aws

관리 설명서

Amazon Chime

Amazon Chime: 관리 설명서

Table of Contents

Amazon Chime 시스템 관리자만 이 안내서의 단계를 완료할 수 있습니다. Amazon Chime 데스크톱 클라이언트, 웹 앱 또는 모바일 앱과 관련하여 도움이 필요한 경우 Amazon Chime 사용 설명서의 지원 받기를 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.

Amazon Chime이란 무엇인가요?

Amazon Chime은 안전하고 포괄적인 애플리케이션을 통해 온라인 회의를 혁신적으로 바꾸는 커뮤니케이션 서비스입니다. Amazon Chime은 디바이스 간에 원활하게 작동하므로 연결성을 유지할 수 있습니다. Amazon Chime은 온라인 회의, 화상 회의, 통화, 채팅에 사용할 수 있습니다. 조직 내부 및 외부에서 콘텐츠를 공유할 수도 있습니다. Amazon Chime은 AWS 클라우드에서 안전하게 실행되는 완전 관리형 서비스로, IT 부서에서 복잡한 인프라를 배포하고 관리할 필요가 없습니다.

자세한 내용은 Amazon Chime을 참조하세요.

관리 개요

관리자는 Amazon Chime 콘솔을 사용하여 Amazon Chime 계정을 생성하고 사용자와 권한을 관리하는 등의 주요 태스크를 수행합니다. Amazon Chime 콘솔에 액세스하여 Amazon Chime 관리자 계정을 생성하려면 먼저 AWS 계정을 생성해야 합니다. 자세한 내용은 Amazon Chime 시스템 관리자를 위한 사전 조건 문서를 참조하세요.

시작하는 방법

Amazon Chime 시스템 관리자를 위한 사전 조건 섹션을 완료한 후에 Amazon Chime 관리자 계정을 생성 및 구성하여 사용자를 추가할 수 있습니다. 사용자에 대해 기본 또는 프로 권한을 선택합니다.

이제 시작할 준비가 되었으면 다음 자습서를 참조하세요.

- 시작하기

사용자 액세스 및 권한에 대한 자세한 내용은 사용자 권한 및 액세스 관리 단원을 참조하세요. 프로 및 기본 권한이 부여된 사용자가 액세스할 수 있는 기능에 대한 자세한 내용은 플랜 및 요금 단원을 참조하세요.

요금

Amazon Chime은 사용량을 기반으로 요금을 청구합니다. 회의가 주최된 날에 회의를 주최한 프로 권한이 있는 사용자에 대해서만 요금을 지불하면 됩니다. 회의 참석자와 채팅 사용자에게는 요금이 청구되지 않습니다.

기본 권한이 부여된 사용자에게는 요금이 부과되지 않습니다. 기본 사용자는 회의를 주최할 수 없지만 회의에 참여하고 채팅을 사용할 수는 있습니다. 요금에 대한 자세한 내용과 프로 및 기본 권한이 부여된 사용자가 액세스할 수 있는 기능에 대한 자세한 내용은 플랜 및 요금 단원을 참조하세요.

리소스

Amazon Chime에 대한 자세한 내용은 다음 리소스를 참조하세요.

- Amazon Chime 도움말 센터
- Amazon Chime 교육 동영상

Amazon Chime 시스템 관리자를 위한 사전 조건

Amazon Chime 콘솔에 액세스하고 Amazon Chime 관리자 AWS 계정을 생성하려면 계정이 있어야 합니다.

Amazon Web Services 계정 생성

Amazon Chime의 관리자 계정을 생성하려면 먼저 AWS 계정을 생성해야 합니다.

주제

- 가입하세요 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성

가입하세요 AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요 AWS 계정 루트 사용자

1. Root user를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

Amazon Chime 관리자 계정 설정에 대한 자세한 내용은 시작하기 섹션을 참조하세요.

시작하기

사용자가 Amazon Chime을 시작하는 가장 쉬운 방법은 30일 동안 무료로 사용할 수 있는 Amazon Chime 프로 버전을 다운로드하여 설치하는 것입니다. 자세한 내용은 Amazon Chime 다운로드를 참조하세요.

Amazon Chime 구매

30일 무료 평가판 사용 기간 후에도 Amazon Chime 프로 버전을 계속 사용하려면, Amazon Chime 관리자 계정을 생성하여 사용자를 추가해야 합니다. 시작하려면 먼저 AWS 계정 생성을 포함하는 Amazon Chime 시스템 관리자를 위한 사전 조건를 완료해야 합니다. 이때 Amazon Chime 관리자 계정을 생성 및 구성하고 다음 작업을 완료하여 사용자를 추가할 수 있습니다.

작업

- 1단계: Amazon Chime 관리자 계정 생성
- 2단계(선택 사항): 계정 설정 구성
- 3단계: 계정에 사용자 추가
- (선택 사항) Amazon Chime 계정에 대한 전화번호 설정

1단계: Amazon Chime 관리자 계정 생성

Amazon Chime 시스템 관리자를 위한 사전 조건 섹션을 완료한 후에는 Amazon Chime 관리자 권한을 생성할 수 있습니다.

Amazon Chime 관리자 계정 생성 방법

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 새 계정를 선택합니다.
3. 계정 이름에 해당 계정의 이름을 입력하고 계정 생성을 선택합니다.
4. (선택 사항) Amazon Chime이 사용 가능한 모든 리전에서 회의를 위해 최적의 AWS 리전을 선택하도록 허용할지 또는 사용자가 선택한 리전만 사용하도록 허용할지 선택할 수 있습니다. 자세한 내용은 회의 설정 관리 섹션을 참조하세요.

2단계(선택 사항): 계정 설정 구성

기본적으로 새 계정은 팀 계정으로 생성됩니다. 도메인을 신청하여 본인의 자격 증명 공급자 또는 Okta SSO에게 연결하는 것을 선호하는 경우에는 엔터프라이즈 계정으로 변환할 수 있습니다. 팀 및 엔터프라이즈 계정 유형에 대한 자세한 내용은 Amazon Chime 팀 계정 또는 엔터프라이즈 계정 중 선택 단원을 참조하십시오.

팀 계정을 엔터프라이즈 계정으로 변환하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 계정 이름을 선택합니다.
3. 자격 증명에서 시작하기를 선택합니다.
4. 콘솔의 단계에 따라 도메인을 신청합니다.
5. (선택 사항) 콘솔의 단계에 따라 자격 증명 공급자를 설정하고 디렉터리 그룹을 구성합니다.

도메인 신청에 대한 자세한 내용은 도메인 신청 단원을 참조하십시오. 자격 증명 공급자 설정에 대한 자세한 내용은 Active Directory에 연결 및 Okta SSO에 연결 단원을 참조하십시오.

또한 공유 화면 및 Amazon Chime 내게 전화 걸기 기능에 대한 원격 제어 등의 옵션에 대한 계정 정책을 허용 또는 금지할 수 있습니다.

계정 정책을 구성하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 해당 계정의 이름을 선택하여 구성합니다.
3. 설정에서 회의를 선택합니다.
4. 정책에 대해 허용 또는 금지할 계정 정책 옵션을 선택하거나 선택 취소합니다.
5. 변경을 선택합니다.

자세한 내용은 회의 설정 관리 섹션을 참조하세요.

3단계: 계정에 사용자 추가

Amazon Chime 팀 계정을 생성한 후에 본인과 사용자를 초대하여 가입할 수 있도록 합니다. 본인 계정을 엔터프라이즈 계정으로 업그레이드하는 경우 사용자를 초대할 필요가 없습니다. 그 대신 엔터프라

이즈 계정으로 업그레이드하고 도메인을 신청합니다. 자세한 내용은 2단계(선택 사항): 계정 설정 구성 섹션을 참조하세요.

Amazon Chime 계정에 사용자를 추가하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 계정의 이름을 선택합니다.
3. 사용자 페이지에서 사용자 초대를 선택합니다.
4. 본인 등 초대할 사용자의 이메일 주소를 입력하고 사용자 초대를 선택합니다.

초대한 사용자에게 생성한 Amazon Chime 팀 계정에 가입을 초대하는 이메일이 발송됩니다. 초대된 사용자가 Amazon Chime 사용자 계정을 등록하는 경우, 기본적으로 프로 권한이 부여되고 30일 무료 사용은 종료됩니다. 초대된 사용자가 이미 업무용 이메일 주소로 Amazon Chime 사용자 계정에 등록한 경우, 해당 계정을 계속 사용할 수 있습니다. 또한 Amazon Chime 다운로드를 선택하고 사용자 계정에 로그인하여 언제든지 Amazon Chime 클라이언트 앱을 다운로드할 수 있습니다.

회의를 주최할 때 프로 권한을 사용하는 사용자에 대해서만 요금이 청구됩니다. 기본 권한이 부여된 사용자에게는 요금이 부과되지 않습니다. 기본 사용자는 회의를 주최할 수 없지만 회의에 참여하고 채팅을 사용할 수는 있습니다. 요금에 대한 자세한 내용과 프로 및 기본 권한이 부여된 사용자가 액세스할 수 있는 기능에 대한 자세한 내용은 플랜 및 요금 섹션을 참조하세요.

사용자 권한을 변경하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 계정의 이름을 선택합니다.
3. 사용자 페이지에서 권한을 변경할 사용자를 선택합니다.
4. 사용자 작업, 사용자 권한 할당을 선택합니다.
5. 권한에서 프로 또는 기본을 선택합니다.
6. 할당을 선택합니다.

다른 사용자에게 관리자 권한을 부여할 수 있고, 본인 계정의 Amazon Chime 콘솔에 대한 해당 사용자의 액세스를 제어할 수 있습니다. 자세한 내용은 Amazon Chime용 Identity and Access Management 섹션을 참조하세요.

(선택 사항) Amazon Chime 계정에 대한 전화번호 설정

Amazon Chime 관리자 계정에는 다음과 같은 전화 옵션을 사용할 수 있습니다.

Amazon Chime Business Calling

사용자가 Amazon Chime에서 직접 전화 통화를 걸고 받거나 문자 메시지를 전송하고 수신할 수 있습니다. Amazon Chime 콘솔에서 전화번호를 프로비저닝하거나 기존 전화번호를 이식합니다. Amazon Chime을 사용하여 전화 통화를 걸고 받거나 문자 메시지를 전송하고 수신하는 권한을 Amazon Chime 사용자에게 할당할 수 있습니다. 자세한 정보는 Amazon Chime에서 전화번호 관리 및 기존 전화번호 포팅 섹션을 참조하세요.

