Option Voice Connector oder Voice Connector-Gruppe aus und führen Sie dann einen der folgenden Schritte aus.

   a. Wenn Sie Voice Connector ausgewählt haben, öffnen Sie die Liste mit den Voice Connector-Optionen und wählen Sie einen Voice Connector aus.

   b. Wenn Sie die Voice Connector-Gruppe ausgewählt haben, öffnen Sie die Liste mit den Voice Connector-Gruppenoptionen und wählen Sie eine Voice Connector-Gruppe aus.
7. Wählen Sie Speichern.

Um Gruppen von Telefonnummern zuzuweisen

1. Aktivieren Sie auf der Registerkarte Inventar die Kontrollkästchen neben den Telefonnummern, die Sie zuweisen möchten.

   > **Note**
   >
   > Die Telefonnummern müssen den Produkttyp Voice Connector haben. Überprüfen Sie außerdem die Spalte Status und stellen Sie sicher, dass Sie nur nicht zugewiesene Nummern auswählen.
2. Wählen Sie „Zuweisen“ und wählen Sie im Dialogfeld „Zuweisungstyp“ die Option „Sprachanschluss“ oder „Sprachverbindergruppe“ aus.
3. Wählen Sie „Zuweisen“ und wählen Sie im Dialogfeld „Telefonnummern zuweisen“ die Option „Voice Connector“ oder „Voice Connector-Gruppe“ und dann „Weiter“ aus.
4. Wählen Sie den Voice Connector oder die Voice Connector-Gruppe aus und wählen Sie dann „Zuweisen“.

Voice Connector-Nummern neu zuweisen

Sie können Telefonnummern von einer Amazon Chime SDK Voice Connector- oder Amazon Chime SDK Voice Connector-Gruppe einer anderen neu zuweisen. Die Nummern müssen dem Produkttyp Voice Connector entsprechen.

Sie können einzelne Nummern oder Gruppen von Nummern neu zuweisen. In den folgenden Schritten wird erklärt, wie Sie beides tun können.

Um einzelne Nummern neu zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie neu zuweisen möchten.
4. Wählen Sie Bearbeiten aus.
5. Wählen Sie unter Zuweisungstyp die Option Voice Connector oder Voice Connector-Gruppe aus. Weiter.
6. Führen Sie eine der folgenden Aktionen aus:

   a. Wenn Sie Voice Connector ausgewählt haben, öffnen Sie die Liste mit den Voice Connector-Optionen und wählen Sie einen neuen Voice Connector aus.

   b. Wenn Sie die Voice Connector-Gruppe ausgewählt haben, öffnen Sie die Liste mit den Voice Connector-Gruppenoptionen und wählen Sie eine neue Voice Connector-Gruppe aus.
7. Wählen Sie Speichern.

Um Gruppen von Telefonnummern neu zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Aktivieren Sie auf der Registerkarte Inventar die Kontrollkästchen neben den Telefonnummern, die Sie neu zuweisen möchten, und wählen Sie dann Neu zuweisen aus.

4. Wählen Sie im Dialogfeld „Neu zuweisen“ die Option „Voice Connector“ oder „Voice Connector-Gruppe“ und dann „Weiter“ aus.
5. Wählen Sie einen Voice Connector oder eine Voice Connector-Gruppe aus und wählen Sie dann „Neu zuweisen“.

Aufheben der Zuweisung von Voice Connector-Telefonnummern

In den folgenden Verfahren wird erklärt, wie Sie die Zuweisung von Telefonnummern zu Amazon Chime SDK Voice Connectors und Voice Connector-Gruppen aufheben. Sie können die Zuweisung von Telefonnummern, die von SIP-Medienanwendungen verwendet werden, nicht aufheben. Stattdessen löschen Sie die SIP-Regel. Weitere Informationen zum Löschen von SIP-Regeln finden Sie Löschen einer SIP-Regel in diesem Handbuch.

> **Note**
>
> Durch das Aufheben der Zuweisung von Nummern und das Löschen von SIP-Regeln werden die Telefoniefunktionen der Benutzer deaktiviert. Nicht zugewiesene Nummern sind jedoch weiterhin in Ihrem Inventar verfügbar, und die Abrechnung erfolgt entsprechend dem jeweiligen Produkttyp.

So heben Sie die Zuweisung einzelner Voice Connector-Telefonnummern auf

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, deren Zuweisung Sie aufheben möchten.
4. Wählen Sie Bearbeiten und wählen Sie unter Zuweisungstyp die Option Voice Connector oder Voice Connector-Gruppe aus.
5. Öffnen Sie die Optionsliste Voice Connector-Optionen oder Voice Connector-Gruppenoptionen und wählen Sie Keine (Zuweisung aufheben) aus, die erste Option in der Liste.

Rufnummern neu zuweisen

Nachdem Sie einem Amazon Chime SDK Voice Connector oder einer Voice Connector-Gruppe eine Telefonnummer zugewiesen haben, können Sie diese Nummer einem anderen Voice Connector oder einer anderen Gruppe zuweisen, ohne die Nummer aufheben zu müssen.

Um eine Telefonnummer neu zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Aktivieren Sie das Kontrollkästchen neben der Nummer, die Sie neu zuweisen möchten, und wählen Sie dann Neu zuweisen aus. .
4. Wählen Sie im Dialogfeld „Neu zuweisen“ die Option „Voice Connector“ oder „Voice Connector-Gruppe“ und dann „Weiter“ aus.
5. Wählen Sie den gewünschten Voice Connector oder die Voice Connector-Gruppe aus und wählen Sie dann „Neu zuweisen“.

Zuweisen von Telefonnummern zu SIP-Medienanwendungen

Um SIP-Medienanwendungen Telefonnummern zuzuweisen, fügen Sie sie zu den SIP-Regeln hinzu, die den Anwendungen zugeordnet sind. Weitere Informationen finden Sie unter Verwaltung von SIP-Medienanwendungen.

Details zur Telefonnummer anzeigen

Sie sehen sich die Details Ihrer Inventar-Telefonnummern aus verschiedenen Gründen an. Sie können beispielsweise den Voice Connector oder die SIP Media Application sehen, der eine Nummer zugewiesen ist. Sie können auch sehen, ob Textnachrichten aktiviert sind.

Um die Details der Telefonnummer einzusehen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.

3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie anzeigen möchten.

> **Note**
>
> Sie können zudem Folgendes durchführen:
>
> 1. Aktivieren Sie das Kontrollkästchen neben der Telefonnummer, die Sie anzeigen möchten.
> 2. Öffnen Sie die Aktionsliste und wählen Sie Details anzeigen aus.

Den Produkttyp einer Telefonnummer ändern

Wenn Sie Amazon Chime SDK Voice Connector-Telefonnummern nicht zugewiesen haben, können Sie diese von einem Produkttyp auf einen anderen umstellen.

> **Note**
>
> Für Nummern außerhalb der USA müssen Sie den Produkttyp SIP Media Application Dial-In verwenden.

Um die Produkttypen zu ändern

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie ändern möchten.
4. Klicken Sie auf der Seite Details auf Edit (Bearbeiten).
5. Wählen Sie im Dialogfeld „Produkttyp bearbeiten“ die Option Voice Connector oder SIP Media Application Dial-In aus und klicken Sie dann auf Speichern.

Den Zuweisungstyp einer Telefonnummer ändern

Wenn Sie keine Amazon Chime SDK Voice Connector- oder Amazon Chime SDK SIP-Medienanwendungs-Telefonnummern zugewiesen haben, können Sie diese von einem Produkttyp auf einen anderen umstellen.

> **Note**
>
> Für Nummern außerhalb der USA müssen Sie den Produkttyp SIP Media Application Dial-In verwenden.

Um die Zuweisungstypen zu ändern

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Telefonnummer aus, die Sie ändern möchten.
4. Klicken Sie auf der Seite Details auf Edit (Bearbeiten).
5. Wählen Sie unter Zuweisungstyp die Option Voice Connector oder Voice Connector-Gruppe aus.

   Je nach Ihrer Wahl wird die Liste der Voice Connector-Optionen oder der Voice Connector-Gruppenoptionen angezeigt.
6. Öffnen Sie die Liste und wählen Sie einen Voice Connector oder eine Voice Connector-Gruppe aus.
7. Wählen Sie Speichern.

Namen für ausgehende Anrufe festlegen

Sie können den Telefonnummern in Ihrem Inventar Anrufernamen zuweisen. Dies gilt nur für gebührenpflichtige Nummern und schließt gebührenfreie Nummern aus. Die Namen werden den Empfängern ausgehender Anrufe angezeigt. Sie können die Namen alle sieben Tage aktualisieren.

> **Note**
>
> Wenn Sie einen Amazon Chime SDK Voice Connector verwenden, um einen Anruf zu tätigen, wird dieser Anruf über ein öffentliches Telefonnetz an den Telefonanbieter des angerufenen Teilnehmers weitergeleitet. Einige Mobilfunkanbieter unterstützen keine Anrufer-ID-Namen, und einige Mobilfunkanbieter verwenden die CNAM-Datenbank von Voice Connectors nicht. Daher kann es sein, dass ein angerufener Teilnehmer die Anrufernamen nicht sieht, oder er sieht möglicherweise einen anderen Anrufernamen als den, den Sie festgelegt haben.
>
> US-Mobilfunkanbieter blockieren oder kennzeichnen zunehmend Telefonnummern, die Spam- oder Betrugsmerkmale aufweisen, wie z. B. ein hohes Anrufvolumen und kurze oder unbeantwortete Anrufe. Um das Risiko zu verringern, dass Ihre Anrufe ähnlich kategorisiert werden, sollten Sie erwägen, Ihre ausgehenden Anrufe beim kostenlosen Anruferregistrierungsdienst zu registrieren.

In den folgenden Schritten wird erklärt, wie Sie Namen für ausgehende Anrufe hinzufügen.

So legen Sie einen Namen für ausgehende Anrufe fest

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Nummer aus, der Sie den Namen hinzufügen möchten.
4. Klicken Sie auf der Seite Details auf Edit (Bearbeiten).
5. Geben Sie im Feld Anrufname einen Namen ein. Sie können bis zu 15 Zeichen verwenden.
6. Wählen Sie Speichern.

Warten Sie 72 Stunden, bis das System den Namen hinzugefügt hat.

Um einen Standard-Anrufenamen zu aktualisieren

- Wiederholen Sie den obigen Vorgang. Warten Sie 72 Stunden, bis das System den Namen aktualisiert hat.

Löschen von Telefonnummern

> **Important**
>
> Sie müssen die Zuweisung von Telefonnummern aufheben, bevor Sie sie löschen können. Führen Sie eine der folgenden Aktionen aus:
>
> - Wenn Sie einen Voice Connector oder eine Voice Connector-Gruppe verwenden, heben Sie die Zuweisung der Nummer auf. Weitere Informationen finden Sie Aufheben der Zuweisung von Voice Connector-Telefonnummern in diesem Handbuch.
> - Wenn Sie eine SIP-Medienanwendung verwenden, löschen Sie die SIP-Regel, die die Nummer enthält. Weitere Informationen finden Sie Löschen einer SIP-Regel in diesem Handbuch.

Wenn Sie eine Nummer löschen, wird sie 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 an den Amazon Chime SDK-Nummernpool zurückgegeben. Wenn Sie eine Nummer zurückfordern müssen, nachdem das System sie aus der Warteschlange 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 SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie auf der Registerkarte Inventar die Nummer aus, die Sie löschen möchten, und wählen Sie dann Löschen aus.
4. Aktivieren Sie im Dialogfeld Telefonnummern löschen das Kontrollkästchen neben Ich verstehe die Auswirkungen dieser Aktion und wählen Sie Löschen aus.

Das System speichert gelöschte Telefonnummern 7 Tage lang in der Löschwarteschlange und löscht sie dann dauerhaft.

Wiederherstellen gelöschter Telefonnummern

Sie können gelöschte Telefonnummern bis zu 7 Tage nach dem Löschen aus der Deletion queue (Löschwarteschlange) wiederherstellen. Durch das Wiederherstellen wird die Telefonnummer wieder in das Inventory (Verzeichnis) verschoben.

Nach Ablauf der 7 Tage verschiebt die Löschwarteschlange die Nummern wieder in den Nummernpool.

So stellen Sie gelöschte Telefonnummern wieder her

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option Telefonnummernverwaltung aus.
3. Wählen Sie die Registerkarte Löschwarteschlange und wählen Sie die Telefonnummer (n) aus, die wiederhergestellt werden sollen.
4. Wählen Sie Move to inventory (In Verzeichnis verschieben) aus.

Optimieren Ihrer Reputation für ausgehende Anrufe

Bei ausgehenden Geschäftsanrufen besteht eine der schwierigsten Aufgaben darin, zu verstehen, warum Kunden beim Abwählen keine Anrufe entgegennehmen. Antworten Kunden bewusst nicht, sind sie gerade in einem anderen geschäftlichen Gespräch oder nicht am Platz? Für Unternehmen ist es unmöglich zu wissen, aber Sie können Maßnahmen ergreifen, um den Anruferfolg zu steigern.

In den folgenden Themen werden Möglichkeiten zur Verbesserung Ihrer Antwortraten für ausgehende Anrufe empfohlen.

Themen

Schritt 1: Kenntnis der bevorzugte Kontaktmethode von Kunden

Einer der größten Fehler, den Unternehmen machen, besteht darin, nicht zu wissen, ob der Kunde per Telefonanruf kontaktiert werden möchte. Haben Sie bei der Interaktion abgefragt, ob Kunden per Telefon, E-Mail oder Textnachricht erreicht werden möchten?

Unternehmen mit mehreren Kontaktmöglichkeiten schneiden im Durchschnitt 70 % besser ab als Unternehmen ohne.

Schritt 2: Branding Ihrer Anrufe

Mithilfe von Branding-Lösungen für Anrufe können Sie erweiterte Anrufanzeigen bieten, die Firmennamen, Logos, den Grund für den Anruf und Ihre Angebote enthalten. Durch das Branding Ihrer Anrufe können die Anrufannahmeraten um 30 % erhöht werden.

Das Amazon Chime SDK und arbeiten mit Lösungsanbietern wie First Orion und Neustar Amazon Connect zusammen, um Telefonie-Anrufservices anbieten zu können. Um die Services direkt mit unseren Partnern zu besprechen, besuchen Sie deren Websites:

- Erste Orion
- Neustar

Schritt 3: Auswählen von Anrufer-IDs, die Kunden etwas sagen

Nicht jedes Unternehmen ist gleich. Was für das eine funktioniert, ist für andere vielleicht verkehrt. Es besteht jedoch ein Korrelation zwischen erfolgreichen ausgehenden Kampagnen und bestimmten Anrufer-IDs. Die folgenden Vorschläge können Ihnen helfen, aussagekräftige Anrufer-IDs zu erstellen:

- Gebietslokalisierung. Verwenden Sie eine Anrufer-ID in derselben Region wie die Interessenten.
- Stadtlokalisierung. Verwenden Sie eine Anrufer-ID in derselben Stadt wie die Interessenten.
- Erkennbare goldene gebührenfreie Nummern wie 0800 123 0000.

Schritt 4: Sicherstellen, dass Ihre Kampagne gültige Nummern anruft

Viele Unternehmen haben keinen Prozess zum Aktualisieren von Kundendaten. Wenn Menschen mobiler als je zuvor sind, ist es für Unternehmen wichtig, Kontaktinformationen zu aktualisieren. Wenn Kunden Ihre Anrufe nicht entgegennehmen, empfehlen wir, Ihre Telefonnummern mit Amazon Pinpoint zu validieren. https://docs.aws.amazon.com/pinpoint/latest/developerguide/validate-phone-numbers.html Der Kunde befindet sich möglicherweise nicht mehr unter der Telefonnummer, die Sie anrufen.

Schritt 5: Tätigen ausgehender Anrufe zu optimalen Zeiten

Stellen Sie sicher, dass Anrufe zu den besten Zeiten getätigt werden. Rufen Sie im Allgemeinen nicht vor 10:00 Uhr oder nach 17:00 Uhr auf, da die Menschen am stärksten beschäftigt sind oder ihre Ruhezeit benötigen. Kunden sollten je nach ihrem Profil dann angerufen werden, wenn es für sie günstig ist. Dies kann bedeuten, dass Sie einen Kunden gegenmittag und einen anderen ammittag anrufen.

Darüber hinaus bieten Vorschriften wie TCPA (in den USA) und OFCOM (in Großbritannien) Anleitungen dazu, wann Endbenutzer nicht anrufen dürfen. Wir raten dringend dazu, diese Vorschriften einzuhalten.

Schritt 6: Überwachen der Reputation Ihrer Anrufer-IDs

Wir empfehlen, die Reputation Ihrer Anrufer-IDs über einen Service wie Free Caller Registry zu überwachen.

Selbst bei den legitimesten Kampagnen für ausgehende Anrufe kennzeichnen einige Personen Ihre Anrufer-ID als Spam, wenn Sie genügend Anrufe tätigen. Dies kann sich auf zwei Arten manifestieren:

1. Automatisches Blockieren Blocklisten werden vendor-by-vendor auf Basis implementiert. Wenn beispielsweise bei Anwendungsanbietern wie Hiya.com auf Samsung-Geräten ein bestimmter Schwellenwert an Berichten erreicht wird, sind bis zu 20 % Ihrer potenziellen Kunden sofort nicht mehr erreichbar.
2. Beschwerden Personen können zahlreiche Websites verwenden, um sich über Anrufe von bestimmten Anrufer-IDs zu beschweren. Einige Ihrer potenziellen Kunden suchen online nach Ihrer Anrufer-ID, wenn Sie sie anrufen. Wenn sie einen schlechten Ruf hat, ist es weniger wahrscheinlich, dass sie den Anruf annehmen.

Der schnellste Weg, mit einer als Spam markierten Anrufer-ID umzugehen, besteht im Wechsel zu einer neuen Telefonnummer. Siehe nächster Schritt.

Schritt 7: Verwenden mehrerer Nummern als Anrufer-ID

Heute verfolgen Unternehmen in der Regel eine intelligentere, effizientere Art des Wählens.