Amazon Chime Voice Connector

기존 전화 시스템에 SIP 트렁킹 서비스를 제공합니다. 기존 전화번호를 이식하거나 Amazon Chime 콘솔에서 새 전화번호를 프로비저닝합니다. 자세한 내용은 Amazon Chime SDK 관리 안내서의 Amazon Chime Voice Connector 관리를 참조하세요.

Amazon Chime 계정 관리

Amazon Chime은 개별 사용자 또는 관리자가 없는 그룹으로 사용할 수 있습니다. 하지만 관리자 기능을 추가하거나 Amazon Chime 프로를 구매하려면 AWS Management Console에서 Amazon Chime 계정을 생성해야 합니다. Amazon Chime 관리자 계정을 생성하는 방법을 알아보거나, Amazon Chime 프로 구매에 대한 자세한 내용을 알아보려면 시작하기 섹션을 참조하세요.

다양한 유형의 Amazon Chime 관리자 계정에 대한 자세한 내용은 Amazon Chime 팀 계정 또는 엔터프라이즈 계정 중 선택 섹션을 참조하세요. 기존 관리자 계정 관리에 대한 자세한 내용은 아래의 주제를 참조하세요.

주제

- Amazon Chime 팀 계정 또는 엔터프라이즈 계정 중 선택
- 도메인 신청
- 팀 계정을 엔터프라이즈 계정으로 변환
- 계정 이름 바꾸기
- 계정 삭제
- 회의 설정 관리
- 채팅 보존 정책 관리
- 채팅 메시지 복원
- 채팅 메시지 삭제
- Active Directory에 연결
- Okta SSO에 연결
- Outlook용 Amazon Chime 추가 기능 배포
- Amazon Chime Meetings App for Slack 설정

Amazon Chime 팀 계정 또는 엔터프라이즈 계정 중 선택

Amazon Chime 관리자 계정을 생성할 때 팀 계정을 만들지 또는 엔터프라이즈 계정을 만들지 선택합니다. Amazon Chime 관리자 계정에 대한 자세한 내용은 시작하기 섹션을 참조하세요.

팀 계정

팀 계정을 사용하면 이메일 도메인을 요청하지 않고도 사용자를 초대한 후 해당 사용자에게 Amazon Chime 프로 권한을 부여할 수 있습니다. 프로 및 기본 권한에 대한 자세한 내용은 요금제 및 요금을 참조하세요.

다른 조직에서 요청하지 모든 이메일 도메인의 사용자를 초대할 수 있습니다. 사용자가 회의를 주최할 때만 그들에 대한 비용을 지불하면 됩니다. 팀 계정의 사용자는 Amazon Chime 앱을 사용하여 동일한 계정에 등록된 다른 Amazon Chime 사용자를 검색하고 연락할 수 있습니다. 또한 조직 외부의 프로 사용자에 대한 비용을 지불할 경우 팀 계정을 선택하는 것이 좋습니다.

엔터프라이즈 계정

엔터프라이즈 계정을 사용하면 조직의 도메인에서 사용자를 더 세부적으로 제어할 수 있습니다. 자체적인 자격 증명 공급자 또는 Okta SSO에 연결하여 인증하고 프로 또는 기본 권한을 할당하도록 선택할 수 있습니다. Amazon Chime은 Microsoft Active Directory도 지원합니다.

엔터프라이즈 계정을 생성하려면 하나 이상의 이메일 도메인을 요청해야 합니다. 이렇게 하면 요청한 도메인을 사용하여 Amazon Chime에 로그인하는 모든 사용자가 중앙 관리식 Amazon Chime 계정에 포함될 수 있습니다. 엔터프라이즈 계정은 지원되는 디렉터리 통합을 통해 사용자를 관리할 때 필요합니다. 자세한 내용은 도메인 신청 및 Active Directory에 연결 섹션을 참조하세요.

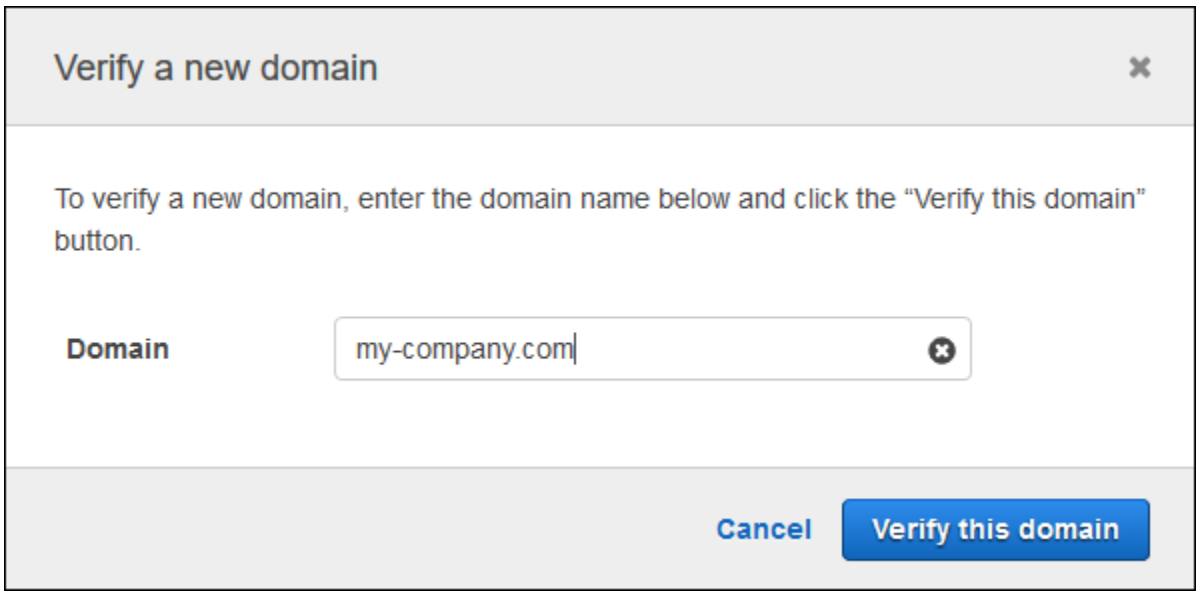
또한 엔터프라이즈 계정에서 사용자 활성화 및 일시 중지를 관리할 수 있습니다. 자세한 정보는 사용자 권한 및 액세스 관리을 참조하세요.

도메인 신청

엔터프라이즈 계정을 생성하고 계정 및 사용자에 대해 제공되는 보다 강력한 제어를 통해 이점을 누리려면 하나 이상의 이메일 도메인을 신청해야 합니다.

도메인을 신청하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 팀 계정의 이름을 선택합니다.
3. 탐색 창에서 자격 증명, 도메인을 선택합니다.
4. 도메인 페이지에서 새 도메인 신청을 선택합니다.
5. 도메인에 대해, 조직에서 이메일 주소에 사용하는 도메인을 입력합니다. 이 도메인 확인을 선택합니다.



6. 화면의 지시에 따라 TXT 레코드를 사용자 도메인의 DNS 서버에 추가합니다. 일반적으로 이 프로세스에는 도메인 계정에 로그인하고, 도메인의 DNS 레코드를 찾고, Amazon Chime이 제공한 이름과 값을 사용하여 TXT 레코드를 추가하는 작업이 포함됩니다. 도메인의 DNS 레코드 업데이트에 대한 자세한 내용은 DNS 공급자 또는 도메인 이름 등록 대행자를 위한 설명서를 참조하십시오.

   Amazon Chime에서는 사용자가 도메인을 소유하고 있는지 확인하기 위해 이 레코드의 존재 여부를 확인합니다. 도메인이 확인되면 해당 상태가 확인 보류에서 확인됨으로 변경됩니다.

   > **Note**
   >
   > Amazon Chime에 의한 DNS 변경 및 확인이 전파되는 데는 최대 24시간이 걸릴 수 있습니다.

7. 조직이 이메일 주소에 추가 도메인 또는 하위 도메인을 사용하는 경우, 각 도메인에 대해 이 절차를 반복합니다.

도메인 신청 문제 해결에 대한 자세한 내용은 도메인 신청 요청이 확인되지 않는 이유는 무엇입니까?를 참조하세요.

팀 계정을 엔터프라이즈 계정으로 변환

기존 팀 계정을 엔터프라이즈 계정으로 변환하려면 Amazon Chime 콘솔에서 하나 이상의 이메일 도메인을 요청합니다. 팀 및 엔터프라이즈 계정의 차이점에 대한 자세한 내용은 Amazon Chime 팀 계정 또

는 엔터프라이즈 계정 중 선택 섹션을 참조하세요. 도메인 요청에 대한 자세한 내용은 도메인 신청 섹션을 참조하세요.

팀 계정을 엔터프라이즈 계정으로 변환하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 계정 이름을 선택합니다.
3. 자격 증명에서 시작하기를 선택합니다.
4. 콘솔의 단계에 따라 도메인을 신청합니다.
5. (선택 사항) 콘솔의 단계에 따라 자격 증명 공급자를 설정하고 디렉터리 그룹을 구성합니다.

계정이 엔터프라이즈 계정으로 전환되면 Active Directory 인스턴스를 통해 연결할지 여부를 결정할 수 AWS Directory Service있습니다. Active Directory 인스턴스에 연결하면 사용자가 Active Directory 자격 증명을 사용하여 Amazon Chime에 로그인할 수 있습니다. 자세한 정보는 Active Directory에 연결을 참조하세요.

Active Directory에 연결하지 않을 경우, 사용자는 Amazon으로 로그인 또는 Amazon.com 계정 자격 증명을 사용하여 Amazon Chime에 로그인을 계속 진행할 수 있습니다.

계정 이름 바꾸기

다음 단계는 관리하는 Amazon Chime 팀 및 엔터프라이즈 계정의 이름을 바꾸는 방법을 설명합니다. 선택한 이름은 사용자를 Amazon Chime에 가입하도록 초대하는 이메일에 표시됩니다.

계정 이름을 바꾸려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.

   계정 페이지는 기본적으로 표시됩니다.
2. 계정 이름 열에서 이름을 바꾸려는 계정을 선택합니다.
3. 왼쪽 창의 설정에서 계정을 선택합니다.

   계정 요약 페이지가 나타납니다.
4. 계정 작업 목록을 열고 계정 이름 변경을 선택합니다.

   계정 이름 변경 대화 상자가 나타납니다.
5. 새 계정 이름을 입력하고 저장을 선택합니다.

계정 삭제

에서 AWS 계정을 삭제하면 Amazon Chime 계정이 자동으로 삭제됩니다. AWS Management Console 또는 Amazon Chime 콘솔을 사용하여 Amazon Chime 팀 또는 엔터프라이즈 계정을 삭제할 수도 있습니다.

> **Note**
>
> 팀 또는 엔터프라이즈 계정에서 관리되지 않는 사용자는 Amazon Chime 도우미의 '사용자 삭제' 명령을 사용하여 삭제를 요청할 수 있습니다. 자세한 내용은 Amazon Chime 도우미 사용을 참조하세요.

팀 계정을 삭제하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 이름 열에서 계정을 선택한 후 설정에서 계정을 선택합니다.
3. 탐색 창에 사용자 페이지가 표시됩니다.
4. 사용자를 선택하고 사용자 작업, 사용자 제거를 선택합니다.
5. 탐색 창에서 계정, 계정 작업, 계정 삭제를 선택합니다.
6. 계정을 삭제하려 한다는 것을 확인합니다.

계정을 삭제할 때 Amazon Chime은 모든 사용자 데이터를 삭제합니다. 여기에는 AWS 계정, 개별 Amazon Chime 계정 또는 관리되지 않는 Amazon Chime 사용자의 해지가 포함됩니다. 그러나 Amazon Chime에서 생성한 사용자 계정 및 Amazon Chime 사용량(고객 계약에 따라 지원되는 서비스 속성)과 관련된 비 콘텐츠 데이터는 포함되지 않습니다.

엔터프라이즈 계정을 삭제하려면

1. 도메인을 제거합니다.

   > **Note**
   >
   > 도메인을 제거할 때 다음과 같이 진행됩니다.
   >
   > - 도메인과 연결된 사용자는 즉시 모든 디바이스에서 로그아웃되며 모든 연락처, 채팅 대화 및 채팅룸에 대한 액세스 권한을 상실합니다.

- 이 도메인의 사용자가 예약한 회의가 더 이상 시작되지 않습니다.
- 일시 중지된 사용자는 사용자 및 사용자 세부 정보 페이지에 계속 일시 중지됨 상태로 표시되며 자신의 데이터에 액세스할 수 없습니다. 해당 이메일 주소로 된 Amazon Chime 계정을 새로 만들 수 없습니다.
- 등록된 사용자는 사용자 및 사용자 세부 정보 페이지에 해제됨으로 표시되며 자신의 데이터에 액세스할 수 없습니다. 해당 이메일 주소로 된 Amazon Chime 계정을 새로 만들 수 있습니다.
- Active Directory 계정이 있고 사용자의 기본 이메일 주소와 연결된 도메인을 제거하는 경우 사용자가 Amazon Chime에 액세스할 수 없고 해당 프로필이 삭제됩니다. 사용자의 보조 이메일 주소와 연결된 도메인을 제거하면 해당 이메일 주소로 로그인할 수 없지만, 해당 Amazon Chime 연락처 및 데이터에 대한 액세스를 유지할 수 있습니다.
- 엔터프라이즈 OpenID Connect(OIDC) 계정이 있고 사용자의 기본 이메일 주소와 연결된 도메인을 제거하는 경우 사용자가 Amazon Chime에 더 이상 액세스할 수 없고 해당 프로필이 삭제됩니다.

2. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
3. 계정 페이지에서 팀 계정의 이름을 선택합니다.
4. 탐색 창에서 설정, 도메인을 선택합니다.
5. 도메인 페이지에서 도메인 제거를 선택합니다.
6. 탐색 창에서 계정, 계정 작업, 계정 삭제를 선택합니다.
7. 계정을 삭제하려 한다는 것을 확인합니다.

계정을 삭제할 때 Amazon Chime은 모든 사용자 데이터를 삭제합니다. 여기에는 AWS 계정, 개별 Amazon Chime 계정 또는 관리되지 않는 Amazon Chime 사용자의 해지가 포함됩니다. 그러나 Amazon Chime에서 생성한 사용자 계정 및 Amazon Chime 사용량(고객 계약에 따라 지원되는 서비스 속성)과 관련된 비 콘텐츠 데이터는 포함되지 않습니다.

회의 설정 관리

Amazon Chime 콘솔에서 회의 설정을 관리합니다.

회의 정책 설정

Amazon Chime 콘솔의 설정, 회의에서 계정 정책을 관리합니다. 다음 정책 옵션 중에서 선택합니다.

화면 공유에서 공유된 제어 활성화

조직의 사용자가 회의 중에 자신의 컴퓨터에 대한 공유된 제어 권한을 부여할 수 있는지 여부를 선택합니다. 사용자의 컴퓨터에 대한 공유된 제어를 요청하는 참석자는 원격 제어를 사용할 수 없다는 오류 메시지를 받습니다.

회의에 참여하기 위해 아웃바운드 통화 활성화

Amazon Chime 내게 전화 걸기 기능을 켭니다. Amazon Chime의 전화를 받아 회의에 참여할 수 있는 옵션을 제공합니다.

회의 애플리케이션 설정

Amazon Chime 콘솔의 설정, 회의에서 애플리케이션 액세스 권한을 관리합니다. 다음과 같은 옵션을 선택할 수 있습니다.

사용자가 Amazon Chime Meetings App for Slack을 사용하여 Amazon Chime에 로그인할 수 있도록 허용

이 옵션을 사용하면 조직의 사용자가 Amazon Chime Meetings App for Slack에서 Amazon Chime에 로그인할 수 있습니다. 자세한 정보는 Amazon Chime Meetings App for Slack 설정을 참조하세요.

회의 리전 설정

Amazon Chime은 회의 품질을 개선하고 지연 시간을 줄이기 위해 모든 참가자를 위한 최적의 AWS 지역에서 회의를 처리합니다. Amazon Chime이 사용 가능한 모든 리전에서 회의를 위해 최적의 리전을 선택하도록 허용할지 또는 사용자가 선택한 리전만 사용하도록 허용할지 선택할 수 있습니다.

언제든지 사용자 계정 회의 설정에서 이 설정을 업데이트할 수 있습니다. 회의 설정에서, 각 리전에서 처리 중인 Amazon Chime 회의의 비율을 볼 수도 있습니다.

회의 리전 설정을 업데이트하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 계정의 이름을 선택합니다.
3. 탐색 창에서 설정, 회의를 선택합니다.
4. 리전에서 다음 옵션 중 하나를 선택합니다.

- 회의 품질을 보장하기 위해 사용 가능한 모든 리전 사용 - Amazon Chime이 사용자를 대신하여 회의 처리를 최적화할 수 있습니다.
- 내가 선택한 리전만 사용 - 드롭다운 메뉴에서 리전을 선택할 수 있습니다.

5. 저장을 선택합니다.

채팅 보존 정책 관리

Amazon Chime 엔터프라이즈 계정을 하나 이상 관리하는 경우 다음에 대한 채팅 보존 정책을 설정할 수 있습니다.

- 엔터프라이즈 계정의 멤버만 포함하는 채팅 대화
- 엔터프라이즈 계정의 멤버가 만든 채팅룸

보존 정책은 설정한 기간에 따라 메시지를 자동으로 삭제합니다. 1일에서 15년까지 지속 기간을 설정할 수 있습니다.

> **Note**
>
> Amazon Chime 엔터프라이즈 계정의 보존 기간은 90일입니다. 이 정책은 계정에 속한 사용자 및 계정에 속하지 않는 사용자와 관련된 대화에 적용됩니다.
> 보존 정책은 다음에 적용되지 않습니다.
>
> - Amazon Chime 엔터프라이즈 계정의 멤버가 포함되지 않은 채팅 대화
> - Amazon Chime 엔터프라이즈 계정에 속하지 않은 사용자가 만든 채팅룸

보존 정책이 Amazon Chime 사용자에게 미치는 영향

엔터프라이즈 계정 관리자가 설정하는 보존 정책은 Amazon Chime 사용자가 동일한 엔터프라이즈 계정, 다른 엔터프라이즈 계정 또는 팀 계정에 속하는지 여부 또는 사용자가 계정의 구성원이 아닌지 여부에 따라 사용자에게 미치는 영향이 다릅니다.

엔터프라이즈 구성원 채팅 대화

다음 표는 보존 정책이 엔터프라이즈 계정 구성원의 채팅 대화에 미치는 영향을 보여줍니다.

채팅 대화에 다음 사용자가 포함된 경우	보존 정책은 다음과 같습니다.
사용자의 엔터프라이즈 계정에 속한 다른 구성원만	사용자의 관리자가 설정
사용자의 엔터프라이즈 계정 외부에 있는 모든 사용자	90일로 자동 설정

엔터프라이즈 구성원 채팅룸

다음 표는 보존 정책이 엔터프라이즈 계정 구성원의 채팅룸에 미치는 영향을 보여줍니다.

다음 사용자가 채팅룸을 만든 경우	보존 정책은 다음과 같습니다.
사용자의 엔터프라이즈 계정에 속한 구성원	사용자의 관리자가 설정
다른 엔터프라이즈 계정 구성원	다른 계정의 관리자가 설정
비 엔터프라이즈 계정 구성원	해당 사항 없음

구성원 채팅 대화

다음 표는 보존 정책이 팀 계정 구성원의 채팅 대화에 미치는 영향을 보여줍니다.

채팅 대화에 다음 사용자가 포함된 경우	보존 정책은 다음과 같습니다.
엔터프라이즈 계정의 구성원이 아닌 사용자만	해당 사항 없음
엔터프라이즈 계정의 구성원 한 명 이상	90일로 자동 설정

팀 구성원 채팅룸

다음 표는 보존 정책이 팀 계정 구성원의 채팅룸에 미치는 영향을 보여줍니다.

다음 사용자가 채팅룸을 만든 경우	보존 정책은 다음과 같습니다.
팀 계정 사용자	해당 사항 없음

다음 사용자가 채팅룸을 만든 경우	보존 정책은 다음과 같습니다.
엔터프라이즈 계정 구성원이 아닌 모든 사용자	해당 사항 없음
엔터프라이즈 계정의 구성원	엔터프라이즈 계정의 관리자가 설정

엔터프라이즈 또는 팀 계정의 구성원이 아닌 Amazon Chime 사용자에게는 엔터프라이즈 계정의 구성원이 만든 채팅룸의 채팅룸 보존 정책만 적용됩니다.

엔터프라이즈 또는 팀 계정에 속하지 않은 수신자와의 채팅 대화

다음 표는 보존 정책이 Amazon Chime 엔터프라이즈 또는 팀 계정의 구성원이 아닌 사용자의 채팅 대화에 미치는 영향을 보여줍니다.