Eine Methode verwendet beispielsweise mehrere Telefonnummern, wenn ausgehende Anrufe getätigt werden. Kunden nehmen einen Anruf eher an, wenn sie das Gefühl haben, nicht wiederholt von derselben Nummer angerufen zu werden.

Schritt 8: Kontakt mit App-Anbietern aufnehmen

Eines der derzeit größten Probleme der Branche besteht darin, dass eine große Anzahl von Anbietern In-App-Dienste zur Blockierung von Anrufen anbietet. Wenn einer dieser In-App-Services Ihre Nummer als Spam markiert, müssen Sie die Premium-Gebühren zahlen, um Ihre Nummer aus ihrer Spam-Liste zu entfernen.

Einige der Drittanbieter schließen sich zusammen, um die Anrufannahmeraten zu erhöhen.

Schritt 9: Ihrer Outreach-Strategie Nachrichten hinzufügen, damit Kunden wissen, wer Sie sind

Wenn Anrufe unbeantwortet bleiben, können Sie SMS verwenden, um potenzielle Kunden zu kontaktieren. Probieren Sie die folgenden Ideen aus, um die Antwortraten zu erhöhen.

1. Senden Sie vor dem Anruf eine SMS, die dem Kunden mitteilt, wer Sie sind und wann Sie anrufen werden. Erlauben Sie dem Kunden optional, auf einen bequemeren Zeitpunkt umzuplanen.
2. Wenn Interessenten nicht antworten, senden Sie eine SMS, damit sie den Anruf verschieben oder einen Rückruf anfordern können.
3. Nutzen Sie Werbeangebote oder Rabatte, die Ihren Interessenten entsprechen.

Schritt 10: Überprüfen Ihrer Strategie für ausgehende Anrufe

Wenn Sie datengestützte Entscheidungen treffen und kontinuierlich Varianten testen, haben Sie die beste Chance, echten Mehrwert zu erzielen. Behandeln Sie jede Änderung an Ihrer Strategie für ausgehende Anrufe als Experiment und stellen Sie sicher, dass Sie die Effektivität Ihrer Änderungen messen und vergleichen können.

Eines der besten Dinge an Amazon Connect ist, dass der Service jederzeit Experimente ermöglicht. Sie können eine Baseline erstellen und dann alle Änderungen vergleichen, um zu beurteilen, wie Sie erfolgreich sein können.

Amazon Chime SDK Voice Connectors verwalten

Was ist ein Amazon Chime SDK Voice Connector?

Ein Amazon Chime SDK Voice Connector bietet einen SIP-Trunking-Dienst (Session Initiation Protocol) für Ihr vorhandenes Telefonsystem. Sie können Ihre Voice Connectors von der Amazon Chime SDK-Konsole aus verwalten und über Ihre Internetverbindung darauf zugreifen, oder Sie können sie verwenden AWS Direct Connect. Weitere Informationen finden Sie unter Was ist AWS Direct Connect? im AWS Direct Connect -Benutzerhandbuch.

> **Important**
>
> Voice Connectors unterstützen keine SMS.

Ausgehende und eingehende Anrufe mit Voice Connector

Nachdem Sie einen Voice Connector erstellt haben, bearbeiten Sie die Einstellungen für Kündigung und Herkunft, um ausgehende oder eingehende Anrufe oder beides zuzulassen. Anschließend weisen Sie dem Voice Connector Telefonnummern zu. Sie können die Amazon Chime SDK-Konsole verwenden, um bestehende Telefonnummern zu portieren oder neue Telefonnummern bereitzustellen. Weitere Informationen finden Sie unter Portieren von Telefonnummern, Bereitstellen von Telefonnummern und Amazon Chime SDK Voice Connector-Telefonnummern zuweisen und deren Zuweisung aufheben.

> **Note**
>
> - Für Amazon Chime SDK Voice Connectors gelten Einschränkungen für ausgehende Auslandsgespräche. Weitere Informationen finden Sie unter Einschränkungen für ausgehende Anrufe.
> - Voice Connectors unterstützen ausgehende Anrufe im E.164-Format und benötigen keinen internationalen Wählcode wie 011. Sie zahlen einen Minutentarif, der vom Zielland des Anrufs abhängt. Eine aktuelle Liste der unterstützten Länder und den Minutentarif für jedes Land finden Sie unter https://aws.amazon.com/chime/voice-connector/pricing/. PSTN-Anrufe mit Voice Connector unterstützen keine privaten Nummerierungsschemata wie 4-, 5- oder 6-stellige Durchwahlnummern.

Voice Connector-Gruppen

Sie können auch eine Voice Connector-Gruppe erstellen und dieser Voice Connectors hinzufügen. Sie können Voice Connectors verwenden, die in verschiedenen AWS Regionen erstellt wurden. Dadurch entsteht ein fehlertoleranter Fallback-Mechanismus für den Fall, dass Verfügbarkeitsereignisse auftreten. Weitere Informationen finden Sie unter Amazon Chime SDK Voice Connector-Gruppen verwalten.

Protokollierung und Überwachung von Voice Connector-Daten

Optional können Sie Protokolle von Ihrem Voice Connector an CloudWatch Logs senden und Medienstreaming von Ihrem Amazon Chime SDK Voice Connector zu Amazon Kinesis aktivieren. Weitere Informationen finden Sie unter CloudWatch Protokolle für das Amazon Chime SDK und Amazon Chime SDK Voice Connector-Medien an Kinesis streamen.

Inhalt

Bevor Sie beginnen

Um einen Amazon Chime SDK Voice Connector verwenden zu können, benötigen Sie eine IP Private Branch Exchange (PBX), einen Session Border Controller (SBC) oder eine andere Sprachinfrastruktur mit Internetzugang, die das Session Initiation Protocol (SIP) unterstützt. Stellen Sie sicher, dass Sie über genügend Bandbreite verfügen, um das maximale Anrufvolumen zu unterstützen. Informationen zu den Banbreitenanforderungen siehe Anforderungen an die Bandbreite.

Um die Sicherheit von Anrufen AWS zu gewährleisten, die von Ihrem lokalen Telefonsystem gesendet werden, empfehlen wir, einen SBC zwischen AWS und Ihrem Telefonsystem zu konfigurieren. Liste des SIP-Datenverkehrs zum SBC über die Amazon Chime SDK Voice Connector-Signalisierung und Medien-IP-Adressen zulassen. Weitere Informationen enthalten die Abschnitte zu empfohlenen Ports und Protokollen in Amazon Chime SDK Sprachanschluss.

Amazon Chime SDK Voice Connectors erwarten, dass Telefonnummern im E.164-Format vorliegen.

Einen Amazon Chime SDK Voice Connector erstellen

Sie verwenden die Amazon Chime SDK-Konsole, um Amazon Chime SDK Voice Connectors zu erstellen.

Um einen Voice Connector zu erstellen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie Create new voice connector (Sprach-Connector erstellen) aus.
4. Geben Sie unter Name des Voice Connectors einen Namen für den Voice Connector ein.
5. Wählen Sie unter Verschlüsselung die Option Aktiviert oder Deaktiviert aus.
6. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus und gehen Sie dann wie folgt vor.

    1. Geben Sie unter Schlüssel den Schlüssel des Tags ein.
    2. Geben Sie unter Wert den Wert des Tags ein.
    3. Wählen Sie bei Bedarf Neues Tag hinzufügen aus, um dem Voice Connector weitere Tags hinzuzufügen.

    Weitere Informationen zu Stichwörtern finden Sie unterHinzufügen von Tags zu Voice Connectors.
7. Wählen Sie „Voice Connector erstellen“.

> **Note**
>
> Wenn Sie die Verschlüsselung aktivieren, wird Ihr Voice Connector so konfiguriert, dass er den TLS-Transport für die SIP-Signalisierung und Secure RTP (SRTP) für Medien verwendet. Eingehende Anrufe verwenden TLS-Transport und unverschlüsselte ausgehende Aufrufe werden blockiert.

Verwenden von Tags mit Voice Connectors

In den Themen in diesem Abschnitt wird erklärt, wie Sie Tags mit Ihren vorhandenen Amazon Chime SDK Voice Connectors verwenden. Mithilfe von Tags können Sie Ihren AWS Ressourcen, wie z. B. Voice Connectors, Metadaten zuweisen. Ein Tag besteht aus einem Schlüssel und einem optionalen Wert, der Informationen über die Ressource oder die auf dieser Ressource gespeicherten Daten speichert. Sie definieren alle Schlüssel und Werte. Sie können beispielsweise einen Tag-Schlüssel `CostCenter` mit dem Wert von erstellen `98765` und das Paar für die Kostenzuweisung verwenden. Sie können einem Voice Connector bis zu 50 Tags hinzufügen.

Hinzufügen von Tags zu Voice Connectors

Sie können Tags zu vorhandenen Amazon Chime SDK Voice Connectors hinzufügen.

Um Tags zu Voice Connectors hinzuzufügen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors, den Sie verwenden möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen und geben Sie dann einen Schlüssel und einen optionalen Wert ein.
6. Wählen Sie bei Bedarf Neues Tag hinzufügen aus, um ein weiteres Tag zu erstellen.
7. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Tags bearbeiten

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto bearbeiten, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So bearbeiten Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors, den Sie verwenden möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Geben Sie in den Feldern Schlüssel oder Wert einen neuen Wert ein.
6. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Entfernen von Tags

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto entfernen, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So entfernen Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors, den Sie verwenden möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Wählen Sie neben dem Tag, das Sie entfernen möchten, die Option Entfernen aus.
6. Wählen Sie Änderungen speichern aus.

Bearbeiten der Amazon Chime SDK Voice Connector-Einstellungen

Nachdem Sie einen Amazon Chime SDK Voice Connector erstellt haben, müssen Sie die Terminierungs- und Ausgangseinstellungen bearbeiten, die ausgehende und eingehende Anrufe zulassen. Sie können auch eine Reihe anderer Einstellungen konfigurieren, z. B. das Streamen zu Kinesis und die Verwendung von Notruf-Routing. Sie verwenden die Amazon Chime Chime-Konsole, um alle Einstellungen zu bearbeiten.

So bearbeiten Sie die Amazon Chime SDK Voice Connector-Einstellungen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Amazon Chime SDK Voice Connectors, den Sie bearbeiten möchten.
4. Die Amazon Chime Chime-Konsole gruppiert die Voice Connector-Einstellungen auf einer Reihe von Tabs. Erweitern Sie die folgenden Abschnitte, um Informationen zur Verwendung der einzelnen Tabs zu erhalten.

Allgemeine Einstellungen bearbeiten

Verwenden Sie die Registerkarte Allgemein, um den Namen eines Voice Connectors zu ändern, die Verschlüsselung zu aktivieren oder zu deaktivieren und das Wildcard-Root-Zertifikat in Ihre SIP-Infrastruktur zu importieren.

Um allgemeine Einstellungen zu ändern

1. (Optional) Geben Sie unter Details einen neuen Namen für den Voice Connector ein.
2. (Optional) Wählen Sie unter Verschlüsselung die Option Aktiviert oder Deaktiviert aus. Weitere Informationen zur Verschlüsselung finden Sie im nächsten Abschnitt.
3. Wählen Sie Speichern.
4. (Optional) Wählen Sie den Link Hier herunterladen, um das Wildcard-Stammzertifikat herunterzuladen. Wir gehen davon aus, dass Sie wissen, wie Sie es zu Ihrer SIP-Infrastruktur hinzufügen können.

Verschlüsselung mit Voice Connectors verwenden

Wenn Sie die Verschlüsselung für einen Amazon Chime SDK Voice Connector aktivieren, verwenden Sie TLS für die SIP-Signalisierung und Secure RTP (SRTP) für Medien. Der Voice Connector-Dienst verwendet den TLS-Port 5061.

Wenn diese Option aktiviert ist, verwenden alle eingehenden Anrufe TLS, und unverschlüsselte ausgehende Anrufe werden blockiert. Sie müssen das Amazon Chime Chime-Stammzertifikat importieren. Der Amazon Chime SDK Voice Connector-Service verwendet ein Wildcard-Zertifikat `*.voiceconnector.chime.aws` in US-Regionen und `*.region.vc.chime.aws` in anderen Regionen. Der Service wird beispielsweise `*.ap-southeast-1.vc.chime.aws` in der Region Asien-Pazifik (Singapur) verwendet. Wir implementieren SRTP wie in RFC 4568 beschrieben.

> **Note**
>
> Voice Connectors unterstützen TLS 1.2

Für ausgehende Anrufe verwendet der Dienst die AWS SRTP-Standardcounterchiffre und die HMAC-SHA1-Nachrichtenauthentifizierung. Wir unterstützen die folgenden Verschlüsselungssammlungen für eingehende und ausgehende Anrufe:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- AES_CM_192_HMAC_SHA1_80
- AES_CM_192_HMAC_SHA1_32
- AES_CM_256_HMAC_SHA1_80
- AES_CM_256_HMAC_SHA1_32

Sie müssen mindestens eine Chiffre verwenden, aber Sie können alle Chiffren in bevorzugter Reihenfolge angeben, ohne dass zusätzliche Kosten für die Voice Connector-Verschlüsselung anfallen.

Wir unterstützen auch diese zusätzlichen TLS-Verschlüsselungssammlungen:

- AES256-GCM-SHA384
- AES256-SHA256

- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256

Die Einstellungen für die Kündigung bearbeiten

Sie verwenden die Terminierungseinstellungen, um ausgehende Anrufe von Ihrem Amazon Chime SDK Voice Connector aus zu aktivieren und zu konfigurieren.

> **Note**
>
> Ihr ausgehender Hostname wird in eine Reihe von IP-Adressen aufgelöst, die sich ändern können, wenn EC2-Instances in Betrieb gehen oder außer Betrieb gehen. Daher sollten Sie Datensätze nicht länger als das DNS-Time-to-Live-Intervall zwischenspeichern. Ein längeres Zwischenspeichern kann zu Anruffehlern führen.

Wählen Sie erneut Save (Speichern) aus.

Um die Kündigungseinstellungen zu bearbeiten

1. Wählen Sie Enabled (Aktiviert).
2. (Optional) Wählen Sie unter Liste der zulässigen Hosts die Option Neu aus, geben Sie die CIDR-Notationen und Werte ein, die Sie zulassen möchten, und klicken Sie dann auf Hinzufügen. Beachten Sie, dass es sich bei den IP-Adresswerten um öffentlich routbare Adressen handeln muss.

-ODER-

Wählen Sie Bearbeiten und ändern Sie die CIDR-Notation.

-ODER-

Wählen Sie Löschen, um den Host zu entfernen.

3. Wählen Sie unter Anrufe pro Sekunde einen anderen Wert aus, falls verfügbar.
4. Öffnen Sie unter Anrufplan die Länderliste und wählen Sie die Länder aus, die der Voice Connector anrufen kann.
5. Wählen Sie unter Anmeldeinformationen die Option Neu aus, geben Sie einen Benutzernamen und ein Passwort ein und wählen Sie dann Speichern aus.
6. Wähle unter Anrufer-ID überschreiben die Option Bearbeiten, wähle eine Telefonnummer aus und wähle dann Speichern aus.
7. Sehen Sie sich unter Letzter Options-Ping die letzte SIP-Optionsnachricht an, die von Ihrer SIP-Infrastruktur gesendet wurde.

Ursprungseinstellungen bearbeiten

Die Ursprungseinstellungen gelten für eingehende Anrufe an Ihren Amazon Chime SDK Voice Connector. Sie können eingehende Routen für Ihre SIP-Hosts konfigurieren, um eingehende Anrufe entgegenzunehmen. Eingehende Anrufe werden basierend auf der für Hosts in der SIP-Infrastruktur festgelegten Priorität und Gewichtung an die Hosts weitergeleitet. Anrufe werden zuerst in der Reihenfolge ihrer Priorität weitergeleitet, wobei 1 die höchste Priorität hat. Wenn Hosts dieselbe Priorität haben, werden die Anrufe nach Maßgabe der relativen Gewichtung auf diese Hosts verteilt.

> **Note**
>
> Verschlüsselungsfähige Sprach-Connectors verwenden TLS (TCP-Protokoll) für alle Anrufe.

Um die Einstellungen für die Herkunft zu bearbeiten

1. Wählen Sie Enabled (Aktiviert).
2. Wählen Sie unter Eingehende Routen die Option Neu aus.

3. Geben Sie Werte für Host, Port, Protocol (Protokoll), Priority (Priorität) und Weight (Gewichtung) ein.
4. Wählen Sie Hinzufügen aus.
5. Wählen Sie Speichern.

Einstellungen für Notrufe bearbeiten

Um Notrufe zu aktivieren, müssen Sie zuerst die Einstellung und Notrufzustellung aktivieren. Informationen dazu finden Sie in den obigen Abschnitten.

Sie benötigen mindestens eine Notruf-Routing-Nummer von einem externen Notfalldienstanbieter, um diese Schritte ausführen zu können. Weitere Informationen zum Abrufen von Nummern finden Sie unterEinrichten von Notfall-Routing-Nummern von Drittanbietern.

Wählen Sie Hinzufügen aus.

So bearbeiten Sie die Einstellungen für Notrufe

1. Wählen Sie Hinzufügen aus.
2. Wählen Sie unter Methode zum Senden von Anrufen ein Element aus der Liste aus, falls verfügbar.
3. Geben Sie die Routing-Nummer für den Notfall ein.
4. Geben Sie die Test-Routing-Nummer ein. Wir empfehlen, eine Test-Routing-Nummer zu beantragen.
5. Wählen Sie unter Land das Land der Bankleitzahl aus, sofern verfügbar.
6. Wählen Sie Hinzufügen aus.

Telefonnummern bearbeiten

Sie können Voice Connector-Telefonnummern zuweisen und deren Zuweisung aufheben. Bei den folgenden Schritten wird davon ausgegangen, dass Sie mindestens eine Telefonnummer in Ihrem Amazon Chime Chime-Inventar haben. Falls nicht, siehe Bereitstellen von Telefonnummern.

Um Telefonnummern zuzuweisen

1. Wählen Sie Assign from inventory (Aus Verzeichnis zuweisen) aus.

2. Wählen Sie eine oder mehrere Telefonnummern aus.
3. Wählen Sie Assign from inventory (Aus Verzeichnis zuweisen) aus.

Die ausgewählten Nummern werden in Ihrer Nummernliste angezeigt.

Um die Zuweisung von Telefonnummern aufzuheben

1. Wählen Sie eine oder mehrere Telefonnummern aus.
2. Wählen Sie Unassign (Zuweisung aufheben) aus.
3. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, wählen Sie „Zuweisung aufheben“.

Streaming-Einstellungen bearbeiten

Die Streaming-Einstellungen aktivieren Amazon Kinesis Video Streams. Der Service speichert, verschlüsselt und indexiert Ihre Streaming-Audiodaten.

Um die Streaming-Einstellungen zu bearbeiten

1. Wählen Sie unter Details die Option Start aus.
2. Wählen Sie unter Streaming-Benachrichtigung ein oder mehrere Ziele aus den Listen aus.
3. Wählen Sie unter Datenaufbewahrungszeitraum die Option Keine Datenspeicherung aus, oder legen Sie ein Aufbewahrungsintervall fest.
4. Wählen Sie unter Call Insights die Option Aktivieren aus und gehen Sie dann wie folgt vor:
    1. Wählen Sie unter Zugriffsberechtigungen eine Rolle aus der Liste aus.
    2. Wählen Sie unter Kinesis Data Stream einen Stream aus der Liste aus.
    3. (Optional) Wählen Sie unter Benutzerdefiniertes Amazon Transcribe Transcribe-Sprachmodell ein Modell aus der Liste aus.
    4. Wählen Sie unter Typ personenbezogener Daten eine Option aus.
    5. Wählen Sie unter Teilergebnisse filtern eine Option aus.
    6. Wählen Sie unter Echtzeitbenachrichtigung senden die Option Start und anschließend eine Option aus den Listen Anrufrichtung und Sprecher aus.
    7. Wählen Sie bei Bedarf „Wort/Wortgruppe hinzufügen“ und geben Sie dann das Wort oder die Wortgruppe ein, über das bzw. den Sie benachrichtigt werden möchten.
5. Wählen Sie Speichern.

Protokollierungseinstellungen bearbeiten

Das Amazon Chime SDK deaktiviert standardmäßig die Protokollierung für Voice Connectors. Wenn Sie die Protokollierung aktivieren, sendet das System die Daten an eine CloudWatch Amazon-Protokollgruppe. Weitere Informationen zur Protokollierung finden Sie unter Überwachung des Amazon Chime SDK mit Amazon CloudWatch

So bearbeiten Sie die Protokollierungseinstellungen

1. Wählen Sie unter SIP-Metrikprotokolle die Option Aktiviert aus.
2. Wählen Sie unter Media Metric Logs die Option Aktiviert aus.

Tag-Einstellungen bearbeiten

Sie können einem Voice Connector 50 Tags hinzufügen und die Tasten und optionalen Werte für die Tags auswählen.

Um die Tag-Einstellungen zu bearbeiten

1. Wählen Sie Tags verwalten aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann einen Schlüssel und einen optionalen Wert ein.
   - Um ein Tag zu entfernen, wähle neben dem Tag, das du löschen möchtest, die Option Entfernen aus.
3. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Amazon Chime SDK Voice Connector-Telefonnummern zuweisen und deren Zuweisung aufheben

Sie können einem Amazon Chime SDK Voice Connector Telefonnummern zuweisen und deren Zuweisung aufheben.

Um Telefonnummern zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors.
4. Wählen Sie Phone numbers (Telefonnummern) aus.
5. Wählen Sie eine oder mehrere Telefonnummern aus, die Sie dem Voice Connector zuweisen möchten.
6. Wählen Sie Assign (Zuweisen).

Sie können auch „Neu zuweisen“ wählen, um Telefonnummern mit dem Produkttyp Voice Connector von einer Voice Connector - oder Voice Connector-Gruppe einer anderen neu zuzuweisen.

Um die Zuweisung von Telefonnummern aufzuheben

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors.
4. Wählen Sie Phone numbers (Telefonnummern) aus.
5. Wählen Sie eine oder mehrere Telefonnummern aus, deren Zuweisung zum Voice Connector aufgehoben werden soll.
6. Wählen Sie Unassign (Zuweisung aufheben) aus.
7. Aktivieren Sie das Kontrollkästchen und wählen Sie Unassign (Zuweisung aufheben) aus.

Löschen eines Amazon Chime SDK Voice Connectors

Bevor Sie einen Amazon Chime SDK Voice Connector löschen können, müssen Sie die Zuweisung aller Telefonnummern aufheben. Weitere Informationen zum Aufheben der Zuweisung von Telefonnummern zu einem Voice Connector finden Sie im vorherigen Thema.

Um einen Voice Connector zu löschen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie Phone numbers (Telefonnummern), Delete voice connector (Sprach-Connector löschen) aus.
4. Aktivieren Sie das Kontrollkästchen und wählen Sie Delete (Löschen) aus.

Konfiguration von Voice Connectors für die Verwendung von Anrufanalysen

> **Note**
>
> Um die Schritte in diesem Abschnitt abzuschließen, müssen Sie zunächst eine Konfiguration für Anrufanalysen erstellen. Informationen zum Erstellen von Konfigurationen finden Sie unterKonfigurationen für Anrufanalysen erstellen.

Sie können Amazon Chime SDK Call Analytics mit Amazon Chime SDK Voice Connector verwenden, um automatisch Erkenntnisse mit Amazon Transcribe und Amazon Transcribe Call Analytics mit Sprachanalyse zu generieren. Dazu verknüpfen Sie Ihre Konfiguration für Anrufanalysen mit einem Amazon Chime SDK Voice Connector. Für jeden Anruf ruft der Voice Connector die Anrufanalyse gemäß der von Ihnen angegebenen Konfiguration auf. Sie können eine Konfiguration mehreren Voice Connectors zuordnen oder für jeden Voice Connector eine eigene Konfiguration erstellen.

Call Analytics verwendet die serviceverknüpfte Rolle Amazon Chime Voice Connector, um die CreateMediaInsightsPipelineAPI in Ihrem Namen aufzurufen.

Um einen Voice Connector zu konfigurieren

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors aus, den Sie einer Konfiguration zuordnen möchten, und wählen Sie dann die Registerkarte Streaming.

4. Falls es noch nicht ausgewählt ist, wählen Sie Start, um mit dem Streaming zu Kinesis Video Streams zu beginnen.
5. Wählen Sie unter Call Analytics die Option Aktivieren aus und wählen Sie im daraufhin angezeigten Menü Ihren Call Analytics-Konfigurations-ARN aus.
6. Wählen Sie Speichern.

> **Note**
>
> Warten Sie nach dem Aktivieren, Deaktivieren oder Ändern einer mit einem Voice Connector verknüpften Konfiguration 5 Minuten, bis die neuen Einstellungen über den Dienst verbreitet werden und wirksam werden.

Amazon Chime SDK Voice Connector-Gruppen verwalten

So funktioniert eine Amazon Chime SDK Voice Connector-Gruppe

Voice Connector-Gruppen verarbeiten nur eingehende PSTN-Anrufe an Ihr SIP-basiertes Telefonsystem. Die Gruppen bieten eine fehlertolerante, regionsübergreifende Anrufweiterleitung. Eine Voice Connector-Gruppe enthält zwei oder mehr Voice Connectors und kann Voice Connectors enthalten, die in verschiedenen Regionen erstellt wurden. AWS Auf diese Weise kann bei eingehenden PSTN-Anrufen ein regionsübergreifendes Failover erfolgen, falls Verfügbarkeitsereignisse den Service in einer AWS Region beeinträchtigen.

Angenommen, Sie erstellen eine Voice Connector-Gruppe und weisen ihr zwei Voice Connectors zu, einen in der Region USA Ost (Nord-Virginia) und den anderen in der Region USA West (Oregon). Sie konfigurieren beide Voice Connectors mit Ursprungseinstellungen, die auf Ihre (n) SIP-Host (s) verweisen.

Nehmen wir nun an, dass ein Anruf beim Voice Connector in der Region USA Ost (Nord-Virginia) eingeht. Wenn in dieser Region ein Verbindungsproblem besteht, wird der Anruf automatisch an den Voice Connector in der Region USA West (Oregon) umgeleitet.

Erste Schritte mit einer Amazon Chime SDK Voice Connector-Gruppe

Erstellen Sie zunächst Voice Connectors in verschiedenen AWS Regionen. Erstellen Sie dann eine Voice Connector-Gruppe und weisen Sie ihr die Voice Connectors zu. Sie können

auch Telefonnummern für Ihre Voice Connector-Gruppe aus Ihrem Amazon Chime SDK-Telefonnummernverwaltungsbestand bereitstellen. Weitere Informationen finden Sie unter Bereitstellen von Telefonnummern. Weitere Informationen zur Erstellung von Amazon Chime SDK Voice Connectors in verschiedenen AWS Regionen finden Sie unterAmazon Chime SDK Voice Connectors verwalten.

Inhalt

Eine Amazon Chime SDK Voice Connector-Gruppe erstellen

Sie können bis zu drei Amazon Chime SDK Voice Connector-Gruppen für Ihr Konto erstellen.

So erstellen Sie eine Gruppe

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie Create group (Gruppe erstellen) aus.
4. Geben Sie im daraufhin angezeigten Dialogfeld unter Name der Voice Connector-Gruppe einen Namen für die Gruppe ein.
5. Wählen Sie Erstellen.

Bearbeiten einer Amazon Chime SDK Voice Connector-Gruppe

Nachdem Sie eine Amazon Chime SDK Voice Connector-Gruppe erstellt haben, können Sie Amazon Chime SDK Voice Connectors für diese Gruppe hinzufügen oder entfernen. Sie können auch die Priorität für die Voice Connectors in der Gruppe bearbeiten.

Um Voice Connectors zu einer Gruppe hinzuzufügen

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

2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der Voice Connector-Gruppe aus, die Sie bearbeiten möchten.
4. Wählen Sie den Tab Voice Connectors, öffnen Sie die Aktionsliste und wählen Sie dann Hinzufügen.
5. Wählen Sie im daraufhin angezeigten Dialogfeld das Kontrollkästchen neben dem Voice Connector aus, den Sie verwenden möchten.
6. Wählen Sie Hinzufügen aus.
7. Wiederholen Sie die Schritte 4 bis 6, um Voice Connectors zur Gruppe hinzuzufügen.

Um die Voice Connector-Priorität in einer Gruppe zu bearbeiten

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der Amazon Chime SDK Voice Connector-Gruppe, die Sie bearbeiten möchten.
4. Wählen Sie unter Aktionen die Option Priorität bearbeiten aus.
5. Geben Sie im daraufhin angezeigten Dialogfeld für jeden Voice Connector eine andere Prioritätsrangfolge ein. 1 ist die höchste Priorität. Voice Connectors mit höherer Priorität werden zuerst versucht.
6. Wählen Sie Speichern.

Um Voice Connectors aus einer Gruppe zu entfernen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der Voice Connector-Gruppe aus, die Sie bearbeiten möchten.
4. Öffnen Sie die Aktionsliste und wählen Sie Entfernen.
5. Aktivieren Sie im daraufhin angezeigten Dialogfeld die Kontrollkästchen neben den Voice Connectors, die Sie entfernen möchten.
6. Wählen Sie Remove (Entfernen) aus.

Zuweisen und Aufheben der Zuweisung von Telefonnummern zu einer Voice Connector-Gruppe

Sie verwenden die Amazon Chime SDK-Konsole, um einer Voice Connector-Gruppe Telefonnummern zuzuweisen oder deren Zuweisung aufzuheben.

Um einer Voice Connector-Gruppe Telefonnummern zuzuweisen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der Voice Connector-Gruppe aus, die Sie bearbeiten möchten.
4. Wählen Sie Phone numbers (Telefonnummern) aus.
5. Wählen Sie Assign from inventory (Aus Verzeichnis zuweisen) aus.
6. Wählen Sie eine oder mehrere Telefonnummern aus, die Sie der Voice Connector-Gruppe zuweisen möchten.
7. Wählen Sie Assign from inventory (Aus Verzeichnis zuweisen) aus.

Sie können auch Reassign (Neu zuweisen) wählen, um Rufnummern mit dem Produkttyp Voice Connector (Sprach-Connector) neu zuzuweisen. Auf diese Weise können Sie diese Nummern von einer Voice Connector- oder Voice Connector-Gruppe einer anderen neu zuweisen.

Um die Zuweisung von Telefonnummern zu einer Voice Connector-Gruppe aufzuheben

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der Voice Connector-Gruppe aus, die Sie bearbeiten möchten.
4. Wählen Sie Phone numbers (Telefonnummern) aus.
5. Wählen Sie die gewünschten Telefonnummern aus der Voice Connector-Gruppe aus und wählen Sie Zuweisung aufheben aus.
6. Wählen Sie Unassign (Zuweisung aufheben) aus.

Löschen einer Amazon Chime SDK Voice Connector-Gruppe

Bevor Sie eine Amazon Chime SDK Voice Connector-Gruppe löschen können, müssen Sie die Zuweisung aller Amazon Chime SDK Voice Connectors und Telefonnummern zu dieser Gruppe aufheben. Weitere Informationen finden Sie im vorhergehenden Abschnitt .

Um eine Voice Connector-Gruppe zu löschen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen der zu löschenden Voice Connector-Gruppe aus.
4. Wählen Sie Delete group (Gruppe löschen) aus.
5. Aktivieren Sie das Kontrollkästchen und wählen Sie Delete (Löschen) aus.

Amazon Chime SDK Voice Connector-Medien an Kinesis streamen

Sie können Telefonanruf-Audio von Amazon Chime SDK Voice Connectors zu Amazon Kinesis Video Streams für Analysen, maschinelles Lernen und andere Verarbeitungsvorgänge streamen. Entwickler können Audiodaten in Kinesis Video Streams speichern und verschlüsseln und mithilfe der Kinesis Video Streams Streams-API-Operation auf die Daten zugreifen. Weitere Informationen finden Sie im Kinesis Video Streams Developer Guide.

> **Note**
>
> - Das Voice Connector-Streaming schränkt die Formate von Telefonnummern nicht ein. Sie können Anrufe von Nummern in den Formaten E.164 und anderen Formaten streamen. Voice Connector-Streaming kann beispielsweise 4-, 5- oder 6-stellige Durchwahlnummern oder 11-stellige private Leitungsnummern unterstützen. Weitere Informationen finden Sie weiter unten SIP-basierte Medienaufnahme und netzwerkbasierte Aufnahmekompatibilität in diesem Handbuch.
> - Das Voice Connector-Streaming unterstützt die Audiokodierung G.711 A-law und G.711 μ-Law.

Verwenden Sie die Amazon Chime SDK-Konsole, um das Medienstreaming für Ihren Voice Connector zu starten. Wenn das Medienstreaming beginnt, verwendet Ihr Voice Connector eine dienstbezogene AWS Identity and Access Management (IAM) -Rolle, um Berechtigungen zum Streamen von Medien an Kinesis Video Streams zu gewähren. Anschließend wird das Anruf-Audio von jedem Voice Connector-Telefonanrufabschnitt in Echtzeit in separate Kinesis Video Streams gestreamt.

Verwenden Sie die Kinesis Video Streams Parser-Bibliothek, um die von Ihrem Voice Connector gesendeten Medienstreams herunterzuladen. Filtern Sie die Streams nach den folgenden Metadaten für persistente Fragmente:

- TransactionId
- VoiceConnectorId

Weitere Informationen finden Sie unter Kinesis Video Streams Parser Library und Verwenden von Streaming-Metadaten mit Kinesis Video Streams im Amazon Kinesis Video Streams Developer Guide.

Weitere Informationen zur Verwendung von dienstbezogenen IAM-Rollen mit Voice Connectors finden Sie unter. Verwenden der Richtlinie für verknüpfte Rollen mit dem Amazon Chime SDK Voice Connector-Service Weitere Informationen zur Verwendung von Amazon CloudWatch mit dem Amazon Chime SDK finden Sie unterProtokollierung und Überwachung im Amazon Chime SDK.

Wenn Sie Medienstreaming für Ihren Voice Connector aktivieren, erstellt das Amazon Chime SDK eine mit dem IAM-Dienst verknüpfte Rolle namens. AWSServiceRoleForAmazonChimeVoiceConnector Wenn Sie die Protokollierung von Anrufdetailaufzeichnungen für Voice Connectors in der Amazon Chime SDK-Konsole konfiguriert haben, werden Streaming-Detailaufzeichnungen an Ihren konfigurierten Amazon S3 S3-Bucket gesendet. Weitere Informationen finden Sie unter Streaming-Detaildatensätze für Amazon Chime SDK Voice Connector.

Starten von Medien-Streaming

Sie verwenden die Amazon Chime SDK-Konsole, um das Medienstreaming für einen Voice Connector zu starten.

Um das Medienstreaming zu starten

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors.
4. Wählen Sie den Tab Streaming.
5. Wählen Sie im Abschnitt Details unter An Kinesis Video Streams senden die Option Start aus.
6. Wählen Sie unter Datenaufbewahrungszeitraum die Option Daten aufbewahren für aus und geben Sie einen Aufbewahrungszeitraum ein.
7. Wählen Sie Speichern.

Sie verwenden die Amazon Chime SDK-Konsole, um das Medienstreaming zu deaktivieren. Wenn Sie Medienstreaming für keinen Ihrer Voice Connectors mehr verwenden müssen, empfehlen wir Ihnen, auch die zugehörige dienstbezogene Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle für Amazon Chime SDK Voice Connectors.

Um das Medienstreaming für Ihren Voice Connector zu beenden

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
3. Wählen Sie den Namen des Voice Connectors.
4. Wählen Sie den Tab Streaming.
5. Wählen Sie im Abschnitt Details unter An Kinesis Video Streams senden die Option Stopp aus.
6. Wählen Sie Speichern.