채팅 대화에 다음 사용자가 포함된 경우	보존 정책은 다음과 같습니다.
엔터프라이즈 계정의 구성원이 아닌 사용자만	해당 사항 없음
엔터프라이즈 계정의 구성원 한 명 이상	90일로 자동 설정

엔터프라이즈 또는 팀 계정에 속하지 않은 사용자가 만든 채팅룸

다음 표는 보존 정책이 Amazon Chime 엔터프라이즈 또는 팀 계정의 구성원이 아닌 사용자의 채팅룸에 미치는 영향을 보여줍니다.

다음 사용자가 채팅룸을 만든 경우	보존 정책은 다음과 같습니다.
엔터프라이즈 또는 팀 계정의 구성원이 아닌 사용자	해당 사항 없음
팀 계정 사용자	해당 사항 없음
엔터프라이즈 계정의 구성원	엔터프라이즈 계정의 관리자가 설정

채팅 보존 활성화

Amazon Chime 엔터프라이즈 계정 관리자는 Amazon Chime 콘솔을 사용하여 해당 계정의 채팅 대화 및 채팅룸의 채팅 보존을 활성화할 수 있습니다. 언제든지 콘솔을 사용하여 채팅 보존 기간을 업데이트하거나 채팅 보존을 비활성화할 수도 있습니다.

채팅 보존을 활성화하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 해당 계정의 이름을 선택합니다.
3. 탐색 창의 설정에서 보존을 선택합니다.
4. 보존 페이지의 채팅 대화 보존에서 슬라이더를 켜기로 이동합니다.
5. 보존 기간에서 첫 번째 상자에 숫자를 입력한 다음 상자 옆에 있는 목록을 열고 일, 주 또는 연도를 선택합니다.
6. 채팅방 보존에서 4-5단계를 반복합니다. 완료하였으면 저장을 선택합니다.

보존 기간을 설정한 후 1일 이내에 계정의 사용자는 보관 기간 외에 전송된 메시지에 액세스할 수 없게 됩니다.

채팅 메시지 복원

> **Note**
>
> Amazon Chime Enterprise 계정 관리자만 이 단계를 완료할 수 있습니다.

채팅 보존 기간을 설정한 후 30일 이내에 채팅 메시지를 복원할 수 있습니다. 채팅 메시지를 복원하면 Amazon Chime 계정의 모든 사용자가 보낸 모든 메시지가 복원됩니다.

30일 기간 내에 다음 중 하나를 수행하여 메시지를 복원할 수 있습니다.

- Amazon Chime 콘솔을 사용하여 데이터 보존 기능을 해제할 수 있습니다.

  -또는-

- 보존 기간을 연장하십시오.

30일의 유예 기간이 지나면 보존 기간에 해당하는 모든 채팅 메시지가 영구적으로 삭제됩니다. 새 채팅 메시지는 보존 기간이 경과하는 즉시 영구 삭제됩니다.

보존 기간 설정 또는 변경에 대한 자세한 내용은 이 섹션 앞부분을 참조하십시오채팅 보존 활성화.

사용자 또는 계정 구성원이 다음 작업 중 하나를 수행하는 경우에도 Amazon Chime에서 채팅 메시지가 영구적으로 삭제됩니다.

- Amazon Chime 채팅방을 삭제합니다. 채팅방 삭제에 대한 자세한 내용은 Amazon Chime 사용 설명서의 채팅방 삭제를 참조하십시오.
- 채팅 메시지가 있는 Amazon Chime 회의를 종료하십시오.

> **Note**
>
> 필요에 따라 회의에서 채팅 메시지를 수동으로 복사하고 저장할 수 있지만 회의가 종료되기 전에 복사해야 합니다. 자세한 내용은 Amazon Chime 사용 설명서의 미팅 내 채팅 사용을 참조하십시오.

채팅 메시지 삭제

데이터 보존 정책을 준수하기 위해 Amazon Chime은 모든 채팅 메시지를 보관하고 최종 사용자가 전송한 메시지를 삭제하지 못하도록 합니다. 하지만 Amazon Chime 시스템 관리자는 한 쌍의 API를 사용하여 대화와 채팅방에서 개별 메시지를 삭제할 수 있습니다. 메시지는 관리자의 Amazon Chime 계정에 있어야 합니다.

사용자는 메시지 ID와 해당 대화 또는 채팅방 ID를 보내 메시지 삭제를 요청할 수 있습니다. Amazon Chime 사용 설명서의 채팅 기능 사용 항목에서 방법을 설명합니다.

삭제 요청을 받으면 코드를 작성하거나 AWS CLI를 사용하여 다음 API를 호출할 수 있습니다.

메시지를 제거하려면

- 다음 중 하나를 수행하십시오.
  - 대화 메시지의 경우 — API를 사용합니다. RedactConversationMessage

    CLI에서 다음 명령을 실행합니다.

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

- 채팅방 메시지의 경우 — RedactRoomMessageAPI를 사용합니다.

  CLI에서 다음 명령을 실행합니다.

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

Active Directory에 연결

Amazon Chime 관리자 계정을 Active Directory에 연결하면 다음과 같은 기능을 통해 이점을 누릴 수 있습니다.

- Amazon Chime 사용자는 자신의 Active Directory 자격 증명으로 로그인할 수 있습니다.
- Amazon Chime 관리자는 암호 교체, 암호 복잡성 규칙 및 멀티 팩터 인증을 비롯하여 어떤 자격 증명 보안 기능을 추가할지 선택할 수 있습니다.
- Active Directory에서 사용자 계정을 제거하면 해당 사용자의 Amazon Chime 계정도 제거됩니다.
- Amazon Chime 프로 권한을 받을 Active Directory 그룹을 지정할 수 있습니다.
  - 기본 또는 프로 권한을 받도록 여러 그룹을 구성할 수 있습니다.
  - 사용자가 Amazon Chime에 로그인하려면 어느 한 그룹의 멤버여야 합니다.
  - 두 그룹의 사용자는 모두 프로 라이선스를 받습니다.

사용자 권한 관리에 대한 자세한 내용은 사용자 권한 및 액세스 관리 섹션을 참조하세요.

필수 조건

Amazon Chime의 Active Directory에 연결하려면 먼저 다음과 같은 사전 조건을 완료해야 합니다.

- 도메인, 활성 디렉터리 및 디렉터리 그룹을 구성할 수 있는 올바른 AWS Identity and Access Management 권한이 있는지 확인하십시오. 자세한 정보는 Amazon Chime용 Identity and Access Management을 참조하세요.
- 미국 동부 (버지니아 북부) 지역에 구성된 디렉터리를 생성하십시오. AWS Directory Service 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요. Amazon Chime은 AD Connector, Microsoft AD 또는 Simple AD를 사용하여 연결할 수 있습니다.

- Amazon Chime 엔터프라이즈 계정을 생성하거나 기존 팀 계정을 엔터프라이즈 계정으로 변환하려면 도메인을 신청하세요. 사용자가 두 개 이상의 도메인에서 업무용 이메일 주소를 보유하고 있는 경우, 이러한 도메인을 모두 요청해야 합니다. 자세한 내용은 도메인 신청 및 팀 계정을 엔터프라이즈 계정으로 변환 섹션을 참조하세요.

Amazon Chime의 Active Directory에 연결

관리자가 Active Directory를 Amazon Chime에 연결한 후 Amazon Chime 엔터프라이즈 계정에서 요청한 도메인 중 하나의 이메일 주소를 사용할 경우, 디렉터리 자격 증명을 사용하여 로그인하라는 메시지가 사용자에게 표시됩니다.

Amazon Chime의 Active Directory에 연결하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 자격 증명에 Active Directory를 선택합니다.
3. 클라우드 디렉터리 ID의 경우 Amazon Chime에 사용할 AWS Directory Service 디렉터리를 선택한 다음 Connect를 선택합니다.

   > **Note**
   >
   > AWS Directory Service 콘솔을 사용하여 디렉터리 ID를 찾을 수 있습니다.

4. 디렉터리가 연결되면 새 그룹 추가를 선택합니다.
5. 그룹에 그룹 이름을 입력합니다. 이름이 대상 디렉터리의 Active Directory 그룹과 정확히 일치해야 합니다. Active Directory Organization Units(OU)는 지원되지 않습니다.
6. 권한 계층에서 기본 또는 프로를 선택합니다.
7. 그룹 추가를 선택합니다.
8. (선택 사항) 이 절차를 반복하여 추가 디렉터리 그룹을 생성합니다.

여러 이메일 주소 구성

관리자가 Amazon Chime의 Active Directory에 연결하면 사용자가 Active Directory 자격 증명을 사용하여 Amazon Chime에 로그인할 수 있습니다. 사용자는 Active Directory 내에서 할당된 여러 이메일 주소를 보유할 수 있습니다. 사용자가 Active Directory 자격 증명을 사용하여 Amazon Chime에 로그인할 수 있도록 하려면 Amazon Chime 관리 계정에서 각각의 해당되는 이메일 도메인을 요청해야 합니다. 자세한 정보는 도메인 신청을 참조하세요.

> **Note**
>
> 사용자가 요청하지 않은 도메인의 이메일 주소를 사용하여 로그인하려고 하면 Amazon으로 로그인을 사용하여 로그인하라는 메시지가 표시됩니다. 요청하지 않은 도메인의 이메일 주소를 사용할 경우 사용자는 관리 계정에 로그인할 수 없습니다.

Amazon Chime 콘솔에서 사용자 세부 정보를 볼 경우, Amazon Chime은 Active Directory의 `EmailAddress` 속성에 있는 단일 이메일 주소를 각 사용자의 기본 이메일 주소로 사용합니다. 이는 Amazon Chime 콘솔의 사용자에 대해 볼 수 있는 유일한 이메일 주소입니다. 그러나 Amazon Chime 계정에서 이러한 도메인을 요청하기만 하면 사용자는 `ProxyAddress` 속성에 나열된 추가 주소로 로그인할 수 있습니다.

잘못된 구성 예

사용자 이름 shirley.rodriguez는 example.com과 anotherdomain.com이라는 두 가지 도메인을 신청한 Amazon Chime 계정의 멤버입니다. Active Directory에서 이 사용자는 다음과 같은 세 개의 이메일 주소를 보유하고 있습니다.

- 기본 이메일 주소: shirley.rodriguez@example.com
- 프록시 이메일 주소 1: shirley.rodriguez@example2.com
- 프록시 이메일 주소 2: srodriguez@example.org

이 사용자는 shirley.rodriguez@example.com 또는 srodriguez@example.org 및 shirley.rodriguez를 사용하여 Amazon Chime에 로그인할 수 있습니다. 이 사용자가 shirley.rodriguez@example2.com을 사용하여 로그인하려고 하면 Amazon으로 로그인하라는 메시지가 표시되며, 관리형 계정에 속하지 않게 됩니다. 이와 같은 이유로 사용자의 모든 이메일 도메인을 요청하는 것이 중요합니다.