SIP-basierte Medienaufnahme und netzwerkbasierte Aufnahmekompatibilität

Sie können einen Amazon Chime SDK Voice Connector verwenden, um Medien zu Kinesis Video Streams zu streamen. Sie können über eine SIP-basierte Medienaufzeichnungsfunktion (SIPREC) oder über die Netzwerkaufzeichnungsfunktion (NBR) streamen, die mit Cisco Unified Border Element (CUBE) verknüpft ist.

Sie benötigen eine Nebenstellenanlage (Private Branch Exchange, PBX), einen SBC (Session Border Controller) oder ein Kontaktcenter, von dem das SIPREC-Protokoll oder die NBR-Funktion unterstützt wird. Die PBX oder SBC muss in der Lage sein, Signale und Medien an öffentliche IP-Adressen zu senden. AWS Weitere Informationen finden Sie unter Bevor Sie beginnen.

So richten Sie das Streaming von RTP-Audio-Streams ein, die mit SIPREC oder NBR geforkt sind

1. Erstellen Sie einen Voice Connector. Weitere Informationen finden Sie unter Einen Amazon Chime SDK Voice Connector erstellen.
2. Starten Sie das Medienstreaming für Ihren Amazon Chime SDK Voice Connector. Weitere Informationen finden Sie unter Starten von Medien-Streaming.
3. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
4. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Voice Connectors aus.
5. Wählen Sie den Voice Connector aus und notieren Sie sich den Namen des ausgehenden Hosts. z. B. *abcdef1ghij2klmno3pqr4*`.voiceconnector.chime.aws`.
6. Führen Sie eine der folgenden Aktionen aus:

   - Für SIPREC — Konfigurieren Sie Ihre PBX, SBC oder eine andere Sprachinfrastruktur so, dass RTP-Streams mit SIPREC an den ausgehenden Hostnamen Ihres Voice Connectors weitergeleitet werden.
   - Für NBR — Konfigurieren Sie Ihre PBX-, SBC- oder andere Sprachinfrastruktur so, dass RTP-Streams mit NBR an den ausgehenden Hostnamen Ihres Voice Connectors weitergeleitet werden. Senden Sie einen zusätzlichen Header- oder URI-Parameter von `X-Voice-Connector-Record-Only` mit dem Wert `true` in `SIP INVITE`.

Verwenden von Amazon Chime SDK-Sprachanalysen mit Voice Connectors

Sie verwenden die Amazon Chime SDK-Anrufanalysen mit Ihren Voice Connectors, um automatisch Einblicke in Ihre Anrufe zu gewinnen. Insbesondere können Sie Benutzer identifizieren und ihren positiven, negativen oder neutralen Ton vorhersagen.

Call Analytics funktioniert mit Amazon Transcribe, Amazon Transcribe Call Analytics und Amazon Chime SDK Voice Analytics.

Der Prozess folgt diesen allgemeinen Schritten:

1. Erstellen Sie eine Konfiguration für die Anrufanalyse, eine statische Struktur, die die Anweisungen für die Datenverarbeitung enthält.
2. Ordnen Sie die Konfiguration einem oder mehreren Voice Connectors zu. Sie können eine Konfiguration mehreren Voice Connectors zuordnen oder für jeden Voice Connector eine eigene Konfiguration erstellen.
3. Der Voice Connector ruft die Anrufanalyse entsprechend der Konfiguration auf.

Call Analytics verwendet die serviceverknüpfte Rolle Amazon Chime Voice Connector, um die CreateMediaInsightsPipelineAPI in Ihrem Namen aufzurufen.

> **Note**
>
> In den folgenden Schritten wird erklärt, wie Sie eine Anrufanalysesitzung mit einem Voice Connector verknüpfen. Um sie abzuschließen, müssen Sie zunächst eine Konfiguration für die Anrufanalyse erstellen. Informationen dazu finden Sie Konfigurationen für Anrufanalysen erstellen in diesem Handbuch. Der Erstellungsprozess weist der Konfiguration einen ARN zu. Kopieren Sie den ARN zur Verwendung in diesen Schritten.

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking Voice Connectors und dann einen Voice Connector aus.
3. Wählen Sie den Tab „Streaming“.
4. Wählen Sie unter An Kinesis Video Streams senden die Option Start aus.
5. Wählen Sie unter Call Analytics die Option Aktivieren, wählen Sie eine Konfiguration aus der Liste aus und klicken Sie dann auf Speichern.

Verwenden von Amazon Chime SDK Voice Connector-Konfigurationsleitfäden

Wir testen Amazon Chime SDK Voice Connectors auf einer Vielzahl von Systemen für private Zweigstellen, Session Border Controller und Contact Center. Wir veröffentlichen diese getesteten Konfigurationen in einer Reihe von Konfigurationshandbüchern.

Die Konfigurationsanleitungen behandeln die Konfigurationsschritte, die für jeden Systemtest verwendet werden. Wir führen diese Arten von Tests durch:

- Aktivieren Sie SIP-Trunking über einen Voice Connector von einer SIP-Plattform eines Drittanbieters aus.
- Aktivieren Sie SIPREC über einen Voice Connector für die Verwendung mit Audiostreams.

Weitere Informationen finden Sie in den Amazon Chime SDK-Konfigurationsleitfäden.

Verwaltung der Amazon Chime SDK-Anrufanalysen

In den Themen in diesem Abschnitt wird erklärt, wie Sie die Amazon Chime SDK-Anrufanalysen verwalten. Sie verwenden Anrufanalysen, um anhand von Audiodaten in Echtzeit Erkenntnisse zu Anrufen zu generieren. Sie können auch gespeicherte Anrufe analysieren. Darüber hinaus können Sie die Sprachanalyse des Amazon Chime SDK verwenden, um Anrufer zu identifizieren und ihre positive, negative oder neutrale Stimmung vorherzusagen.

Themen

Konfigurationen für Anrufanalysen erstellen

Um Anrufanalysen zu verwenden, erstellen Sie zunächst eine Konfiguration, eine statische Struktur, die die Informationen enthält, die zum Erstellen einer Anrufanalyse-Pipeline erforderlich sind. Sie können die Amazon Chime SDK-Konsole verwenden, um eine Konfiguration zu erstellen, oder die CreateMediaInsightsPipelineConfigurationAPI aufrufen.

Eine Konfiguration für Anrufanalysen umfasst Details zu Audioprozessoren, z. B. Aufzeichnung, Sprachanalyse oder Amazon Transcribe. Sie umfasst auch Insight-Ziele und die Konfiguration von Alarmereignissen. Optional können Sie Ihre Anrufdaten zur weiteren Analyse in einem Amazon S3 S3-Bucket speichern.

Konfigurationen beinhalten jedoch keine spezifischen Audioquellen. Auf diese Weise können Sie die Konfiguration in mehreren Anrufanalyse-Workflows wiederverwenden. Sie können beispielsweise dieselbe Konfiguration für Anrufanalysen mit unterschiedlichen Voice Connectors oder für verschiedene Amazon Kinesis Video Streams (KVS) -Quellen verwenden.

Sie verwenden die Konfigurationen, um Pipelines zu erstellen, wenn SIP-Anrufe über einen Voice Connector erfolgen oder wenn neue Medien an einen Amazon Kinesis Video Stream (KVS)

gesendet werden. Die Pipelines wiederum verarbeiten die Medien gemäß den Spezifikationen in der Konfiguration.

Sie können eine Pipeline jederzeit programmgesteuert beenden. Pipelines beenden auch die Medienverarbeitung, wenn ein Voice Connector-Anruf beendet wird. Darüber hinaus können Sie eine Pipeline anhalten. Dadurch werden Aufrufe der zugrunde liegenden Amazon Machine Learning-Dienste deaktiviert und bei Bedarf wieder aufgenommen. Die Anrufaufzeichnung wird jedoch ausgeführt, während Sie eine Pipeline anhalten.

Themen

Voraussetzungen

Um Anrufanalysen mit Amazon Transcribe, Amazon Transcribe Analytics oder Amazon Chime SDK Voice Analytics verwenden zu können, benötigen Sie die folgenden Voraussetzungen:

- Ein Amazon Chime SDK Voice Connector. Falls nichtEinen Amazon Chime SDK Voice Connector erstellen, finden Sie weitere Informationen weiter oben in diesem Handbuch.
- EventBridge Amazon-Ziele. Falls nicht, lesen Sie Überwachung des Amazon Chime SDK mit Amazon CloudWatch weiter oben in diesem Handbuch nach.
- Eine dienstbezogene Rolle, die es dem Voice Connector ermöglicht, auf Aktionen auf den EventBridge Zielen zuzugreifen. Weitere Informationen finden Sie weiter Verwenden der Richtlinie für verknüpfte Rollen mit dem Amazon Chime SDK Voice Connector-Service oben in diesem Handbuch.
- Ein Amazon Kinesis Kinesis-Datenstream. Falls nicht, finden Sie weitere Informationen unter Erstellen eines Kinesis-Videostreams im Amazon Kinesis Video Stream-Entwicklerhandbuch. Sprachanalyse und Transkription erfordern einen Kinesis-Stream.
- Um Anrufe offline zu analysieren, müssen Sie einen Amazon Chime SDK-Data Lake erstellen. Informationen dazu finden Sie unter Creating an Amazon Chime SDK Data Lake im Amazon Chime SDK Developer Guide.

Konfiguration für Anrufanalysen erstellen

Nachdem Sie die Konfiguration erstellt haben, aktivieren Sie die Anrufanalyse, indem Sie der Konfiguration einen Voice Connector zuordnen. Sobald Sie dies getan haben, wird die Anrufanalyse automatisch gestartet, wenn ein Anruf bei diesem Voice Connector eingeht. Weitere Informationen finden Sie weiter Konfiguration von Voice Connectors für die Verwendung von Anrufanalysen oben in diesem Handbuch.

In den folgenden Abschnitten wird erklärt, wie Sie die einzelnen Schritte des Prozesses abschließen. Erweitern Sie sie in der angegebenen Reihenfolge.

Geben Sie die Konfigurationsdetails an

Um Konfigurationsdetails anzugeben

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Call Analytics die Option Configurations und anschließend Create configuration aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:

    a. Geben Sie einen Namen für die Konfiguration ein. Der Name sollte Ihren Anwendungsfall und alle Tags widerspiegeln.

    b. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus und geben Sie dann Ihre Tag-Schlüssel und optionalen Werte ein. Sie definieren die Schlüssel und Werte. Mithilfe von Tags können Sie die Konfiguration abfragen.

    c. Wählen Sie Weiter aus.

Aufnahme konfigurieren

Um die Aufnahme zu konfigurieren

- Gehen Sie auf der Seite Aufzeichnung konfigurieren wie folgt vor:

    a. Wählen Sie das Kontrollkästchen Anrufaufzeichnung aktivieren aus. Dies ermöglicht die Aufzeichnung von Voice Connector-Anrufen oder KVS-Streams und das Senden der Daten an Ihren Amazon S3 S3-Bucket.

b. Wählen Sie unter Dateiformat die Option WAV mit PCM aus, um die beste Audioqualität zu erzielen.

   –oder–

   Wählen Sie OGG mit OPUS, um das Audio zu komprimieren und den Speicher zu optimieren.

c. (Optional) Wählen Sie bei Bedarf den Link Amazon S3 S3-Bucket erstellen und folgen Sie diesen Schritten, um einen Amazon S3 S3-Bucket zu erstellen.

d. Geben Sie die URI Ihres Amazon S3 S3-Buckets ein, oder wählen Sie Durchsuchen, um nach einem Bucket zu suchen.

e. (Optional) Wählen Sie Sprachverbesserung aktivieren, um die Audioqualität Ihrer Aufnahmen zu verbessern.

f. Wählen Sie Weiter aus.

Weitere Informationen zur Sprachverbesserung finden Sie im nächsten Abschnitt.

Grundlegendes zur Sprachverbesserung

Die Sprachverbesserung trägt dazu bei, die Audioqualität der aufgezeichneten Telefonanrufe in den Amazon S3 S3-Buckets Ihrer Kunden zu verbessern. Telefonanrufe werden schmalbandgefiltert und mit einer Rate von 8 kHz abgetastet. Die Sprachverbesserung erhöht die Abtastrate von 8 kHz auf 16 kHz und verwendet ein Modell für maschinelles Lernen, um den Frequenzinhalt von Schmalband auf Breitband zu erweitern, sodass die Sprache natürlicher klingt. Die Sprachverbesserung verwendet auch ein Geräuschreduzierungsmodell namens Amazon Voice Focus, um Hintergrundgeräusche im verbesserten Audio zu reduzieren.

Wenn die Sprachverbesserung aktiviert ist, wird die Verarbeitung der Sprachverbesserung durchgeführt, nachdem die Anrufaufzeichnung abgeschlossen ist. Die erweiterte Audiodatei wird als Originalaufnahme in Ihren Amazon S3 S3-Bucket geschrieben und dem Basisdateinamen der Originalaufnahme wird das Suffix _enhanced hinzugefügt. Mit der Sprachverbesserung können Anrufe mit einer Länge von bis zu 30 Minuten bearbeitet werden. Für Anrufe, die länger als 30 Minuten dauern, werden keine verbesserten Aufzeichnungen generiert.

Informationen zur programmgesteuerten Verwendung der Sprachverbesserung finden Sie unter Verwenden von APIs zur Erstellung von Konfigurationen für Anrufanalysen im Amazon Chime SDK Developer Guide.

Weitere Informationen zur Sprachverbesserung finden Sie unter Grundlegendes zur Sprachverbesserung auf https://docs.aws.amazon.com/chime/latest/dg/.

Konfigurieren Sie Analysedienste

Amazon Transcribe bietet Texttranskriptionen von Anrufen. Sie können die Transkripte dann verwenden, um andere Machine-Learning-Dienste wie Amazon Comprehend oder Ihre eigenen Machine-Learning-Modelle zu erweitern.

> **Note**
>
> Amazon Transcribe bietet auch automatische Spracherkennung. Sie können diese Funktion jedoch nicht mit benutzerdefinierten Sprachmodellen oder der Redaktion von Inhalten verwenden. Wenn Sie die Sprachenidentifikation zusammen mit anderen Funktionen verwenden, können Sie außerdem nur die Sprachen verwenden, die von diesen Funktionen unterstützt werden. Weitere Informationen finden Sie unter Sprachenidentifikation mit Streaming-Transkriptionen im Amazon Transcribe Developer Guide.

Amazon Transcribe Call Analytics ist eine auf maschinellem Lernen basierende API, die Gesprächsprotokolle, Stimmungen und Einblicke in Konversationen in Echtzeit bietet. Der Service macht das Notieren überflüssig und ermöglicht sofortige Maßnahmen bei erkannten Problemen. Der Service bietet auch Analysen nach dem Anruf, z. B. zur Stimmung des Anrufers, zu Anrufern, zur Gesprächszeit, zu Unterbrechungen, zur Gesprächsgeschwindigkeit und zu Gesprächsmerkmalen.

> **Note**
>
> Standardmäßig streamt die Analyse nach dem Anruf Anrufaufzeichnungen in Ihren Amazon S3 S3-Bucket. Um zu vermeiden, dass doppelte Aufzeichnungen erstellt werden, sollten Sie die Anrufaufzeichnung und die Analyse nach dem Anruf nicht gleichzeitig aktivieren.

Schließlich kann Transcribe Call Analytics Konversationen anhand bestimmter Phrasen automatisch kennzeichnen und dabei helfen, vertrauliche Informationen aus Audio und Text zu redigieren. Weitere Informationen zu den Medienprozessoren für Anrufanalysen, den von diesen Prozessoren generierten Erkenntnissen und Ausgabezielen finden Sie unter Call Analytics processor and output targets im Amazon Chime SDK Developer Guide.

Um Analysedienste zu konfigurieren

1. Aktivieren Sie auf der Seite Analysedienste konfigurieren die Kontrollkästchen neben Sprachanalyse oder Transkriptionsdienste. Sie können beide Elemente auswählen.

   Aktivieren Sie das Kontrollkästchen Sprachanalyse, um eine beliebige Kombination aus Lautsprechersuche und Stimmenanalyse zu aktivieren.

   Markieren Sie das Kontrollkästchen Transkriptionsdienste, um Amazon Transcribe oder Transcribe Call Analytics zu aktivieren.

   a. Um die Lautsprechersuche zu aktivieren

      - Aktivieren Sie das Kontrollkästchen Ja, ich stimme der Zustimmungsbestätigung für Amazon Chime SDK Voice Analytics zu und wählen Sie dann Akzeptieren aus.

   b. Um die Stimmenanalyse zu aktivieren

      - Wählen Sie das Kontrollkästchen Stimmenanalyse aus.

   c. Um Amazon Transcribe zu aktivieren

      i. Wählen Sie die Schaltfläche Amazon Transcribe.

      ii. Führen Sie unter Spracheinstellungen einen der folgenden Schritte aus:

         A. Wenn Ihre Anrufer nur eine Sprache sprechen, wählen Sie Bestimmte Sprache aus, öffnen Sie dann die Sprachenliste und wählen Sie die Sprache aus.

         B. Wenn deine Anrufer mehrere Sprachen sprechen, kannst du sie automatisch identifizieren. Wählen Sie Automatische Spracherkennung.

         C. Öffnen Sie die Liste Sprachoptionen für die automatische Sprachenidentifikation und wählen Sie mindestens zwei Sprachen aus.

         D. (Optional) Öffnen Sie die Liste der bevorzugten Sprachen und geben Sie eine bevorzugte Sprache an. Wenn die im vorherigen Schritt ausgewählten Sprachen übereinstimmende Konfidenzwerte aufweisen, transkribiert der Service die bevorzugte Sprache.

         E. (Optional) Erweitern Sie die Einstellungen zum Entfernen von Inhalten, wählen Sie eine oder mehrere Optionen aus und wählen Sie dann eine oder mehrere der zusätzlichen Optionen aus, die angezeigt werden. Der Hilfstext erklärt jede Option.

F. (Optional) Erweitern Sie Zusätzliche Einstellungen, wählen Sie eine oder mehrere Optionen aus und wählen Sie dann eine oder mehrere der zusätzlichen Optionen aus, die angezeigt werden. Der Hilfstext erklärt jede Option.

d. Um Amazon Transcribe Call Analytics zu aktivieren

i. Wählen Sie die Schaltfläche Amazon Transcribe Call Analytics.

ii. Öffnen Sie die Sprachliste und wählen Sie eine Sprache aus.

iii. (Optional) Erweitern Sie die Einstellungen zum Entfernen von Inhalten, wählen Sie eine oder mehrere Optionen aus und wählen Sie dann eine oder mehrere der zusätzlichen Optionen aus, die angezeigt werden. Der Hilfstext erklärt jede Option.

iv. (Optional) Erweitern Sie Zusätzliche Einstellungen, wählen Sie eine oder mehrere Optionen aus und wählen Sie dann eine oder mehrere der zusätzlichen Optionen aus, die angezeigt werden. Der Hilfstext erklärt jede Option.

v. (Optional) Erweitern Sie die Einstellungen für Analysen nach dem Anruf und gehen Sie wie folgt vor:

A. Aktivieren Sie das Kontrollkästchen „Analyse nach dem Anruf“.

B. Geben Sie die URI Ihres Amazon S3 S3-Buckets ein.

C. Wählen Sie einen Redaktionstyp für den Inhalt aus.

2. Wenn Sie mit Ihrer Auswahl fertig sind, wählen Sie Weiter.

Konfigurieren Sie die Ausgabedetails

Nachdem Sie die Schritte zur Medienverarbeitung abgeschlossen haben, wählen Sie ein Ziel für die Analyseausgabe aus. Call Analytics bietet Live-Einblicke über Amazon Kinesis Data Streams und optional über ein Data Warehouse in einem Amazon S3 S3-Bucket Ihrer Wahl. Um das Data Warehouse zu erstellen, verwenden Sie eine CloudFormation Vorlage. Die Vorlage hilft Ihnen bei der Erstellung der Infrastruktur, die die Anruf-Metadaten und Einblicke in Ihren Amazon S3 S3-Bucket bereitstellt. Weitere Informationen zum Erstellen des Data Warehouse finden Sie unter Creating an Amazon Chime Data Lake und Call Analytics Data Model im Amazon Chime SDK Developer Guide.

Wenn Sie die Sprachanalyse bei der Erstellung einer Konfiguration aktivieren, können Sie auch Sprachanalyse-Benachrichtigungsziele wie AWS Lambda, Amazon Simple Queue Service oder Amazon Simple Notification Service hinzufügen. In den folgenden Schritten wird erklärt, wie das geht.

Um Ausgabedetails zu konfigurieren

1. Öffnen Sie die Kinesis-Datenstream-Liste und wählen Sie Ihren Datenstream aus.

   > **Note**
   >
   > Wenn Sie Ihre Daten visualisieren möchten, müssen Sie den Kinesis-Datenstream auswählen, der vom Amazon S3 S3-Bucket und Amazon Kinesis Data Firehose verwendet wird.

2. (Optional) Erweitern Sie Zusätzliche Sprachanalyse-Benachrichtigungsziele und wählen Sie eine beliebige Kombination von AWS Lambda-, Amazon SNS- und Amazon SQS SQS-Zielen aus.
3. (Optional) Aktivieren Sie unter Analysieren und Visualisieren von Erkenntnissen das Kontrollkästchen Historische Analyse mit Data Lake durchführen.
4. Wenn Sie fertig sind, wählen Sie Weiter.

Konfigurieren von Zugriffsberechtigungen

Um Anrufanalysen zu aktivieren, müssen der Dienst für maschinelles Lernen und andere Ressourcen über Berechtigungen für den Zugriff auf Datenträger und die Bereitstellung von Erkenntnissen verfügen. Weitere Informationen finden Sie unter Using the Call Analytics Resource Access Role im Amazon Chime SDK Developer Guide.

So konfigurieren Sie Zugriffsberechtigungen

1. Führen Sie auf der Seite Zugriffsberechtigungen konfigurieren einen der folgenden Schritte aus:

   1. Wählen Sie Neue Servicerolle erstellen und verwenden aus.
   2. Geben Sie im Feld Suffix für den Namen der Servicerolle ein beschreibendes Suffix für die Rolle ein.

   –oder–

   1. Wählen Sie Bestehende Servicerolle verwenden aus.
   2. Öffnen Sie die Liste der Servicerollen und wählen Sie eine Rolle aus.
2. Wählen Sie Weiter aus.

(Optional) Konfigurieren Sie Warnmeldungen in Echtzeit

> **Important**
>
> Um Benachrichtigungen in Echtzeit verwenden zu können, müssen Sie zuerst Amazon Transcribe oder Amazon Transcribe Call Analytics aktivieren.

Sie können eine Reihe von Regeln erstellen, die Echtzeitwarnungen an Amazon senden EventBridge. Wenn ein von Amazon Transcribe oder Amazon Transcribe Call Analytics generierter Einblick während einer Analysesitzung mit Ihrer angegebenen Regel übereinstimmt, wird eine Warnung gesendet. Benachrichtigungen haben den Detailtyp. `Media Insights Rules Matched` EventBridge unterstützt die Integration mit nachgelagerten Diensten wie Amazon Lambda, Amazon SQS und Amazon SNS, um Benachrichtigungen für den Endbenutzer auszulösen oder eine andere benutzerdefinierte Geschäftslogik zu initiieren. Weitere Informationen finden Sie weiter unten in Automatisieren des Amazon Chime SDK mit EventBridge diesem Abschnitt.

Um Warnmeldungen zu konfigurieren

1. Wählen Sie unter Echtzeitwarnungen die Option Aktive Echtzeitwarnungen aus.
2. Wählen Sie unter Regeln die Option Regel erstellen aus.
3. Geben Sie im Feld Regelname einen Namen für die Regel ein.
4. Öffnen Sie die Liste Regeltyp und wählen Sie den Regeltyp aus, den Sie verwenden möchten.
5. Verwenden Sie die angezeigten Steuerelemente, um der Regel Schlüsselwörter hinzuzufügen und Logik anzuwenden, z. B. erwähnt oder nicht erwähnt.
6. Wählen Sie Weiter aus.

Überprüfen und erstellen

Um die Konfiguration zu erstellen

1. Überprüfen Sie die Einstellungen in den einzelnen Abschnitten. Wählen Sie bei Bedarf Bearbeiten, um eine Einstellung zu ändern.
2. Wählen Sie Create configuration (Konfiguration erstellen).

Ihre Konfiguration wird auf der Konfigurationsseite der Amazon Chime SDK-Konsole angezeigt.

Verwenden von Call Analytics-Konfigurationen

Nachdem Sie eine Konfiguration erstellt haben, verwenden Sie sie, indem Sie sie mit einem oder mehreren Amazon Chime SDK Voice Connectors verknüpfen. Weitere Informationen finden Sie weiter Konfiguration von Voice Connectors für die Verwendung von Anrufanalysen oben in diesem Handbuch.

Konfiguration der Call Analytics-Konfiguration wird aktualisiert

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Konfiguration für Anrufanalysen aktualisieren.

Um eine Konfiguration zu aktualisieren

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Call Analytics die Option Konfigurationen und dann die Konfiguration aus, die Sie aktualisieren möchten.
3. Wählen Sie rechts oben die Option Edit (Bearbeiten) aus.
4. Folgen Sie nach Konfigurationen für Anrufanalysen erstellen Bedarf den Schritten unter, um die Konfigurationseinstellungen zu ändern.

   Möglicherweise müssen Sie die Richtlinien für die Servicerolle ändern, damit sie mit der aktualisierten Konfiguration kompatibel sind, oder Sie müssen eine neue Servicerolle auswählen.
5. Wenn Sie fertig sind, wählen Sie Konfiguration aktualisieren.

> **Note**
>
> Wenn die Konfiguration mit einem Voice Connector verknüpft ist, verwendet der Voice Connector diese Konfiguration automatisch. Wenn Sie jedoch ein Ziel für Sprachanalyse-Benachrichtigungen aktivieren, deaktivieren oder anpassen, warten Sie fünf Minuten, bis diese neuen Einstellungen wirksam werden.

Konfigurationen für Anrufanalysen werden gelöscht

In den Schritten in diesem Abschnitt wird erklärt, wie Sie eine Amazon Chime SDK-Konfiguration für Anrufanalysen dauerhaft löschen.

> **Important**
>
> Sie können einen Löschvorgang nicht rückgängig machen.

So löschen Sie eine Konfiguration

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Call Analytics die Option Configurations und anschließend das Optionsfeld neben der Konfiguration aus, die Sie löschen möchten.
3. Wählen Sie Löschen aus.
4. Geben Sie im Dialogfeld „Konfiguration löschen“ die Eingabe ein, **`confirm`** um den Löschvorgang zu bestätigen, und wählen Sie dann Löschen aus.

Aktivieren von Sprachanalysen

> **Important**
>
> Als Voraussetzung für die Verwendung dieser Funktion bestätigen Sie, dass die Erfassung, Verwendung, Speicherung und Aufbewahrung der biometrischen Kennungen und biometrischen Informationen Ihres Anrufers („biometrische Daten“) in Form eines digitalen Sprachprofils die Zustimmung des Anrufers durch eine Schriftversion erfordert. Eine solche Zustimmung ist nach verschiedenen Bundesgesetzen erforderlich, einschließlich der Biometriegesetz in den Bundesstaaten Illinois, Puerto, Phoenix und anderen Bundesstaatsdatengesetzen.
>
> Sie müssen jedem Aufrufer durch einen Prozess, der die informierte Zustimmung jedes Aufrufers klar widerspiegelt, eine Textfreigabe bereitstellen, bevor Sie den Sprachanalyseservice des Amazon Chime SDK verwenden, wie es gemäß den Bedingungen Ihrer Vereinbarung zur AWS Steuerung Ihrer Nutzung des Services erforderlich ist.

> **Note**
>
> Um Sprachanalysen zu aktivieren, benötigen Sie mindestens eine Konfiguration für Amazon Chime SDK Voice Connector und mindestens eine Konfiguration für die Anrufanalyse des Amazon Chime SDK. Weitere Informationen zum Erstellen von Sprach-Connectors finden Sie unter Einen Amazon Chime SDK Voice Connector erstellen. Informationen zum Erstellen einer Anrufanalyse-Konfiguration finden Sie unter Konfigurationen für Anrufanalysen erstellen. Informationen zum Aktualisieren einer Konfiguration finden Sie unter

In den Themen in diesem Abschnitt wird erläutert, wie Sie Amazon Chime SDK Sprachanalysen für Amazon Chime SDK Sprach-Connectors aktivieren. Sprachanalysen verwenden Machine Learning, um einige oder alle der folgenden Funktionen zu aktivieren:

- Sprechersuche – Konvertiert die Stimme eines Anrufers in eine Vektoreinbettung . Anschließend wird die Einbettung mit einer Datenbank bekannter Spracheinbettungen verglichen. Wenn eine oder mehrere Übereinstimmungen gefunden werden, wird eine Rangliste der Sprachprofil-ID-Übereinstimmungen mit hoher Ähnlichkeit zusammen mit einem entsprechenden Satz von Zuverlässigkeitswerten zurückgegeben.

  > **Note**
  >
  > Die Sprechersuche ist nicht für Anwendungsfälle zur Authentifizierung oder Identitätsprüfung konzipiert, z. B. für die Überprüfung der Identität eines Sprechers mit extrem hoher Genauigkeit.

- Sprachtonanalyse – Prognostiziert die in einem Sprachsignal ausgedrückte Stimmung auf der Grundlage einer kombinierten Analyse sprachlicher und neuronaler Informationen.

  > **Note**
  >
  > Zur Erinnerung: Bei der Sprachtonanalyse müssen Sie alle gesetzlichen Anforderungen erfüllen. Dazu gehört, die Zustimmung des Sprechers gemäß den gesetzlichen Vorschriften einzuholen und die Funktion nicht zu verwenden, um Entscheidungen über den Sprecher zu treffen, die rechtliche oder ähnlich wichtige Auswirkungen haben würden, wie z. B. Arbeitskräfte, Arzt, Kreditwürdigkeit oder Finanzangebote.

Um Sprachanalysen zu aktivieren, verwenden Administratoren die Amazon Chime SDK-Konsole, um Folgendes zu tun:

- Konfigurieren Sie Sprach-Connectors so, dass eine oder mehrere der oben aufgeführten Funktionen verwendet werden.
- Erstellen Sie Benachrichtigungsziele. Benachrichtigungsziele empfangen asynchron Sprachanalyseereignisse, und Sie müssen mindestens ein Ziel haben.
- Erstellen Sie Sprachprofildomänen. Sprachprofildomänen enthalten Gruppen von Sprachprofilen. Ein Sprachprofil besteht wiederum aus einer Vektoreinbettung der Stimme eines Anrufers sowie einer eindeutigen ID. Standardmäßig können Sie 3 Sprachprofildomänen erstellen und jede Domäne kann 20.000 Sprachprofile enthalten. Sie können bei Bedarf eine Erhöhung für beide Limits beantragen.

Entwickler können eine Reihe von APIs verwenden, um dieselben Aufgaben auszuführen. Weitere Informationen finden Sie unter Verwenden des PSTN-Sprachanalysedienstes des Amazon Chime SDK im Amazon Chime SDK-Entwicklerhandbuch.

Sprachprofil-Domänen verwalten

Die Amazon Chime SDK-Lautsprechersuche erstellt Sprachprofile, Vektorkarten der Stimme eines Anrufers. Eine Sprachprofil-Domain stellt eine Sammlung von Sprachprofilen dar. Sie müssen eine Sprachprofildomäne erstellen, bevor Entwickler die StartSpeakerSearchTaskAPI aufrufen können.

> **Important**
>
> Bei der Lautsprechersuche wird eine Spracheinbettung erstellt, mit der die Stimme eines Anrufers mit zuvor gespeicherten Sprachdaten verglichen werden kann. Die Erfassung, Verwendung, Speicherung und Aufbewahrung biometrischer Identifikatoren und biometrischer Informationen in Form einer digitalen Einbettung kann die informierte Zustimmung des Anrufers in Form einer schriftlichen Mitteilung erfordern. Eine solche Zustimmung ist nach verschiedenen staatlichen Gesetzen erforderlich, darunter den biometrischen Gesetzen in Illinois, Texas, Washington und anderen Datenschutzgesetzen der Bundesstaaten. Bevor Sie die Lautsprecher-Suchfunktion verwenden, müssen Sie alle Hinweise bereitstellen und alle Einwilligungen einholen, die nach geltendem Recht und gemäß den AWS-Servicebedingungen für Ihre Nutzung der Funktion erforderlich sind. Bevor Sie den Amazon Chime SDK-Sprachanalysedienst nutzen, müssen Sie jedem Anrufer eine schriftliche Mitteilung zukommen lassen, wobei die informierte Zustimmung jedes

Anrufers deutlich zum Ausdruck kommt, wie es in den Bedingungen Ihrer Vereinbarung zur AWS Regelung Ihrer Nutzung des Dienstes vorgeschrieben ist.

In den folgenden Themen wird erklärt, wie Sie Sprachprofil-Domains erstellen und verwalten.

Themen

Sprachprofil-Domänen erstellen

In den Schritten in diesem Abschnitt wird erklärt, wie Sie Domains mit Sprachprofilen erstellen. Beachten Sie Folgendes:

- Domainnamen dürfen 256 Zeichen nicht überschreiten.
- Domainbeschreibungen dürfen 512 Zeichen nicht überschreiten.

Die Amazon Chime SDK-Konsole zeigt eine Fehlermeldung an, wenn Sie eines der Grenzwerte überschreiten.

Note

Sie müssen einen symmetrischen KMS-Schlüssel verwenden, um all Ihre Domains zu verschlüsseln. Weitere Informationen finden Sie unter Verschlüsselung mit Sprachanalyse verwenden. Außerdem müssen Ihre Endbenutzer damit einverstanden sein, dass ihre Stimme aufgezeichnet wird, bevor Sie eine Sprachanalysesitzung starten. Weitere Informationen zur Einwilligung finden Sie unterDie Einwilligungserklärung zur Sprachanalyse verstehen.

So erstellen Sie eine Sprachprofil-Domain

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus.
3. Wählen Sie Domain für Sprachprofile erstellen aus.
4. Wählen Sie unter Zustimmungsbestätigung die Option Ja, ich stimme der Zustimmungsbestätigung für Amazon Chime Speaker Search zu.
5. Geben Sie unter Setup einen Namen und eine Beschreibung für die Domain ein und wählen Sie dann einen KMS-Schlüssel aus.
6. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus und geben Sie dann einen Schlüssel und einen optionalen Wert ein. Wiederholen Sie den Vorgang nach Bedarf, um weitere Tags hinzuzufügen.
7. Wenn Sie fertig sind, wählen Sie Sprachprofil-Domain erstellen.

Sprachprofil-Domänen bearbeiten

Sie können jede Sprachprofil-Domain bearbeiten, unabhängig davon, wer sie erstellt hat.

Um eine Sprachprofil-Domain zu bearbeiten

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus.
3. Aktivieren Sie das Kontrollkästchen neben der Domain, die Sie bearbeiten möchten, und wählen Sie dann Bearbeiten aus.
4. Ändern Sie bei Bedarf den Namen und die Beschreibung der Domain und wählen Sie dann Speichern.

Sprachprofil-Domains löschen

Sie können jede Sprachprofil-Domain löschen, unabhängig davon, wer sie erstellt hat.

> **Important**
>
> Wenn Sie eine Domain löschen, löschen Sie auch alle zugehörigen Sprachprofile, und Sie können das Löschen nicht rückgängig machen.

Um eine Sprachprofildomäne zu löschen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus.
3. Aktivieren Sie das Kontrollkästchen neben der Domain, die Sie löschen möchten, und wählen Sie dann Löschen aus.
4. Wählen Sie im daraufhin angezeigten Dialogfeld Ich verstehe, dass diese Aktion nicht rückgängig gemacht werden kann, und wählen Sie dann Löschen aus.