다른 Amazon Chime 사용자는 shirley.rodriguez@example.com 또는 srodriguez@example.org 이메일 주소를 사용하여 이 사용자를 연락처로 추가하거나, 회의에 초대하거나, 대리인으로 추가할 수 있습니다.

올바른 구성 예

사용자 이름 shirley.rodriguez는 example.com, example2.com, example.org라는 세 가지 도메인을 신청한 Amazon Chime 계정의 멤버입니다. Active Directory에서 이 사용자는 다음과 같은 세 개의 이메일 주소를 보유하고 있습니다.

- 기본 이메일 주소: shirley.rodriguez@example.com

- 프록시 이메일 주소 1: shirley.rodriguez@example2.com
- 프록시 이메일 주소 2: srodriguez@example.org

이 사용자는 자신의 업무용 이메일 주소를 사용하여 Amazon Chime에 로그인할 수 있습니다. 또한 다른 사용자는 이 사용자의 업무용 이메일 주소를 사용하여 이 사용자를 연락처로 추가하거나, 회의에 초대하거나, 대리인으로 추가할 수 있습니다.

Okta SSO에 연결

엔터프라이즈 계정이 있는 경우 Okta SSO에 연결하여 사용자 권한을 인증하고 할당할 수 있습니다.

> **Note**
>
> 지정된 이메일 주소 도메인 집합 내의 모든 사용자를 관리할 수 있는 엔터프라이즈 계정을 생성해야 하는 경우 도메인 신청 단원을 참조하십시오.

Amazon Chime을 Okta에 연결하려면 Okta 관리 콘솔의 애플리케이션 2개를 구성해야 합니다. 첫 번째 애플리케이션이 수동으로 구성되어 OpenID Connect를 통해 사용자를 Amazon Chime 서비스에 인증합니다. 두 번째 애플리케이션은 Okta Integration Network(OIN)에서 Amazon Chime SCIM 프로비저닝으로 사용할 수 있습니다. 사용자 및 그룹에 대한 변경과 관련하여 Amazon Chime에 대한 업데이트를 푸시하도록 구성됩니다.

Okta SSO에 연결하려면

1. Okta 관리 콘솔에서 Amazon Chime 애플리케이션(OpenID Connect)을 생성합니다.
    1. Okta Administration Dashboard에 로그인한 다음 Add Application(애플리케이션 추가)을 선택합니다. 새 애플리케이션 생성 대화 상자에서 웹, 다음을 선택합니다.
    2. 애플리케이션 설정 구성:
        a. 애플리케이션 **`Amazon Chime`**의 이름을 지정합니다.
        b. 로그인 리디렉션 URI에 **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`** 값을 입력합니다.
        c. 허용되는 권한 부여 유형 섹션에서 모든 옵션을 선택하여 활성화합니다.
        d. 로그인 시작 위치 드롭다운 메뉴에서 Okta 또는 앱을 선택하고 관련된 모든 옵션을 선택합니다.

e. 로그인 URI 시작에 **`https://signin.id.ue1.app.chime.aws/auth/okta`** 값을 입력합니다.

f. 저장을 선택합니다.

g. 2단계의 경우 클라이언트 ID, 클라이언트 암호 및 발행자 URI 정보가 필요하므로 이 페이지를 열어 둡니다.

2. Amazon Chime 콘솔에서 다음 단계를 따릅니다.

1. Okta SSO 구성 페이지의 상단에서 수신 키 설정을 선택합니다.
2. 수신 Okta 키 설정 대화 상자에서 다음을 수행합니다.

a. Okta 애플리케이션 설정 페이지에서 클라이언트 ID 및 클라이언트 암호 정보를 붙여 넣습니다.

b. Okta API 페이지에서 적절한 발행자 URI를 붙여 넣습니다. 발행자 URI는 `https://example.okta.com` 같은 Okta 도메인이어야 합니다.

3. Okta 관리 콘솔에서 Amazon Chime SCIM 프로비저닝 애플리케이션을 설정하여 Amazon Chime과 일부 자격 증명 및 그룹 멤버십 정보를 교환합니다.

1. Okta 관리 콘솔에서 애플리케이션, 애플리케이션 추가를 선택하고 Amazon Chime SCIM Provisioning을 검색한 다음 해당 애플리케이션을 추가합니다.

> **Important**
>
> 초기 설정에서 사용자에게 애플리케이션 표시 안 함 및 Okta Mobile 앱에 애플리케이션 아이콘 표시 안 함을 선택한 다음 완료를 선택합니다.

2. 프로비저닝 탭에서 API 통합 구성 및 API 통합 활성화를 선택합니다. 다음 단계를 위해 API 액세스 키를 복사해야 하므로 이 페이지를 열어 둡니다.
3. Amazon Chime 콘솔에서 액세스 키 생성을 선택하여 API 액세스 키를 생성합니다. API 통합 구성 대화 상자의 Okta API 토큰 필드에 해당 키를 복사하고 통합 테스트를 선택한 다음, 저장을 선택합니다.
4. Okta에서 Amazon Chime을 업데이트하는 데 사용할 작업 및 속성을 구성합니다. 프로비저닝 탭의 앱 대상 섹션에서 편집을 선택하고 사용자 활성화, 사용자 속성 업데이트 및 사용자 비활성화를 선택한 다음 저장을 선택합니다.
5. 할당 탭에서 새 SCIM 앱에 대한 권한을 사용자에게 부여합니다.

> **Important**
>
> 라이선스에 관계없이 Amazon Chime에 액세스해야 하는 모든 사용자가 포함된 그룹을 통해 권한을 부여하는 것이 좋습니다. 해당 그룹은 이전 1단계에서 사용자 대면 OIDC 애플리케이션을 할당하는 데 사용된 그룹과 동일해야 합니다. 그렇지 않으면 최종 사용자가 로그인할 수 없습니다.

6. 푸시 그룹 탭에서 Amazon Chime에 동기화할 그룹 및 멤버십을 구성합니다. 이 그룹은 기본 및 프로 사용자를 구별하는 데 사용됩니다.

4. Amazon Chime에 디렉터리 그룹 구성:

   1. Amazon Chime 콘솔에서 Okta Single Sign-On 구성 페이지로 이동합니다.
   2. 디렉터리 그룹에서 새 그룹 추가를 선택합니다.
   3. Amazon Chime에 추가할 디렉터리 그룹의 이름을 입력합니다. 이름은 이전 3-f 단계에서 구성된 푸시 그룹 중 하나와 정확히 일치해야 합니다.
   4. 이 그룹의 사용자가 기본 또는 프로 기능을 수신해야 하는지 선택하고 저장을 선택합니다. 이 프로세스를 반복하여 추가 그룹을 구성합니다.

> **Note**
>
> 그룹을 찾을 수 없다는 오류 메시지가 표시되는 경우 두 시스템이 동기화를 완료하지 않은 것일 수 있습니다. 몇 분 기다린 후 새 그룹 추가를 다시 선택합니다.

디렉터리 그룹의 사용자에 대해 기본 또는 프로 기능을 선택하면 Amazon Chime 엔터프라이즈 계정에서 해당 사용자의 라이선스, 기능 및 비용에 영향을 줍니다. 자세한 내용은 요금을 참조하십시오.

Outlook용 Amazon Chime 추가 기능 배포

Amazon Chime은 두 가지 Microsoft Outlook용 추가 기능, 즉 Windows용 Outlook용 Amazon Chime 추가 기능과 Outlook용 Amazon Chime 추가 기능을 제공합니다. 이러한 추가 기능은 동일한 예약 기능을 제공하지만, 다른 유형의 사용자를 지원합니다. Microsoft Office 365 구독자와 온프레미스 Microsoft Exchange 2013 이상을 사용하는 조직은 Outlook용 Amazon Chime 추가 기능을 사용할 수 있습니다. 온프레미스 Exchange 서버에서 Exchange Server 2010 이하를 실행하는 Windows 사용자와 Outlook 2010 사용자는 Windows에서 Outlook용 Amazon Chime 추가 기능을 사용해야 합니다.

Outlook용 Amazon Chime 추가 기능을 설치할 권한이 없는 Windows 사용자는 Windows에서 Outlook용 Amazon Chime 추가 기능을 선택해야 합니다.

어떤 추가 기능이 자신과 조직에 적합한지에 대한 자세한 내용은 적합한 Outlook 추가 기능 선택을 참조하십시오.

조직에서 Outlook용 Amazon Chime 추가 기능을 선택할 경우 중앙 집중식 배포를 통해 이 기능을 사용자에게 배포할 수 있습니다. 자세한 내용은 관리자를 위한 Outlook Amazon Chime 애드인 설치 설명서를 참조하세요.

Amazon Chime Meetings App for Slack 설정

Slack Enterprise Grid 조직을 사용 중이고 Slack 조직을 소유하고 있거나 관리하고 있는 경우, 조직에 맞게 Amazon Chime Meetings App for Slack을 설정할 수 있습니다. Slack 워크스페이스 관리자인 경우 워크스페이스에 대해 Amazon Chime Meetings App for Slack을 설정할 수 있습니다.

다음 섹션의 단계에서는 두 가지 유형의 설정을 모두 수행하는 방법, 그리고 추가 작업을 완료하는 방법(예: 워크스페이스를 조직으로 마이그레이션하는 방법)을 설명합니다.

주제

- 조직에서 Amazon Chime Meetings App for Slack 설치
- 워크스페이스에서 Amazon Chime Meetings App for Slack 설치
- 워크스페이스를 조직으로 마이그레이션
- 워크스페이스를 Amazon Chime 팀 계정과 연결

조직에서 Amazon Chime Meetings App for Slack 설치

Slack 조직에 Amazon Chime Meetings App for Slack을 설치하면 사용자가 조직의 다양한 워크스페이스에서 다른 사용자와 즉각적인 회의 및 통화를 시작할 수 있습니다. 또한 워크스페이스 관리자는 모든 새 워크스페이스에 Slack 회의 애플리케이션을 위한 Amazon Chime 회의 앱을 자동으로 설치할 수 있습니다. 다음 단계에서는 방법에 대해 설명합니다.

> **Note**
>
> 다음 단계에서는 사용자가 조직 소유자 또는 관리자이고 Slack 관리 콘솔에 로그인할 수 있다고 가정합니다.