Verwenden von Tags mit Sprachprofildomänen

In den Themen in diesem Abschnitt wird erklärt, wie Sie Tags mit Ihren vorhandenen Amazon Chime SDK-Sprachprofil-Domains verwenden können. Mithilfe von Tags können Sie Ihren Domains Metadaten zuweisen. Ein Tag besteht aus einem Schlüssel und einem optionalen Wert, der Informationen über die Ressource oder die auf dieser Ressource gespeicherten Daten speichert. Sie definieren alle Schlüssel und Werte. Sie können beispielsweise einen Tag-Schlüssel CostCentermit dem Wert 98765 erstellen und das Paar für die Kostenzuweisung verwenden. Sie können einer Sprachprofil-Domain bis zu 50 Tags hinzufügen.

Hinzufügen von Tags zu Sprachprofil-Domains

Gehen Sie wie folgt vor, um einer vorhandenen Sprachprofil-Domain Tags hinzuzufügen.

Um Tags hinzuzufügen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus.
3. Wählen Sie die Domain aus, der Sie Tags hinzufügen möchten.

4. Wähle „Tags verwalten“ und dann „Neues Tag hinzufügen“.
5. Geben Sie einen Wert in das Feld Schlüssel und einen optionalen Wert in das Feld Wert ein.
6. Wählen Sie bei Bedarf Neues Tag hinzufügen aus, um ein weiteres Tag zu erstellen.
7. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Domain-Tags für Sprachprofile bearbeiten

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto bearbeiten, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So bearbeiten Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus. .
3. Wählen Sie die Domain mit den Tags aus, die Sie bearbeiten möchten.
4. Wählen Sie Tags verwalten aus.
5. Ändern Sie nach Bedarf die Werte in den Feldern Schlüssel und Wert.

   -ODER-

   Wählen Sie Neues Tag hinzufügen und fügen Sie ein oder mehrere Tags hinzu.
6. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Domain-Tags für Sprachprofile werden entfernt

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto entfernen, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So entfernen Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich Voice Profile Domains aus. .

3. Wählen Sie die Domain mit den Tags aus, die Sie bearbeiten möchten.
4. Wählen Sie Tags verwalten aus.
5. Wählen Sie unter jedem der Tags, die Sie löschen möchten, die Option Entfernen aus.
6. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Die Einwilligungserklärung zur Sprachanalyse verstehen

Wenn Sie eine Sprachprofil-Domain oder eine Konfiguration für Anrufanalysen erstellen, die Sprachanalysen verwendet, wird Ihnen diese Einwilligungsbestätigung angezeigt:

Als Voraussetzung für die Nutzung dieser Funktion erkennen Sie an, dass für die Erfassung, Verwendung, Speicherung und Aufbewahrung der biometrischen Identifikatoren und biometrischen Informationen („biometrische Daten“) eines Sprechers in Form einer digitalen Einbettung die informierte Zustimmung des Sprechers erforderlich sein kann, auch in Form einer schriftlichen Mitteilung. Eine solche Zustimmung ist nach verschiedenen staatlichen Gesetzen erforderlich, darunter den biometrischen Gesetzen in Illinois, Texas, Washington und anderen Datenschutzgesetzen der Bundesstaaten. Bevor du die Sprechersuche nutzen kannst, musst du jedem Sprecher alle erforderlichen Hinweise zukommen lassen und alle erforderlichen Einwilligungen einholen, wie es das geltende Recht vorschreibt und wie in unseren Nutzungsbedingungen für deine Nutzung der Funktion dargelegt ist.

Bevor Sie den Amazon Chime SDK-Sprachanalyse-Service nutzen, müssen Sie jedem Anrufer eine schriftliche Mitteilung zukommen lassen, wobei die informierte Zustimmung jedes Anrufers deutlich zum Ausdruck kommt, wie es in den Bedingungen Ihrer Vereinbarung mit AWS über Ihre Nutzung des Service vorgeschrieben ist.

Gemäß dem Biometric Information Privacy Act („BIPA“) müssen Sie für jeden Redner in Illinois die folgenden Informationen schriftlich als schriftliche Mitteilung bereitstellen, wobei die informierte Zustimmung jedes Anrufers eindeutig wiedergegeben wird, bevor Sie die Sprechersuche verwenden:

„[Ihr Firmenname („Firma“)] nutzt Amazon Web Services als Dienstleister für Sprachsuchdienste. Biometrische Identifikatoren und biometrische Informationen („biometrische Daten“) können von Amazon Web Services im Namen von [Unternehmen] gesammelt, gespeichert und verwendet werden, um die Stimme eines Anrufers mit zuvor gespeicherten Sprachdaten zu vergleichen. Biometrische Daten, die im Rahmen dieses Prozesses generiert werden, werden bis zu drei Jahre nach Ihrer letzten Interaktion mit [Unternehmen] oder länger aufbewahrt, sofern dies nach geltendem Recht zulässig oder vorgeschrieben ist, und danach vernichtet. Sofern nicht nach geltendem Recht

vorgeschrieben oder zulässig, wird [Unternehmen] Amazon Web Services anweisen, biometrische Daten, die im Namen von [Unternehmen] gespeichert sind, dauerhaft zu vernichten, wenn der ursprüngliche Zweck der Erfassung oder Beschaffung solcher Daten erfüllt wurde, und zwar innerhalb von drei Jahren nach Ihrer letzten Interaktion mit den Diensten oder nachdem Sie von Ihnen darüber informiert wurden, dass diese Daten vernichtet werden sollten, je nachdem, was zuerst eintritt. Biometrische Daten können zwischen [Unternehmen] und Amazon Web Services übertragen werden, soweit dies für die Bereitstellung und den Empfang dieses Dienstes erforderlich ist. Sie geben hiermit Ihre ausdrückliche, informierte, schriftliche Erklärung und erklären sich damit einverstanden, dass [Unternehmen] und Amazon Web Services Ihre biometrischen Daten wie hier beschrieben erheben, verwenden und speichern.“

Indem Sie das unten stehende Kästchen ankreuzen, erklären Sie sich damit einverstanden, jedem Redner in Illinois die oben genannten Informationen schriftlich zur Verfügung zu stellen und von jedem Sprecher in Illinois eine ausgefertigte schriftliche Erklärung zu erhalten, wie von BIPA verlangt.

Einrichten von Notrufen

Das Amazon Chime SDK bietet zwei Möglichkeiten, Notrufe einzurichten. Beide Methoden gelten nur für Aufrufe in oder in den USA.

- Validierte Adressen – Geben Sie die physische Adresse ein, von der Aufrufe stammen können, und validieren Sie sie. Wenn Sie diese Option wählen, wird die validierte Adresse für alle Sprach-Connectors des Amazon Chime SDK verfügbar. Das Amazon Chime SDK leitet dann Aufrufe an den nächstgelegenen öffentlichen Sicherheitsannahmepunkt weiter.
- Weiterleitung durch Dritte – Fügen Sie einem Amazon Chime SDK Voice Connector Notruf-Routing-Nummern hinzu. Wenn Sie diese Option wählen, leitet ein Drittanbieterservice Ihrer Wahl die Anrufe weiter und Sie müssen keine Adresse validieren. Sie können diese Methode verwenden, um Notrufe von außerhalb der USA zu tätigen, aber die Aufrufe müssen an einen Endpunkt in den USA gehen.

> **Note**
>
> Wenn Sie keine Adressen oder Routing-Nummern verwenden, kann die Adressvalidierung zu Beginn eines 911-Aufrufs durchgeführt werden, um sicherzustellen, dass er an den entsprechenden Public Safety Answering Point (PSAP) weitergeleitet wird, was bedeutet, dass die Ankunft der Hilfe länger dauern kann.

In den folgenden Abschnitten wird erläutert, wie Sie beide Optionen verwenden.

Themen

Validieren von Adressen für Notrufe

Um die Erstellung von Adressen für Notrufe zu verwenden, geben Sie die Adressen ein und validieren sie. Das Amazon Chime SDK leitet die Aufrufe dann an den nächstgelegenen lokalen Public Safety Answering Point (PSAP) weiter. Beachten Sie Folgendes:

- Sie müssen eine Adresse nur einmal validieren, können sie aber mehrmals validieren.
- Sie überprüfen nur die Adresse eines Gebäudes. Geben Sie keine Suite- oder Jungfernnummern an.
- Sie können Adressen nur in den USA validieren.

> **Note**
>
> Wir empfehlen dringend, Ihre validierten Adressen in PIDF-LO-Objekten in Ihren SIP-Anfragen zu verwenden. Weitere Informationen finden Sie unter Verwenden von PIDF-LO in Notrufen.

So validieren Sie eine Adresse

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter `Phone Numbers` die Option `Emergency Calling` aus.
3. Geben Sie unter `Validate Address`die Adresse Ihres Gebäudes ein.

   > **Note**
   >
   > Geben Sie die Adresse genau so ein, wie sie in der SIP-Einladung angezeigt wird. Dadurch wird sichergestellt, dass die Adresse erkannt wird, wenn jemand anruft.

4. Wählen Sie `Validate`.

Einrichten von Notfall-Routing-Nummern von Drittanbietern

Um Notruf-Routing-Nummern verwenden zu können, benötigen Sie Folgendes:

- Ein Amazon Chime SDK Voice Connector.
- Eine Notruf-Routing-Nummer von einem Drittanbieter. Dies muss eine US-Nummer sein, und Sie geben diese Nummer an das Amazon Chime SDK an. Sie können einen Amazon Chime SDK Voice Connector nur für Notrufe erstellen.

Nach der Einrichtung verwendet das Amazon Chime SDK beim Aufrufen von Notfalldiensten Ihre Notrufnummer, um Anrufe über ein öffentliches Telefonnetz an Ihren externen Notfalldienstanbieter weiterzuleiten. Ihr externer Notfalldienstanbieter leitet Ihren Anruf dann an den Notfalldienst weiter.

Das Einrichten von Notruf-Routing-Nummern außerhalb der USA erfordert, dass Sie die folgenden Voraussetzungen erfüllen:

- Fordern Sie Notruf-Routing-Nummern von einem externen Notdienstanbieter an. Stellen Sie sicher, dass es sich um US-Nummern handelt.
- Aktivieren und konfigurieren Sie Beendigungs- und Ursprungseinstellungen für einen Sprach-Connector. Informationen dazu finden Sie unter Bearbeiten der Amazon Chime SDK Voice Connector-Einstellungen.

So richten Sie Notruf-Routing-Nummern für Ihren Voice Connector ein

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Sprach-Konnektoren aus.
3. Wählen Sie den Namen des Sprach-Connectors aus.
4. Wählen Sie die Registerkarte Notruf aus.
5. Wählen Sie unter Konfiguration des Notfalldienstanbieters eines Drittanbieters die Option Hinzufügen aus.
6. Wählen Sie für Methode zum Senden von Anrufen die Option DNIS (Dialed Number Identification Service) aus.
7. Geben Sie für Notfallruf-Routing-Nummer für den Anruf von Notfalldiensten die Telefonnummer eines Drittanbieters für den Anruf von Notfalldiensten im E.164-Format ein.
8. Geben Sie unter Test-Routingnummer für das Testen von Anrufen an Notfalldienste die Telefonnummer eines Drittanbieters für das Testen von Anrufen an Notfalldienste im E.164-Format ein.
9. Wählen Sie für Land die Option USA aus.
10. Wählen Sie Hinzufügen aus.

Verwenden von PIDF-LO in Notrufen

Amazon Chime SDK Voice Connectors unterstützen erweiterte 911 (E911)-Aufrufe. Wenn Sie Notrufe über einen Sprach-Connector tätigen, können Sie Standortinformationen für Anrufer senden, indem Sie ein GEOPRIV Presence Information Data Format Location Object (PIDF-LO) in Ihre SIP-Anfragen aufnehmen. Das Objekt muss den `Geolocation-Routing` Header enthalten, der auf festgelegt ist`Yes`. Wir empfehlen dringend, die Adresse zu validieren. Wenn Sie keine Adressen oder Routing-Nummern verwenden, kann die Adressvalidierung zu Beginn eines 911-Aufrufs durchgeführt werden, um sicherzustellen, dass er an den entsprechenden Public Safety Answering Point (PSAP) weitergeleitet wird, was bedeutet, dass die Ankunft der Hilfe länger dauern kann.

Das folgende Beispiel zeigt eine SIP-Einladung mit einem PIDF-LO-Objekt, das eine Adresse enthält.

```
INVITE sip:911@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws;transport=TCP SIP/2.0
Via: SIP/2.0/TCP IPaddress:12345;rport;branch=z9hG4bKKXN2D41yvDUKH
From: +15105186683 ><sip:+15105186683@IPaddress:12345>;tag=tag
To: <sip:911@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws>;transport=TCP
Call-ID: 12abcdef-3456-7891-012g-h7i8j9k6l0a1
CSeq: 43615607 INVITE
Contact: <sip:IPaddress:12345>
Max-Forwards: 70
Geolocation-Routing: Yes
Geolocation: <cid:a1ef610291734f98a467b973819e90ed>;inserted-by=vpc@ng911.test.com
Content-Type: multipart/mixed;boundary=unique-boundarystring
Content-Length: 271
Accept: application/sdp, application/pidf+xml

--unique-boundarystring
Content-Type: application/sdp
v=0
o=FreeSWITCH 1636327400 1636327401 IN IP4 IPaddress
s=FreeSWITCH
c=IN IP4 IPaddress
t=0 0
m=audio 11398 RTP/SAVP 9 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=sendrecv
a=ptime:20

--unique-boundarystring
```

```
Content-Type: application/pidf+xml
Content-ID: <pidftest@test.com>
<?xml version="1.0" encoding="utf-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:bp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
entity="sip:amazontest911@test.com">
<tuple id="0">
    <status>
    <gp:geopriv>
        <gp:location-info>
        <ca:civicAddress>
            <ca:country>US</ca:country>
            <ca:A1>WA</ca:A1>
            <ca:A3>Seattle</ca:A3>
            <ca:HNO>1812</ca:HNO>
            <ca:RD>Example</ca:RD>
            <ca:STS>Ave</ca:STS>
            <ca:NAM>Low Flying Turtle</ca:NAM>
            <ca:PC>98101</ca:PC>
        </ca:civicAddress>
        </gp:location-info>
    </gp:geopriv>
    </status>
    <timestamp>2021-09-22T13:37:31.03</timestamp>
</tuple>
</presence>
--unique-boundarystring--
```

Verwaltung von SIP-Medienanwendungen

Sie können die Amazon Chime SDK-Konsole verwenden, um SIP-Medienanwendungen (Session Initiation Protocol) zu erstellen. Mit SIP-Medienanwendungen können Sie einfacher und schneller benutzerdefinierte Signal- und Medienanweisungen erstellen, die Sie normalerweise auf Ihrer PBX (Private Branch Telephone Exchange) erstellen würden.

Sie verwenden die Konsole auch, um SIP-Regeln zu erstellen. SIP-Regeln legen fest, wie eine SIP-Medienanwendung eine Verbindung zu einem Amazon Chime SDK-Meeting herstellen kann. Anrufe können zu und von öffentlichen DID- oder gebührenfreien Telefonnummern, die aus Ihrem Amazon Chime SDK-Inventar bereitgestellt wurden, oder zu und von einem Anforderungs-URI-Hostnamen, dem Namen, der einem Amazon Chime SDK Voice Connector zugewiesen wurde, gehen. Das Amazon Chime SDK führt die SIP-Regeln aus, wenn ein Benutzer einen Anruf tätigt oder empfängt. Informationen zur Verwendung von SIP-Regeln finden Sie unter. Verwalten von SIP-Regeln

Sie müssen ein AWS Lambda Benutzer sein, bevor Sie SIP-Medienanwendungen erstellen können. Die SIP-Medienanwendungen verwenden Lambda-Funktionen aus den folgenden Gründen:

- Sie können komplexe Logik schreiben, die Entscheidungen beinhaltet. Ein Anrufer kann sich beispielsweise mit einem Festnetztelefon in eine Besprechung einwählen. Diese Telefonnummer wiederum löst Lambda-Funktionen aus, die nach einer Meeting-PIN fragen und den Anrufer zur richtigen Besprechung weiterleiten.
- Sie können Lambda-Funktionen ohne Serverinfrastruktur bereitstellen.

Weitere Informationen finden Sie AWS Lambda unter Erste Schritte mit AWS Lambda.

> **Note**
>
> Für SIP-Medienanwendungen des Amazon Chime SDK gelten Einschränkungen für ausgehende Auslandsgespräche. Weitere Informationen finden Sie unter Einschränkungen für ausgehende Anrufe.

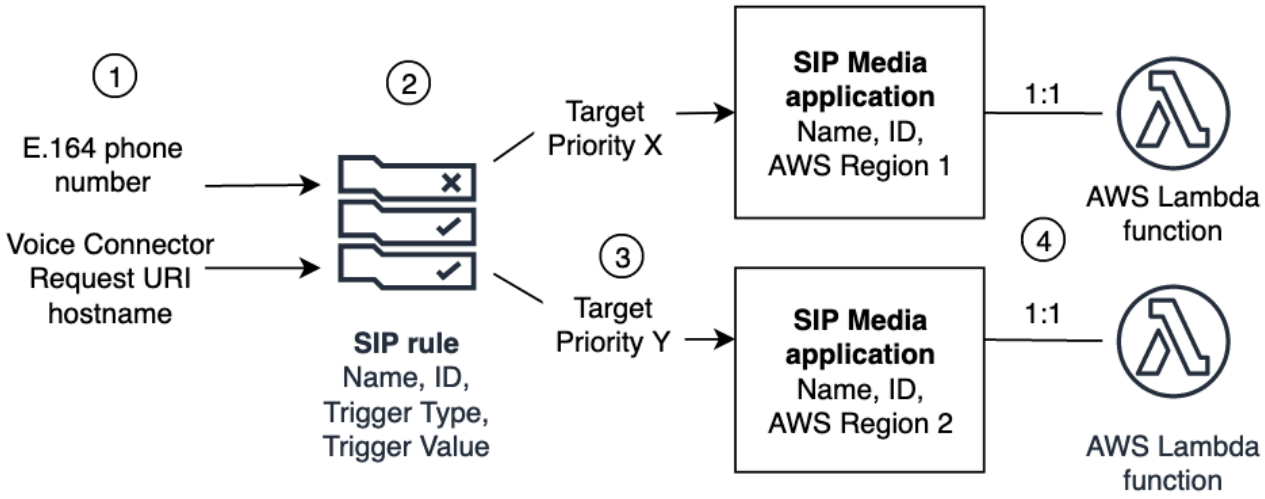
Themen

Grundlegendes zu SIP-Anwendungen und -Regeln

Um das Session Initiation Protocol (SIP) mit dem Amazon Chime SDK zu verwenden, erstellen Sie SIP-Medienanwendungen und SIP-Regeln. Sie erstellen beide in der Amazon Chime SDK-Konsole.