조직에서 Amazon Chime Meetings App for Slack을 설치하려면

1. Slack 관리 콘솔의 왼쪽 창에서 앱을 선택합니다.

   앱 페이지가 나타나며 조직에 설치된 앱이 있는 경우 해당 앱이 나열됩니다.
2. 페이지 오른쪽 위 모서리에 있는 앱 관리를 선택한 다음, 앱 설치를 선택합니다.

   설치할 앱 찾기 대화 상자가 나타납니다.
3. **`Amazon Chime Meetings`**를 검색한 다음, 검색 결과에서 해당 항목을 선택합니다.

   Amazon Chime Meetings를 워크스페이스에 추가 대화 상자가 나타나고 조직 내의 워크스페이스가 나열됩니다.
4. Amazon Chime Meetings App for Slack을 설치할 워크스페이스를 선택합니다.
5. (선택 사항) 모든 새 워크스페이스에 Amazon Chime Meetings App for Slack을 자동으로 설치하려면 향후 워크스페이스의 기본값을 선택하고 다음을 선택합니다.

   이 앱에 요청된 권한 검토 대화 상자가 나타나고 Amazon Chime Meetings App for Slack에 대한 권한 및 작업이 표시됩니다.
6. 다음을 선택합니다.
7. Amazon Chime Meetings App for Slack을 기본적으로 새 워크스페이스에 설치하도록 선택한 경우, 이 앱을 향후 워크스페이스의 기본값으로 설정할 준비 완료를 선택한 다음, 저장을 선택합니다. 그렇지 않은 경우 저장만 선택합니다.

> **Note**
>
> OAuth를 사용하여 조직에 앱을 설치할 수도 있습니다. 자세한 내용은 Slack 도움말의 OAuth와 설치를 참조하세요.

워크스페이스에서 Amazon Chime Meetings App for Slack 설치

워크스페이스에 Amazon Chime Meetings App for Slack을 설치하면 사용자가 조직의 해당 워크스페이스에서 다른 사용자와 즉각적인 회의 및 통화를 시작할 수 있습니다. 사용자는 Amazon Chime 사용자 프로필이 없어도 Amazon Chime Meetings App for Slack을 사용할 수 있습니다. 사용자는 Slack 사용자 프로필로 로그인하여 언제든지 통화나 회의를 시작할 수 있습니다. 사용자가 두 명 이상의 다른 사람과 회의를 진행해야 할 경우, Amazon Chime 팀 계정을 설정하고 추가 사용자에게 프로 권한을 부여해야 합니다. Amazon Chime 통화 및 회의 시작에 대한 자세한 내용은 Amazon Chime 사용 설명

서의 Amazon Chime Meetings App for Slack 사용을 참조하세요. Amazon Chime 팀 계정 설정에 대한 자세한 내용은 이 안내서의 워크스페이스를 Amazon Chime 팀 계정과 연결 섹션을 참조하세요.

Slack 워크스페이스에 Amazon Chime Meetings App for Slack을 설치하려면

1. Slack App Directory로 이동하여 Amazon Chime Meetings App을 찾습니다.
2. Slack에 추가를 선택하여 Slack App Directory에서 Amazon Chime Meetings App for Slack을 설치합니다.
3. Slack 워크스페이스 통화 설정을 Amazon Chime을 사용하여 Slack에서 통화 활성화로 구성합니다.

워크스페이스를 조직으로 마이그레이션

Slack 조직을 소유한 경우 워크스페이스를 해당 조직으로 마이그레이션할 수 있습니다. 워크스페이스 마이그레이션에 대한 자세한 내용은 Slack 도움말의 워크스페이스를 Enterprise Grid로 이전을 참조하세요.

워크스페이스를 Amazon Chime 팀 계정과 연결

워크스페이스를 Amazon Chime 팀 계정과 연결하여 사용자의 권한을 관리합니다. 회의 주최자를 Amazon Chime 프로로 업그레이드하면 최대 250명의 참석자와 25개의 비디오 타일로 회의를 시작하고 오디오용으로 전화를 걸기 위한 전화번호를 포함할 수 있습니다. 사용자에게 Amazon Chime 기본 권한을 할당하여 one-on-one 회의를 시작하거나 Amazon Chime 회의에 참여할 수 있도록 하십시오. 자세한 내용은 Amazon Chime 요금을 참조하세요.

> **Note**
>
> Amazon Chime 팀 계정을 Slack 워크스페이스와 연결하면 사용자가 Amazon Chime Meetings App for Slack에서 Amazon Chime에 로그인할 수 있습니다. 이 설정은 언제든지 변경할 수 있습니다. 자세한 정보는 회의 설정 관리을 참조하세요.

Slack 워크스페이스를 Amazon Chime Team 계정과 연결하려면 먼저 계정을 AWS 생성해야 합니다. AWS 계정 생성 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Chime 시스템 관리자를 위한 사전 조건

Amazon Chime Meetings App for Slack 설치 시 Amazon Chime 팀 계정을 Slack 워크스페이스와 연결하려면

1. Slack 워크스페이스에 Amazon Chime Meetings App for Slack을 설치한 직후 지금 업그레이드를 선택합니다.
2. 안내에 따라 계정 자격 증명을 사용하여 Amazon Chime 콘솔에 AWS 로그인합니다.
3. 프롬프트 메시지에 따라 Amazon Chime에서 새로운 팀 계정을 생성하거나 기존 팀 계정을 선택합니다.

    - 새 계정 생성 - Slack 사용자를 초대할 새 Amazon Chime 계정을 생성합니다. 계정 이름을 입력하고 Slack 사용자를 초대할지 여부를 선택한 다음 생성을 선택합니다.
    - 기존 계정 선택 - Slack 사용자를 초대할 기존 Amazon Chime 계정을 선택합니다. 계정을 선택한 다음 초대를 선택합니다.

Amazon Chime에 참여하도록 Slack 사용자를 초대하면 초대하는 이메일이 사용자에게 발송됩니다. 사용자가 초대를 수락하면 자동으로 Amazon Chime 프로로 업그레이드됩니다.

Amazon Chime Meetings App for Slack을 설치할 때 Slack 워크스페이스를 Amazon Chime 팀 계정과 연결하지 않은 경우 다음 단계를 사용하여 해당 작업을 수행할 수 있습니다.

Amazon Chime Meetings App for Slack 설치 후 Amazon Chime 팀 계정을 Slack 워크스페이스와 연결하려면

1. 계정에 로그인합니다. AWS
2. Slack 작업 영역에 관리자로 로그인합니다.
3. https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz로 이동합니다.
4. 프롬프트 메시지에 따라 Amazon Chime에서 새로운 팀 계정을 생성하거나 기존 팀 계정을 선택합니다.

    - 새 계정 생성 - Slack 사용자를 초대할 새 Amazon Chime 계정을 생성합니다. 계정 이름을 입력하고 Slack 사용자를 초대할지 여부를 선택한 다음 생성을 선택합니다.
    - 기존 계정 선택 - Slack 사용자를 초대할 기존 Amazon Chime 계정을 선택합니다. 계정을 선택한 다음 초대를 선택합니다.

사용자 관리

> **Note**
>
> 이 섹션의 단계에서는 일련의 사용자 전자 메일 주소가 있거나 관리자 계정을 Active Directory에 연결했다고 가정합니다. 자세한 내용은 이 가이드의 Active Directory에 연결 을 참조하십시오.

Amazon Chime 콘솔을 사용하여 사용자를 추가하고 관리할 수 있습니다. 사용자를 초대하여 사용자를 추가합니다. 사용자가 초대를 수락하면 사용자 아래에 해당 사용자가 표시되는데, 여기에는 계정의 모든 사용자 및 사용자 세부 정보가 나열됩니다. 자세한 정보는 사용자 세부 정보 보기을 참조하세요.

Amazon으로 로그인(LWA)을 사용하는 계정 관리자에게는 권한 계층을 관리하고 계정에서 사용자를 제거하는 옵션도 표시됩니다. 이러한 작업은 구성한 계정 중 어떤 계정을 사용하는지에 따라 Active Directory 또는 Okta를 통해 관리됩니다. 자세한 내용은 사용자 권한 및 액세스 관리 단원을 참조하십시오.

목차

사용자 추가

Amazon Chime 계정에 가입하도록 초대하여 사용자를 Amazon Chime 계정에 추가할 수 있습니다. Amazon Chime 콘솔에서 사용자 후보에게 초대를 전송하면 되며, 아래의 단계에 방법이 설명되어 있습니다.

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.

관리하는 계정 목록이 나타납니다.

2. 멤버를 추가할 계정을 선택한 다음, 사용자 초대를 선택합니다.

   새 사용자 초대 대화 상자가 나타납니다.

3. 초대할 사용자의 이메일 주소를 입력합니다. 각 주소는 세미콜론(;)으로 구분합니다.
4. [사용자 초대]를 선택합니다.

새 사용자가 목록에 나타납니다. 팀 계정에 사용자를 초대한 경우, 해당 사용자가 초대를 수락하기 전까지는 해당 사용자의 세부 정보가 표시되지 않습니다.

사용자 세부 정보 보기

Amazon Chime 콘솔의 사용자에서 계정의 모든 사용자 목록 및 사용자 세부 정보를 볼 수 있습니다. 이메일 주소로 특정 사용자를 검색하고 이름을 선택하면 사용자 세부 정보가 표시됩니다. 사용자 세부 정보에서 사용자에 대한 세부 정보를 보고, 사용자 계정을 업데이트할 수 있습니다.

아래 표에는 콘솔에 표시되는 사용자 세부 정보가 나열되어 있습니다.

> **Note**
>
> 팀 계정 사용자의 경우 초대를 수락하기 전까지는 전체 사용자 세부 정보가 표시되지 않습니다.