Das folgende Diagramm zeigt, wie die Anwendungen und Regeln funktionieren. Es zeigt, wie SIP-Regeln Anrufe von Telefonnummern und Anforderungs-URI-Hostnamen an verschiedene SIP-Anwendungen weiterleiten können.

Die Zahlen im Bild entsprechen den Zahlen im Text unter dem Bild.



Sie können SIP-Regeln (2) nur Telefonnummern aus Ihrem Chime-Inventar und Voice Connectors (1) zuweisen. Außerdem müssen Sie in Ihrem PSTN-Audiodienst eine Telefonnummer oder einen Amazon Chime SDK Voice Connector angeben. In den Schritten unter wird Eine SIP-Medienanwendung erstellen erklärt, wie das geht. Beim Empfang eines Anrufs an eine Telefonnummer ruft die SIP-Regel eine SIP-Medienanwendung und die zugehörige Lambda-Funktion auf (4). Die Lambda-Funktion führt Code aus, der Aktionen wie das Abspielen von Wartemusik, die Teilnahme an einem Meeting oder das Stummschalten eines Anrufs aufruft. Um die Ausfallsicherheit in mehreren Regionen zu gewährleisten, können SIP-Regeln (2) alternative Ziel-SIP-Medienanwendungen in verschiedenen AWS Regionen (3) in der Reihenfolge ihrer Priorität für den Failover angeben. Wenn ein Ziel ausfällt, versucht der PSTN-Audiodienst es mit dem nächsten. Beachten Sie, dass sich jedes alternative Ziel in einer anderen Region befinden muss. AWS

Verwenden von SIP-Medienanwendungen

Eine SIP-Medienanwendung ist ein verwaltetes Objekt, das Werte aus einer SIP-Regel an eine AWS Lambda Zielfunktion weitergibt. Sie können SIP-Medienanwendungen erstellen, anzeigen, aktualisieren und löschen. Beachten Sie, dass Sie die Details jeder Anwendung einsehen können und dass andere Administratoren Ihre Anwendungen einsehen können.

> **Note**
>
> Sie benötigen eine AWS Lambda Funktion, bevor Sie eine SIP-Medienanwendung erstellen können. Weitere Informationen finden Sie unter Erste Schritte mit AWS Lambda.

Themen

Eine SIP-Medienanwendung erstellen

Sie erstellen eine SIP-Medienanwendung, wenn Sie Anrufe zu und von einem Anforderungs-URI-Hostnamen, einer Amazon Chime SDK Voice Connector-Gruppe oder einer privaten Telefonnummer aktivieren müssen.

Um eine SIP-Medienanwendung zu erstellen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Medienanwendungen und auf der daraufhin angezeigten Seite die Option SIP-Medienanwendung erstellen aus.
3. Geben Sie unter Name einen Namen für Ihre Anwendung ein.
4. Kopieren Sie einen der folgenden Werte und fügen Sie ihn in das ARN-Feld ein:

   - Der ARN einer Lambda-Funktion

- Der ARN des Alias einer Lambda-Funktion
- Der ARN einer Version einer Lambda-Funktion

> **Note**
>
> Sie können Alias- und Versions-ARNs erstellen, wenn Sie eine Lambda-Funktion erstellen, und Sie benötigen einen Alias- oder Versions-ARN, wenn Sie Lambda-Parallelität aktivieren möchten. Weitere Informationen zu Lambda-Funktionsaliasen, Versionsaliasen und Parallelität finden Sie unter Lambda-Funktionsaliase, Lambda-Funktionsversionen und Managing Lambda provisioned concurrency im Developer Guide.AWS Lambda

5. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, und gehen Sie dann wie folgt vor:

   1. Geben Sie einen Wert in das Feld Schlüssel ein.
   2. (Optional) Geben Sie einen Wert in das Feld Wert ein.
   3. Wählen Sie bei Bedarf Neues Tag hinzufügen aus, um weitere Tags hinzuzufügen.

6. Wählen Sie SIP-Medienanwendung erstellen. .

   Eine Erfolgsmeldung wird oben auf der Seite „SIP-Medienanwendung erstellen“ angezeigt, und Ihre Medienanwendung wird in der Liste der Anwendungen angezeigt. Wenn Sie eine Fehlermeldung sehen, folgen Sie den Anweisungen.

Verwenden von Tags mit SIP-Medienanwendungen

In den Themen in diesem Abschnitt wird erklärt, wie Sie Tags mit Ihren vorhandenen Amazon Chime SDK SIP-Medienanwendungen verwenden können. Mithilfe von Tags können Sie Ihren AWS Ressourcen, wie z. B. SIP-Medienanwendungen, Metadaten zuweisen. Ein Tag besteht aus einem Schlüssel und einem optionalen Wert, der Informationen über die Ressource oder die auf dieser Ressource gespeicherten Daten speichert. Sie definieren alle Schlüssel und Werte. Sie können beispielsweise einen Tag-Schlüssel `CostCenter` mit dem Wert von erstellen `98765` und das Paar für die Kostenzuweisung verwenden. Sie können einer SIP-Medienanwendung bis zu 50 Tags hinzufügen.

Themen

- Hinzufügen von Tags zu SIP-Medienanwendungen

- Tags bearbeiten
- Entfernen von Tags

Hinzufügen von Tags zu SIP-Medienanwendungen

Sie können bestehenden Amazon Chime SDK SIP-Medienanwendungen bis zu 50 Tags hinzufügen.

Um Tags hinzuzufügen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP Media Applications aus.
3. Wählen Sie den Namen der SIP-Medienanwendung aus, die Sie verwenden möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Wählen Sie Neues Tag hinzufügen und geben Sie dann einen Schlüssel und einen optionalen Wert ein.
6. Wählen Sie bei Bedarf Neues Tag hinzufügen aus, um ein weiteres Tag zu erstellen.
7. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Tags bearbeiten

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto bearbeiten, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So bearbeiten Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP Media Applications aus.
3. Wählen Sie den Namen der SIP-Medienanwendung aus, die Sie ändern möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Geben Sie in den Feldern Schlüssel oder Wert einen neuen Wert ein.
6. Wenn Sie fertig sind, wählen Sie Änderungen speichern.

Entfernen von Tags

Wenn Sie über die erforderlichen Berechtigungen verfügen, können Sie alle Tags in Ihrem AWS Konto entfernen, unabhängig davon, wer sie erstellt hat. IAM-Richtlinien können Sie jedoch daran hindern.

So entfernen Sie Tags

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP Media Applications aus.
3. Wählen Sie den Namen der SIP-Medienanwendung aus, die Sie ändern möchten.
4. Wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
5. Wählen Sie neben dem Tag, das Sie entfernen möchten, die Option Entfernen aus.
6. Wählen Sie Änderungen speichern aus.

Eine SIP-Medienanwendung anzeigen

Andere Administratoren können Ihre SIP-Medienanwendungen einschließlich ihrer Details einsehen, und Sie können deren Daten einsehen.

Um eine SIP-Medienanwendung anzusehen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich SIP Media Applications aus.

   Die SIP-Medienanwendungsseite wird angezeigt und enthält alle Anwendungen in Ihrer Organisation.
3. Um die Details einer Anwendung anzuzeigen, wählen Sie den Namen der Anwendung.

Aktualisierung einer SIP-Medienanwendung

Sie können den Namen und die Amazon Resource Names (ARNs) Ihrer Lambda-Funktion für Ihre SIP-Medienanwendungen aktualisieren. Sie können die Region nicht aktualisieren. AWS

Um eine SIP-Medienanwendung zu aktualisieren

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich SIP Media Applications aus.

   Die Seite mit der SIP-Medienanwendung wird angezeigt.
3. Wählen Sie den Namen der Anwendung, die Sie aktualisieren möchten.

   Die Anwendung wird auf einer eigenen Seite angezeigt.
4. Wählen Sie Bearbeiten aus.
5. Ändern Sie bei Bedarf Folgendes:

   - Der Name der Anwendung
   - Der Lambda-ARN, Alias-ARN oder der Versions-ARN
   - Die Tags. Weitere Informationen zum Ändern von Tags finden Sie unter

   > **Note**
   >
   > Sie können Alias- und Versions-ARNs erstellen, wenn Sie eine Lambda-Funktion erstellen, und Sie benötigen einen Alias- oder Versions-ARN, wenn Sie Lambda-Parallelität aktivieren möchten. Weitere Informationen zu Lambda-Funktionsaliasen, Versionsaliasen und Parallelität finden Sie unter Lambda-Funktionsaliase, Lambda-Funktionsversionen und Managing Lambda provisioned concurrency im Developer Guide.AWS Lambda
6. Wählen Sie Speichern.

   Eine Erfolgsmeldung wird angezeigt. Wenn Sie eine Fehlermeldung sehen, folgen Sie den Anweisungen.

Löschen einer SIP-Medienanwendung

Sie löschen eine SIP-Medienanwendung aus verschiedenen Gründen, z. B. aus den folgenden:

- Sie verwenden keine Telefonnummer oder keinen Anforderungs-URI-Hostnamen mehr.
- Sie machen einen Fehler beim Erstellen einer SIP-Medienanwendung.

> **Note**
>
> Als bewährte Methode sollten Sie sicherstellen, dass das Löschen der Anwendung den Anruffluss nicht stört. Durch das Löschen der Anwendung werden auch keine zugehörigen Telefonnummern oder SIP-Regeln gelöscht.

Um eine SIP-Medienanwendung zu löschen

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich SIP Media Applications aus.

   Die Seite mit der SIP-Medienanwendung wird angezeigt.
3. Wählen Sie das Optionsfeld neben dem Namen der Anwendung.
4. Wählen Sie Löschen aus.

   Das Dialogfeld Anwendungsname löschen wird angezeigt.
5. Wählen Sie Ich verstehe, dass diese Aktion nicht rückgängig gemacht werden kann, und wählen Sie dann Löschen aus.

Verwalten von SIP-Regeln

Eine SIP-Regel ordnet Ihre SIP-Medienanwendung einer Telefonnummer oder einem Anforderungs-URI-Hostnamen zu. Sie können eine SIP-Regel mehreren SIP-Medienanwendungen zuordnen. Jede Anwendung führt dann nur diese Regel aus. Eine Übersicht über die Funktionsweise von SIP-Regeln mit SIP-Medienanwendungen finden Sie unter Grundlegendes zu SIP-Anwendungen und -Regeln im vorherigen Abschnitt.

> **Note**
>
> Um SIP-Regeln zu erstellen, benötigen Sie mindestens eine DID oder gebührenfreie Telefonnummer, bei der ein Produkttyp in Ihrem Amazon Chime SDK-Bestand auf SIP Media Application Dial-In festgelegt ist, oder mindestens einen Anforderungs-URI-Hostnamen, den Namen, der einem Amazon Chime SDK Voice Connector zugewiesen ist. Weitere Informationen zu Telefonnummern finden Sie unter Verwalten von Telefonnummern. Weitere Informationen zu Anforderungs-URI-Hostnamen finden Sie in den Schritten im nächsten Abschnitt.

Inhalt

Erstellen einer SIP-Regel

Bevor Sie eine SIP-Regel erstellen können, benötigen Sie mindestens eine DID oder gebührenfreie Telefonnummer, bei der ein Produkttyp in Ihrem Amazon Chime SDK-Bestand auf SIP Media Application Dial-In oder einen Anforderungs-URI-Hostnamen festgelegt ist, der einem Amazon Chime SDK Voice Connector zugeordnet ist, und eine SIP-Medienanwendung. Weitere Informationen zu SIP-Anwendungen finden Sie unter Eine SIP-Medienanwendung erstellen. Außerdem können Sie Regeln verwenden, die von anderen Administratoren erstellt wurden.

So erstellen Sie eine SIP-Regel

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter Telefonnummern die Option SIP-Medienanwendungen aus.
3. Wählen Sie die SIP-Anwendung aus, für die Sie eine Regel erstellen möchten, und wählen Sie dann die Registerkarte Regeln.
4. Kopieren Sie die Telefonnummer oder den Wert für den Namen des ausgehenden Hosts, fügen Sie den Wert in Notepad oder ein ähnliches Programm ein und lassen Sie dieses Programm zur späteren Verwendung geöffnet.
5. Wählen Sie im Navigationsbereich SIP-Regeln aus.

   Die Seite mit den SIP-Regeln wird angezeigt.
6. Wählen Sie Erstellen.

   Das Dialogfeld Eine SIP-Regel erstellen wird angezeigt.
7. Geben Sie im Feld Name einen Namen für die Regel ein und führen Sie dann einen der folgenden Schritte aus:

   Erstellen einer Regel für eine Telefonnummer

   A. Standardmäßig wird in der Liste Auslösertyp die Option Zu Telefonnummer angezeigt. Wenn dies nicht der Fall ist, öffnen Sie die Liste und wählen Sie diesen Wert aus.

   B. Geben Sie für Telefonnummer eine Telefonnummer ein oder wählen Sie eine aus der Liste aus. Wenn Sie eine Zahl eingeben, verwenden Sie dieses Format: **+1***zehnstellige Zahl* . Zum Beispiel: +15095551212.

   Erstellen einer Regel für einen Anforderungs-URI-Hostnamen

   A. Öffnen Sie die Liste Trigger-Typ und wählen Sie URI-Hostname anfordern aus.

   B. Fügen Sie den Hostnamen, den Sie in Schritt 2 kopiert haben, in das Feld Hostname des Anforderungs-URI ein.
8. Um die Regel sofort zu verwenden, lassen Sie das Kontrollkästchen Aktiviert aktiviert. Um die Regel zu deaktivieren, z. B. bis ein Amazon Chime SDK Voice Connector und sein Hostname verfügbar sind, aktivieren Sie das Kontrollkästchen.

9. Wählen Sie Weiter und öffnen Sie auf der Seite Schritt 2 die Liste der SIP-Medienanwendungen und wählen Sie die zu verwendende SIP-Medienanwendung aus.
10. Wählen Sie nach Bedarf Eine SIP-Medienanwendung hinzufügen aus, um die Regel mit mehreren Anwendungen zu verwenden.
11. Wählen Sie Erstellen.

    Es wird eine Erfolgsmeldung angezeigt. Wenn eine Fehlermeldung angezeigt wird, folgen Sie den Anweisungen.

Anzeigen einer SIP-Regel

Andere Administratoren können Ihre SIP-Regeln einschließlich ihrer Details anzeigen, und Sie können dasselbe mit ihren Regeln tun.

So zeigen Sie eine SIP-Regel an

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Regeln aus.

   Die Seite mit den SIP-Regeln wird angezeigt und zeigt alle Regeln in Ihrer Organisation an.
3. Um die Details einer Regel anzuzeigen, wählen Sie den Namen der Regel aus.

Aktualisieren einer SIP-Regel

Die einzige Aktualisierung, die Sie an einer SIP-Regel vornehmen können, besteht darin, ihren Namen zu ändern. In der Regel ändern Sie einen Regelnamen so, dass er dem Namen der entsprechenden SIP-Medienanwendung entspricht.

So aktualisieren Sie eine SIP-Regel

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Regeln aus.
3. Wählen Sie den Namen der Regel aus, die Sie ändern möchten.

   Die Seite für diese Regel wird angezeigt.

4. Wählen Sie Bearbeiten aus.
5. Geben Sie unter Name einen neuen Namen für die Regel ein und wählen Sie dann Speichern aus.

Aktivieren einer SIP-Regel

Sie können jede SIP-Regel aktivieren, auch Regeln, die von einem anderen Administrator erstellt wurden. Als bewährte Methode sollten Sie die Details der Regel anzeigen, bevor Sie sie aktivieren. Weitere Informationen finden Sie unter Anzeigen einer SIP-Regel.

So aktivieren Sie eine SIP-Regel

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Regeln aus.

   Die Seite mit den SIP-Regeln wird angezeigt.
3. Scrollen Sie nach Bedarf nach unten bis zum Ende der Liste der Regeln und verwenden Sie dann die horizontale Scrollleiste, um die Spalte Status anzuzeigen.

   Deaktivierte Regeln haben ein rotes Deaktiviert-Symbol.
4. Führen Sie einen der folgenden Schritte aus, um eine Regel zu aktivieren:

   Verwenden der Liste Aktionen

   A. Scrollen Sie über und wählen Sie die Optionsschaltfläche neben dem Namen der Regel aus.

   B. Scrollen Sie nach oben, öffnen Sie die Liste Aktionen und wählen Sie Aktivieren und fahren Sie dann mit Schritt 5 fort.

   Verwenden der Schaltfläche Aktivieren

   A. Wählen Sie den Namen der Regel aus.

   B. Wählen Sie Aktivieren aus, neben Bearbeiten, und fahren Sie dann mit Schritt 5 fort.
5. Wenn Sie Aktivieren mit einer der in Schritt 4 beschriebenen Methoden auswählen, wird das Dialogfeld Regel(en) aktivieren angezeigt. Wählen Sie Ich habe verstanden, dass die hier aufgeführten Regel(n) die SIP-Medienanwendung auslösen, und wählen Sie dann Aktivieren aus.