필드	설명	예
표시 이름	Amazon Chime에 표시되는 사용자 이름입니다. Amazon으로 로그인(LWA) 사용자의 경우 이 이름이 전체 이름입니다. Active Directory 사용자의 경우 DISPLAY_NAME_ATTRIBUTE가 사용됩니다.	Major, Mary
이메일 주소	LWA 사용자의 경우 등록에 사용된 이메일 주소입니다.	mary.major@example.com

필드	설명	예
	Active Directory 사용자의 경우에는 Active Directory의 기본 이메일 주소가 표시됩니다.	
등록	사용자의 현재 등록 상태입니다. 상태 값은 엔터프라이즈 계정(초대가 발송되지 않은 경우)과 팀 계정(초대가 발송된 경우) 간에 다릅니다.	등록, 미등록(팀 계정), 일시 중지됨(엔터프라이즈 계정)
권한 계층	기본적으로 프로로 설정되며, 사용자가 회의를 주최할 수 있습니다. 기본으로 변경할 수 있습니다.	프로, 기본
초대됨	팀 계정의 경우 사용자가 계정에 초대된 날짜입니다.	2020년 1월 5일
조인함	사용자가 Amazon Chime에 처음 로그인한 날짜입니다. 프로 평가판 사용자의 경우 프로 평가판을 시작한 날짜이기도 합니다.	2020년 1월 10일
개인 PIN	사용자가 회의를 예약하는 데 사용할 수 있는 개인 회의 PIN입니다.	0123456789
공개 설정	사용자가 선택한 참석 설정입니다.	공개 또는 비공개
참석한 회의	사용자가 참석한 회의 수입니다.	87
구성한 회의	사용자가 구성한 회의 수입니다.	12

필드	설명	예
회의 만족도	설문조사에 대한 긍정적인 응답의 비율. end-of-meeting	92%
마지막 활동 날짜	사용자가 마지막으로 활동한 날짜입니다.	2020년 6월 12일
전송한 채팅 메시지	사용자가 전송한 채팅 메시지 수입니다.	1025
전화번호	있는 경우 사용자에게 할당된 전화번호입니다.	+12065550100

사용자 권한 및 액세스 관리

Amazon Chime 사용자에게 프로 또는 기본 권한을 할당하여 액세스할 수 있는 기능을 관리합니다. 기본 사용자는 회의를 주최할 수 없지만, 회의에 참여하고 채팅을 사용할 수는 있습니다. 프로 및 기본 권한이 부여된 사용자가 액세스할 수 있는 기능에 대한 자세한 내용은 플랜 및 요금 단원을 참조하세요.

사용자를 초대하거나 일시 중지하여 Amazon Chime 관리자 계정에 로그인할 수 있는 사용자를 관리합니다. 엔터프라이즈 계정 관리자만 사용자를 일시 중지할 수 있습니다. 팀 계정 관리자는 해당 계정에서 사용자를 제거하여 더 이상 사용자 권한에 대한 요금을 지불하지 않도록 할 수 있습니다. 하지만 사용자를 일시 중지시키고 로그인하지 못하게 할 수는 없습니다. 팀 계정과 엔터프라이즈 계정의 차이점에 대한 자세한 내용은 Amazon Chime 계정 관리 섹션을 참조하세요.

사용자 권한 관리

Amazon Chime 관리자는 Amazon Chime 계정의 사용자에 대한 프로 및 기본 권한을 관리할 수 있습니다.

Amazon Chime 계정에 Active Directory 또는 Okta를 구성한 경우, 그룹 멤버십을 통해 사용자 권한을 관리합니다. Active Directory 또는 Okta를 구성하지 않은 경우에는 Amazon Chime 콘솔에서 사용자 권한을 관리합니다.

팀 계정 및 엔터프라이즈 Amazon으로 로그인

사용자가 Amazon으로 로그인(LWA) 계정으로 로그인하는 Amazon Chime 팀 계정 또는 엔터프라이즈 LWA 계정을 관리하는 경우, Amazon Chime 콘솔에서 프로 및 기본 권한을 관리할 수 있습니다.

팀 계정 및 엔터프라이즈 LWA의 사용자 권한을 관리하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 Amazon Chime 계정 이름을 선택합니다.
3. 사용자를 선택하세요.
4. 사용자를 선택하고 작업, 권한 할당을 선택합니다.
5. 권한에서 다음 옵션 중 하나를 선택합니다.
   - 프로
   - 기본
6. 할당을 선택합니다.

엔터프라이즈 Active Directory 또는 엔터프라이즈 OpenID Connect(Okta) 계정

사용자가 Active Directory 또는 Okta 자격 증명으로 로그인할 경우, 해당 사용자를 프로 또는 기본 권한이 할당된 디렉터리 그룹의 멤버로 설정하여 권한을 관리합니다.

사용자에게 프로 권한을 할당하려면 해당 사용자를 프로 권한이 할당된 Active Directory 또는 Okta 그룹의 멤버로 설정합니다. 사용자에게 프로 권한을 할당하려면 해당 사용자를 기본 권한이 할당된 그룹의 멤버로 설정합니다. 프로 또는 기본 권한이 없는 사용자는 Amazon Chime에 로그인할 수 없습니다.

사용자 액세스 관리

Amazon Chime 계정을 관리할 경우 사용자를 초대하여 계정에 로그인하도록 허용할 수 있습니다. 엔터프라이즈 계정 관리자는 사용자 액세스를 일시 중지하여 계정에 로그인하지 못하도록 할 수 있습니다.

팀 계정 사용자 초대 및 삭제

팀 계정을 관리할 경우, Amazon Chime 콘솔을 사용하여 이메일 도메인의 사용자를 초대할 수 있습니다.

> **Note**
>
> 사용자의 30일 프로 체험판은 초대를 수락하면 종료됩니다.

사용자를 팀 계정에 초대하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 팀 계정 이름을 선택합니다.
3. 사용자, 사용자 초대를 선택합니다.
4. 초대할 사용자의 이메일 주소를 입력하고, 여러 이메일 주소를 세미콜론(**;**)으로 구분합니다.
5. [사용자 초대]를 선택합니다.

아래의 절차는 사용자에게 할당된 프로 또는 기본 권한을 제거하여 팀 계정에서 사용자의 연결을 해제합니다. 제거된 사용자는 Amazon Chime에 계속 로그인할 수 있지만, 더 이상 Amazon Chime 계정의 유료 멤버가 아닙니다.

팀 계정에서 사용자를 제거하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 팀 계정 이름을 선택합니다.
3. 사용자를 선택하세요.
4. 제거할 사용자를 선택하고 작업, 사용자 제거를 선택합니다.

사용자에게 할당된 모든 프로 또는 기본 권한은 제거됩니다. 이 사용자는 연락처에서 자동 완성 기능을 사용하여 새 팀 사용자를 검색할 수 없습니다.

엔터프라이즈 계정 사용자 초대 및 일시 중지

엔터프라이즈 계정을 관리할 경우, 요청한 도메인의 이메일 주소로 Amazon Chime에 등록한 사용자가 계정에 자동으로 추가됩니다. Active Directory 또는 Okta를 구성한 경우 사용자는 Amazon Chime용으로 구성한 디렉터리 그룹의 멤버여야 합니다.

엔터프라이즈 계정에 사용자를 초대하려면

- 조직의 사용자에게 초대 이메일을 전송하고 Amazon Chime 사용 설명서의 Amazon Chime 계정 생성에 나와 있는 단계를 따르도록 안내합니다.

사용자들은 여러분이 계정에 대해 요청한 도메인 중 하나의 이메일 주소로 로그인합니다. 사용자가 자신의 Amazon Chime 사용자 계정을 만드는 단계를 완료하면, Amazon Chime 콘솔에서 엔터프라이즈 계정의 사용자에 해당 계정이 자동으로 나타납니다.

아래의 절차를 수행하면 Active Directory 또는 Okta가 구성되지 않은 엔터프라이즈 계정의 사용자가 일시 중지됩니다. 이 경우 사용자가 Amazon Chime에 로그인할 수 없습니다.

엔터프라이즈 계정에서 사용자를 정지시키려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에서 엔터프라이즈 계정 이름을 선택합니다.
3. 사용자를 선택하세요.
4. 일시 중지할 사용자를 선택하고 작업, 사용자 일시 중지를 선택합니다.
5. 확인란을 선택하고 일시 중지를 선택합니다.

Active Directory 또는 Okta가 구성되지 않은 엔터프라이즈 계정의 사용자가 있는 경우, 아래의 절차를 사용하여 사용자를 일시 중지합니다.

엔터프라이즈 Active Directory 또는 OpenID Connect(Okta) 계정에서 사용자를 정지시키려면

- 다음 중 하나를 수행하십시오.
  - Active Directory 또는 Okta 관리자 대시보드에서 사용자를 일시 중지하거나 비활성으로 표시합니다.
  - 기본 또는 프로 권한이 할당된 Active Directory 그룹에서 해당 사용자를 제거합니다.

개인 회의 PIN 변경

개인 회의 PIN은 사용자가 등록할 때 생성되는 고정 ID입니다. PIN을 통해 Amazon Chime 사용자는 다른 Amazon Chime 사용자와의 회의 일정을 손쉽게 예약할 수 있습니다. 개인 회의 PIN을 사용하면 회의 구성자가 새로운 회의를 예약할 때 각 회의의 세부 정보를 기억할 필요가 없습니다.

사용자가 자신의 개인 회의 PIN이 공개되었다고 생각할 경우, 사용자의 PIN을 재설정하고 새로운 ID를 생성할 수 있습니다. 개인 회의 PIN을 업데이트한 후에 해당 사용자가 기존의 개인 회의 PIN을 사용하여 예약한 모든 회의를 업데이트해야 합니다.

개인 회의 PIN을 변경하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 Amazon Chime 계정의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택합니다.

4. PIN을 변경해야 하는 사용자를 검색합니다.
5. 사용자 세부 정보 페이지를 열려면 사용자의 이름을 선택합니다.
6. 사용자 작업, 개인 PIN 재설정, 확인을 선택합니다.

프로 평가판 관리

사용자가 Amazon Chime 팀 초대를 수락하거나, 엔터프라이즈 계정에 추가되면 사용자의 무료 평가판이 종료되고 프로 권한을 갖게 됩니다. 이를 통해 예약된 회의를 계속 주최할 수 있습니다. 사용자의 권한 계층을 기본으로 변경하면 회의 주최자 역할을 할 수 없습니다.

Amazon Chime 사용량 기반 요금을 사용하면 사용자가 회의를 주최한 날에 회의를 주최한 사용자에 대해서만 요금을 지불합니다. 회의 참석자와 채팅 사용자에게는 요금이 청구되지 않습니다.

프로 사용자가 당일에 끝나는 회의를 주최했고 다음 중 한 개 이상이 해당되는 경우 프로 사용자는 활동 중인 프로 사용자로 간주됩니다.

- 회의가 예약됨
- 회의에 세 명 이상의 사용자가 포함됨
- 회의에 한 개 이상의 레코딩 이벤트가 있음
- 회의에 전화 접속 참석자가 포함됨
- 회의에 H.323 또는 SIP를 통해 합류한 참석자가 포함됨

자세한 내용은 플랜 및 요금을 참조하십시오.

사용자 첨부 파일 요청

엔터프라이즈 계정을 관리하고 적절한 권한을 가지고 있는 경우 사용자는 자신이 Amazon Chime에 업로드한 첨부 파일을 요청하고 받을 수 있습니다. 사용자가 1:1 및 그룹 대화 또는 자신들이 만든 채팅룸에 업로드한 첨부 파일을 가져올 수 있습니다.