Deaktivieren einer SIP-Regel

Deaktivieren Sie SIP-Regeln, wenn Sie die Verbindung, die die Regel bereitstellt, nicht benötigen. Außerdem müssen Sie eine SIP-Regel deaktivieren, bevor Sie diese Regel oder eine zugehörige SIP-Medienanwendung löschen. Sie können jede Regel deaktivieren, die von einem beliebigen Administrator erstellt wurde. Als bewährte Methode sollten Sie sich die Details der Regel ansehen, bevor Sie sie deaktivieren, und überprüfen, ob das Deaktivieren der Regel einen Gesprächsablauf nicht beeinträchtigt. Weitere Informationen finden Sie unter Anzeigen einer SIP-Regel.

So deaktivieren Sie eine SIP-Regel

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Regeln aus.

   Die Seite mit den SIP-Regeln wird angezeigt.
3. Scrollen Sie nach Bedarf nach unten bis zum Ende der Liste der Regeln und verwenden Sie dann die horizontale Scrollleiste, um die Spalte Status anzuzeigen.

   Aktivierte Regeln haben ein grünes Aktiviertes Symbol.
4. Führen Sie einen der folgenden Schritte aus, um eine Regel zu deaktivieren:

   Verwenden der Liste Aktionen

   A. Scrollen Sie über und wählen Sie die Optionsschaltfläche neben dem Namen der Regel aus.

   B. Scrollen Sie nach oben, öffnen Sie die Liste Aktionen und wählen Sie Deaktivieren aus.

      Das Dialogfeld Regel(en) deaktivieren wird angezeigt. Fahren Sie mit Schritt 5 fort.

   Verwenden der Schaltfläche Deaktivieren

   A. Scrollen Sie über und wählen Sie den Namen der Regel aus.

   B. Wählen Sie Deaktivieren, neben Bearbeiten aus.

      Das Dialogfeld Regel(en) deaktivieren wird angezeigt. Fahren Sie mit Schritt 5 fort.
5. Wählen Sie Ich weiß, dass diese Aktion die oben genannten Regeln stoppt, die die SIP-Medienanwendung auslösen, und dann Deaktivieren aus.

Löschen einer SIP-Regel

In der Regel löschen Sie eine SIP-Regel, wenn Sie den zugehörigen Hostnamen oder die Telefonnummer des Anforderungs-URI nicht benötigen. Außerdem können Sie eine SIP-Regel löschen, wenn Sie einen Fehler beim Erstellen machen.

> **Note**
>
> Sie müssen eine Regel deaktivieren, bevor Sie sie löschen können. Weitere Informationen zum Deaktivieren von Regeln finden Sie unter Deaktivieren einer SIP-Regel.

So löschen Sie eine SIP-Regel

1. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
2. Wählen Sie im Navigationsbereich unter PSTN Audio die Option SIP-Regeln aus.

   Die Seite mit den SIP-Regeln wird angezeigt.
3. Wählen Sie das Optionsfeld neben dem Namen der Regel aus.
4. Öffnen Sie die Liste Aktionen und wählen Sie Löschen aus.

   Das Dialogfeld Regel(en) löschen wird angezeigt.
5. Wählen Sie Ich weiß, dass diese Aktion nicht rückgängig gemacht werden kann und dann Löschen aus.

Verwalten globaler Einstellungen für das Amazon Chime SDK

Verwalten Sie die Einstellungen für den Aufrufdetaildatensatz für das Amazon Chime SDK.

Konfigurieren von Anrufdetaildatensätzen

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

Sie können Einstellungen für Anrufdetails für Amazon Chime SDK Voice Connectors konfigurieren. Weitere Informationen zu Amazon Chime SDK Voice Connectors finden Sie unter Verwaltung von Telefonnummern im Amazon Chime SDK.

So konfigurieren Sie Anrufdetaildatensatz-Einstellungen

1. Erstellen Sie einen Amazon S3-Bucket, indem Sie die Schritte unter Erste Schritte mit Amazon Simple Storage Service im Benutzerhandbuch für Amazon Simple Storage Service befolgen.
2. Öffnen Sie die Amazon Chime SDK-Konsole unter https://console.aws.amazon.com/chime-sdk/home.
3. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Anrufdetaildatensätze aus.
4. Öffnen Sie die Liste Protokollziel und wählen Sie einen S3-Bucket aus.
5. Wählen Sie Speichern.

Sie können die Protokollierung von Anrufdetaildatensätzen jederzeit beenden.

So beenden Sie die Protokollierung von Anrufdetaildatensätzen

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

2. Wählen Sie im Navigationsbereich unter SIP Trunking die Option Anrufdetaildatensätze aus.
3. Wählen Sie Protokollierung deaktivieren aus.

Anrufdetaildatensätze für Amazon Chime SDK Voice Connector

Wenn Sie sich dafür entscheiden, Anrufdetaildatensätze für Ihren Amazon Chime SDK Voice Connector zu erhalten, werden diese an Ihren Amazon S3-Bucket gesendet. Das folgende Beispiel zeigt das allgemeine Format eines Amazon Chime SDK Voice Connector-Aufrufdetaildatensatznamens.

```
Amazon-Chime-Voice-Connector-CDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-
j3456789k012
```

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

```
Amazon-Chime-Voice-Connector-CDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

Das folgende Beispiel zeigt das allgemeine Format eines Amazon Chime SDK Voice Connector-Aufrufdetaildatensatzes.

```
{
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "Status": "Completed",
    "StatusMessage": "OK",
    "SipAuthUser": "XXXX",
    "BillableDurationSeconds": 6,
    "BillableDurationMinutes": 0.1,
    "SchemaVersion": "2.0",
    "SourcePhoneNumber": "+12065550100",
    "SourcePhoneNumberName": "North Campus Reception",
    "SourceCountry": "US",
    "DestinationPhoneNumber": "+12065550101",
    "DestinationPhoneNumberName": "South Campus Reception",
    "DestinationCountry": "US",
    "UsageType": "USE1-US-US-outbound-minutes",
```

```
    "ServiceCode": "AmazonChimeVoiceConnector",
    "Direction": "Outbound",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
    "Region": "us-east-1",
    "Streaming": true
}
```

Streaming-Detaildatensätze für Amazon Chime SDK Voice Connector

Wenn Sie sich dafür entscheiden, Anrufdetaildatensätze für Ihren Amazon Chime SDK Voice Connector zu empfangen und Medien an Kinesis Video Streams zu streamen oder SIPREC-Anforderungen zu senden, werden Streaming-Detaildatensätze an Ihren Amazon S3-Bucket gesendet. Weitere Informationen finden Sie unter Amazon Chime SDK Voice Connector-Medien an Kinesis streamen.

Das folgende Beispiel zeigt das allgemeine Format des Namens eines Streaming-Detaildatensatzes.

```
Amazon-Chime-Voice-Connector-SDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-
j3456789k012
```

Das folgende Beispiel zeigt die Daten, die im Namen des Streaming-Detaildatensatzes dargestellt werden.

```
Amazon-Chime-Voice-Connector-SDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

Das folgende Beispiel zeigt das allgemeine Format eines Streaming-Detaildatensatzes.

```
{
    "SchemaVersion": "1.0",
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
```

```
    "Status": "Completed",
    "StatusMessage": "Streaming succeeded",
    "ServiceCode": "AmazonChime",
    "UsageType": "USE1-VC-kinesis-audio-streaming",
    "BillableDurationSeconds": 6,
    "Region": "us-east-1"
}
```

Netzwerkkonfiguration und Bandbreiten-Anforderungen

Das Amazon Chime SDK 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.

Das Amazon Chime SDK verwendet Amazon Elastic Compute Cloud (Amazon EC2) und andere AWS Dienste auf Port TCP/443. Wenn Ihre Firewall den Port TCP/443 blockiert, müssen Sie für die folgenden Dienste eine `*.amazonaws.com` Zulassungsliste oder AWS IP-Adressbereiche in die Liste aufnehmen: Allgemeine AWS-Referenz

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Allgemein

Die folgenden Ziele und Ports sind erforderlich, wenn Sie das Amazon Chime SDK in Ihrer Umgebung ausführen.

Bestimmungsort	Ports
*.chime.aws	TCP:443
*.amazonaws.com	TCP:443

Amazon Chime SDK WebRTC-Mediensitzungen

Domain	Subnetz	Ports
*.chime.aws	99.77.128.0/18	TCP:443 UDP:3478
*.sdkassets.chime.aws		TCP:443

Amazon Chime SDK Sprachanschluss

Die folgenden Ziele und Ports werden empfohlen, wenn Sie Amazon Chime SDK Voice Connectors verwenden.

SIP-Signalisierung

AWS-Region	Bestimmungsort	Ports
USA Ost (Nord-Virginia)	3.80.16.0/23	UDP/5060 TCP/5060 TLS/5061
USA West (Oregon)	99.77.253.0/24	UDP/5060 TCP/5060 TLS/5061
Asien-Pazifik (Seoul)	99,77,242,0/24	UDP/5060 TCP/5060 TLS/5061
Asien-Pazifik (Singapur)	99,77,240,0/24	UDP/5060 TCP/5060 TLS/5061
Asien-Pazifik (Sydney)	99,77,239,0/24	UDP/5060 TCP/5060 TLS/5061
Asien-Pazifik (Tokio)	99,77,244,0/24	UDP/5060 TCP/5060

AWS-Region	Bestimmungsort	Ports
		TLS/5061
Kanada (Zentral)	99,77,233,0/24	UDP/5060 TCP/5060 TLS/5061
Europa (Frankfurt)	99,77,247,0/24	UDP/5060 TCP/5060 TLS/5061
Europa (Irland)	99,77,250,0/24	UDP/5060 TCP/5060 TLS/5061
Europa (London)	99,77,249,0/24	UDP/5060 TCP/5060 TLS/5061

Medien

AWS Region	Bestimmungsort	Ports
Asien-Pazifik (Seoul)	99,77,242,0/24	UDP/5000:65000
Asien-Pazifik (Singapur)	99,77,240,0/24	UDP/5000:65000
Asien-Pazifik (Sydney)	99,77,239,0/24	UDP/5000:65000
Asien-Pazifik (Tokio)	99,77,244,0/24	UDP/5000:65000
Kanada (Zentral)	99,77,233,0/24	UDP/5000:65000

AWS Region	Bestimmungsort	Ports
Europa (Frankfurt)	99,77,247,0/24	UDP/5000:65000
Europa (Irland)	99,77,250,0/24	UDP/5000:65000
Europa (London)	99,77,249,0/24	UDP/5000:65000
USA Ost (Nord-Virginia)	3.80.16.0/23	UDP/5000:65000
USA Ost (Nord-Virginia)	52.55.62.128/25	UDP/1024:65535
USA Ost (Nord-Virginia)	52.55.63.0/25	UDP/1024:65535
USA Ost (Nord-Virginia)	34.212.95.128/25	UDP/1024:65535
USA Ost (Nord-Virginia)	34.223.21.0/25	UDP/1024:65535
USA West (Oregon)	99.77.253.0/24	UDP/5000:65000

Amazon Voice Focus für Spediteure, Medienziele und Häfen

AWS Region	Bestimmungsort	Ports
USA Ost (Nord-Virginia)	99,77,254,0/24	UDP/5000:65000
USA West (Oregon)	99,77,232,0/24	UDP/5000:65000

Anforderungen an die Bandbreite

Das Amazon Chime SDK hat die folgenden Bandbreitenanforderungen für die bereitgestellten Medien:

- 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
  - 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

Für Amazon Chime SDK Voice Connectors gelten die folgenden Bandbreitenanforderungen:

- Audio
  - Gespräch: ~90 Kbit/s nach oben und nach unten. Dazu gehören Medien-Nutzlast und Paket-Overhead.
- T.38-Fax
  - Mit V.34: ~40 Kbit/s. Dazu gehören Medien-Nutzlast und Paket-Overhead.
  - Ohne V.34: ~20 Kbit/s. Dazu gehören Medien-Nutzlast und Paket-Overhead.

Administrative Unterstützung für das Amazon Chime SDK

Wenn Sie Administrator sind und den Support für das Amazon Chime SDK kontaktieren müssen, wählen Sie eine der folgenden Optionen aus:

- Wenn Sie bereits über ein AWS-Support-Konto verfügen, rufen Sie das Support-Center auf und senden Sie ein Ticket.
- Öffnen Sie andernfalls die AWS Management Console und wählen Sie Amazon Chime SDK , Support , Anfrage senden aus.

Es ist hilfreich, die folgenden Informationen anzugeben:

- Eine ausführliche Beschreibung des Problems.
- Den Zeitpunkt, zu dem das Problem aufgetreten ist, einschließlich Ihrer Zeitzone.

Dokumentenverlauf für das Amazon Chime SDK Administration Guide

In der folgenden Tabelle werden wichtige Änderungen am Amazon Chime SDK-Administrationshandbuch beschrieben, die im März 2022 beginnen. Abonnieren Sie einen RSS-Feed für Benachrichtigungen über Aktualisierungen dieser Dokumentation.

Änderung	Beschreibung	Datum
Alexa In-Skill Calling wurde entfernt	Aufgrund von Änderungen durch das Amazon Alexa-Team können Sie Alexa-Anrufe nicht mehr zu SIP-Medienanwendungen hinzufügen. Weitere Informationen finden Sie auf der Seite Alexa Smart Properties.	1. April 2024
Die Richtlinie für dienstbezogene Rollen wurde aktualisiert	Die `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` zusätzliche Berechtigung, die es ermöglicht CloudWatch , Metriken für die Verwendung in Service-Dashboards bereitzustellen. Weitere Informationen finden Sie unter Verwenden von Rollen mit Amazon Chime SDK-Medien-Pipelines und verwalteten AWS-Richtlinien: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	8. Dezember 2023

Aktualisierte Richtlinie für dienstbezogene Rollen, neue Meeting-Regionen	Die `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` zusätzlichen Berechtigungen, die es Kinesis Video Streams ermöglichen, Audio-, Video- und Screenshare-Daten an Amazon Chime SDK-Meetings zu streamen. Weitere Informationen finden Sie unter Verwenden von Rollen mit Amazon Chime SDK-Medien-Pipelines und AWS-verwalteten Richtlinien:. AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	25. September 2023
Verbesserung der Stimme	Administratoren können jetzt die Sprachverbesserung aktivieren, eine Funktion, die die Audioqualität von PSTN-Anrufen verbessert, aktivieren. Weitere Informationen finden Sie im Abschnitt Grundlegendes zur Sprachverbesserung unter Erstellen einer Konfiguration für Anrufanalysen.	31. August 2023

Die Richtlinie für dienstbezogene Rollen wurde aktualisiert	Die `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` hinzugefügten Berechtigungen, die den Zugriff auf die GetMediaInsightsPipelineConfigurationAPI ermöglichen. Amazon Chime Voice Connectors benötigen diese Berechtigungen, um Media Insights-Pipeline-Konfigurationen zu erhalten. Weitere Informationen finden Sie unter Voice Connectors für die Verwendung von Anrufanalysen konfigurieren.	14. April 2023
Tagging für Voice Connectors	Administratoren können Amazon Chime SDK Voice Connectors jetzt Tags zuweisen. Tags weisen Metadaten in Form von Schlüssel-Wert-Paaren zu, die Sie definieren. Weitere Informationen finden Sie unter Verwenden von Tags mit Voice Connectors.	13. April 2023

Neue und aktualisierte Richtlinien für dienstverknüpfte Rollen	Entwickler können die verknüpfte Rolle mit dem AmazonChime SDKEvents -Dienst verwenden, um auf Streaming-Dienste wie Kinesis Firehose zuzugreifen. Weitere Informationen finden Sie unter Verwenden der dienstverknüpften Rolle mit SDKEvents AmazonChime. Wir haben den `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` Namen auch zu Using service linked roles hinzugefügt. Weitere Informationen finden Sie unter Verwenden von AmazonChimeVoiceConnectorServiceLinkedRolePolicy.	27. März 2023
Anrufanalysen und Sprachanalysen	Administratoren und Entwickler mit Administratorberechtigungen können Voice Connectors für die Verwendung mit Anrufanalysen konfigurieren. Bei Bedarf können Sie auch Sprachanalysen aktivieren. Weitere Informationen finden Sie in diesem Handbuch unter Verwaltung von Amazon Chime SDK-Anrufanalysen und Konfiguration von Voice Connectors für die Verwendung von Anrufanalysen.	27. März 2023

Die Sicherheitsrichtlinie wurde aktualisiert	Die AWS verwaltete Amazon Chime SDK-Richtlinie fügte neue Berechtigungen hinzu, die es Ihnen ermöglichen, Amazon Chime SDK Media Pipelines zu verwenden, um Media Pipelines zu erstellen, zu lesen und zu löschen.	10. Januar 2023
Neue AWS Regionen für die SIP-Signalisierung	Administratoren können SIP-Medienanwendungen jetzt AWS Regionen in Asien, Kanada und Europa zuordnen. Weitere Informationen finden Sie unter Netzwerkkonfiguration und Bandbreitenanforderungen.	18. November 2022
Telefonieren mit Alexa	Entwickler von Alexa Skill könnten Anrufe direkt von ihren Skills aus aktivieren. Diese Funktion wurde entfernt.	18. November 2022
Notruf 911 aktualisiert	Wir haben den Notrufprozess aktualisiert. Weitere Informationen finden Sie unter Notruf einrichten.	04. August 2022

Neue serviceverknüpfte Rolle	Eine neue dienstbezogene Rolle ermöglicht es Entwickle rn, Medien-Pipelines in Amazon Chime SDK-Meeti ngs zu verwenden. Weitere Informationen finden Sie unter AWS-verwaltete Richtlini e: AmazonChime SDK MediaPipelinesServiceLinked RolePolicy.	26. April 2022
Amazon Chime SDK-Admin istrationshandbuch veröffent licht	Das Amazon Chime SDK-Administrationshandbuch wurde veröffentlicht. Informati onen zu Änderungen vor März 2022 finden Sie unter Dokumentverlauf für Amazon Chime im Amazon Chime Chime-Administratorhandbuch .	24. März 2022

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.