> **Note**
>
> Amazon Chime 팀 계정을 관리하는 경우 하나 이상의 도메인을 요청하여 엔터프라이즈 계정으로 업그레이드할 수 있습니다. 또는 팀 계정에서 사용자를 제거하면 관리되지 않는 사용자가 Amazon Chime 도우미를 사용하여 첨부 파일을 가져올 수 있습니다.

사용자 첨부 파일을 요청하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정 페이지에서 Amazon Chime 계정의 이름을 선택합니다.
3. 설정에서 계정, 계정 작업, 첨부 파일 요청을 선택합니다.
4. 대략 24시간 내에 계정 요약 페이지는 각 첨부 파일에 액세스하는 데 사용하는 미리 서명된 URL 목록이 포함된 파일에 대한 링크를 제공합니다.
5. 파일을 다운로드합니다.

> **Note**
>
> 파일에 대해 적절한 수준의 액세스 제어를 유지해야 합니다. 파일을 받은 사용자는 누구든지 제공된 URL 목록을 사용하여 관련 첨부 파일을 다운로드할 수 있습니다.
> 미리 서명된 URL은 6일 후에 만료됩니다. 7일마다 한 번 요청을 제출할 수 있습니다.

AWS Identity and Access Management (IAM) 정책을 사용하여 Amazon Chime 관리 콘솔 및 첨부 파일 요청 작업에 대한 액세스를 관리하려면 Amazon Chime 관리형 정책 FullAccess (UserManagement, 또는) 중 하나를 사용하십시오. ReadOnly 또는 `StartDataExport` 작업 및 `RetrieveDataExport` 작업을 포함하도록 사용자 지정 정책을 업데이트할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 Amazon Chime에서 정의한 작업을 참조하세요.

Amazon Chime에서 자동 업데이트를 관리하는 방법

Amazon Chime은 클라이언트를 업데이트하는 다양한 방법을 제공합니다. Amazon Chime을 브라우저에서 실행하는지, 데스크톱에서 실행하는지, 모바일 장치에서 실행하는지에 따라 방법이 달라집니다.

Amazon Chime 웹 애플리케이션(https://app.chime.aws)은 항상 최신 기능 및 보안 수정 사항과 함께 로드됩니다.

Amazon Chime 데스크톱 클라이언트는 사용자가 종료 또는 로그아웃을 선택할 때마다 업데이트가 있는지 확인합니다. 이는 Windows 및 macOS 시스템에 적용됩니다. 클라이언트를 실행하면 3시간마다 업데이트가 있는지 확인합니다. Windows 도움말 메뉴 또는 macOS Amazon Chime 메뉴에서 업데이트 확인을 선택하여 업데이트가 있는지 확인할 수도 있습니다.

데스크톱 클라이언트가 업데이트를 감지하면 Amazon Chime에서는 사용자에게 업데이트를 설치하라는 메시지를 표시합니다. 단, 회의가 진행 중인 경우는 예외입니다. 회의가 진행 중인 경우는 다음과 같습니다.

- 회의에 참석 중인 경우.
- 아직 진행 중인 회의에 초대된 경우.

Amazon Chime에 최신 버전을 설치하라는 메시지가 표시되며, 설치를 연기할 수 있도록 15초 카운트다운이 제공됩니다. 사용자는 나중에 다시 시도를 선택하여 업데이트를 연기할 수 있습니다.

사용자가 업데이트를 연기했고 진행 중인 회의에 참석하고 있지 않은 경우, 클라이언트에서는 3시간 후에 업데이트를 확인하고 설치하라는 메시지를 다시 표시합니다. 카운트다운이 끝나면 설치가 시작됩니다.

> **Note**
>
> macOS 시스템에서는 사용자가 지금 다시 시작을 선택하여 업데이트를 시작해야 합니다.

모바일 디바이스에서 - Amazon Chime 모바일 애플리케이션은 App Store 및 Google Play에서 제공하는 업데이트 옵션을 사용하여 Amazon Chime 클라이언트의 최신 버전을 제공합니다. 또한 모바일 디바이스 관리 시스템을 사용하여 업데이트를 배포할 수 있습니다.

사용자를 다른 팀 계정으로 마이그레이션하기

대상 계정이 아직 없는 경우 대상 계정을 생성하고 구성하여 사용자를 다른 팀 계정으로 마이그레이션합니다. 그런 다음, 대상 계정에 사용자를 추가합니다. 다음 단계를 통해 마이그레이션의 각 부분을 완료하는 방법에 대한 정보를 확인할 수 있습니다.

사용자를 마이그레이션하려면

1. 대상 팀 계정이 아직 없다면 계정을 생성합니다. 자세한 정보는 1단계: Amazon Chime 관리자 계정 생성을 참조하세요.
2. 필요한 경우, 계정을 구성합니다. 자세한 정보는 2단계(선택 사항): 계정 설정 구성을 참조하세요.
3. 계정에 사용자를 추가합니다. 자세한 내용은 3단계: 계정에 사용자 추가을(를) 참조하세요.

Amazon Chime에서 전화번호 관리

Amazon Chime 콘솔을 사용하여 전화번호를 프로비저닝합니다. 번호를 프로비저닝할 때는 Amazon Chime에서 관리하는 번호 풀에서 번호를 요청합니다. 번호 할당을 해제한 다음 삭제하면 번호가 풀로 돌아갑니다. 번호를 포팅할 때는 Amazon Chime에서 번호를 주고 받게 됩니다.

> **Note**
>
> Amazon Chime 콘솔을 사용하는 경우 Amazon Chime 비즈니스 전화 번호만 프로비저닝할 수 있습니다. 국제 번호가 필요한 경우 Amazon Chime 음성 커넥터 및 SIP 미디어 애플리케이션을 사용합니다. 이를 위해서는 먼저 Amazon Chime SDK 관리 계정을 생성해야 합니다. 자세한 내용은 Amazon Chime SDK 관리자 안내서의 다음 주제를 참조하십시오.
>
> - 사전 조건
> - 전화번호 인벤토리 관리
> - 음성 커넥터 관리
> - SIP 미디어 애플리케이션 관리

다음 섹션의 항목에서는 Amazon Chime 전화번호를 제공하고 관리하는 방법을 설명합니다.

내용

전화번호 프로비저닝

Amazon Chime 콘솔을 사용하여 Amazon Chime 계정에 전화번호를 프로비저닝합니다. 이 번호는 Amazon Chime에서 관리하는 풀에서 가져온 것입니다. Amazon Chime Business Calling을 선택하여 전화번호를 프로비저닝하고 기존 Amazon Chime 사용자에게 전화번호를 할당할 수 있습니다.

프로비저닝이 완료되면 전화번호가 인벤토리에 표시됩니다. 그런 다음, 개별 사용자에게 전화번호를 할당합니다.

전화번호를 프로비저닝하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 주문, 전화번호 프로비저닝을 선택합니다.
4. 비즈니스 통화를 선택한 후 다음을 선택합니다.
5. 사용 가능한 전화번호를 검색합니다. 원하는 전화번호를 선택한 다음 프로비저닝을 선택합니다.

프로비저닝이 진행되는 동안 주문 및 대기 중 목록에 전화번호가 표시됩니다.

기존 전화번호 포팅

전화번호를 프로비저닝하는 것 외에도 전화 사업자의 번호를 인벤토리로 포팅할 수 있습니다. 여기에는 무료 전화번호도 포함됩니다.

> **Note**
>
> 국제 번호를 포팅하거나, Amazon Chime 음성 커넥터를 사용하거나, SIP 미디어 애플리케이션을 사용해야 하는 경우, Amazon Chime SDK 관리자 계정을 생성하고 Amazon Chime SDK 콘솔을 사용해야 합니다. 이에 대한 자세한 내용은 Amazon Chime SDK 관리자 안내서의 사전 요구 사항을 참조하십시오.

다음 섹션에서는 전화번호를 포팅하는 방법을 설명합니다.

주제

번호 포팅을 위한 사전 요구 사항

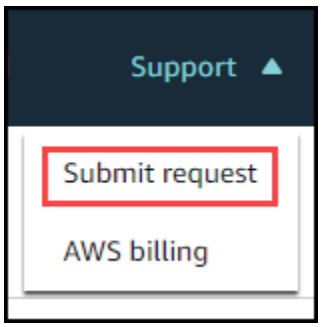
포트 번호를 입력하려면 에이전시 레터 (LOA) 가 있어야 합니다. 국내 전화번호에 대한 LOA가 있어야 합니다. 에이전시 레터 (LOA) 양식을 다운로드하여 작성하십시오. 다른 이동 통신사의 전화번호를 입력해야 하는 경우 각 이동 통신사에 대해 별도의 LOA를 작성하십시오.

전화번호 포팅:

기존 전화번호를 포팅하기 위한 지원 요청을 생성합니다.

기존 전화 번호를 포팅하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 페이지 상단의 명령 모음에서 Support를 선택한 다음 요청 제출을 선택합니다.



그러면 AWS Support 콘솔로 이동합니다.

> **Note**
>
> AWS Support 센터 페이지로 바로 이동할 수도 있습니다. 그럴 경우 사례 만들기를 선택한 다음 아래 단계를 따르세요.

3. 어떻게 도와드릴까요? 에서 다음을 수행하세요.
   a. 계정 및 결제 지원을 선택합니다.
   b. 서비스 목록에서 Chime SDK (번호 관리) 를 선택합니다.
   c. 범주 목록에서 전화번호 포트 인을 선택합니다.
   d. 다음 단계: 추가 정보를 선택합니다
4. 추가 정보에서 다음을 수행하십시오.
   a. 제목에 **`Porting phone numbers in`**을 입력합니다.

b. 설명에 다음 정보를 입력합니다.

미국 번호를 포팅하는 경우:

- 계정의 결제 전화번호(BTN).
- 인증하는 개인 이름. 현재 통신사 계정 결제를 담당하는 개인의 이름입니다.
- 현재 통신사(알려진 경우)
- 서비스 계정 번호(현재 통신사와 함께 이 정보가 표시되는 경우)
- 서비스 PIN(가능한 경우)
- 서비스 주소 및 고객 이름(현재 통신사 연락처에 표시됨)
- 포팅 등록 날짜 및 시간
- (선택 사항) 청구 전화번호 (BTN) 를 포팅하려면 다음 옵션 중 하나를 선택하십시오.
  - 내 BTN을 이식하고 있으며 내가 제공하고 있는 BTN을 새로운 BTN으로 교체하고 싶습니다. 이 새로운 BTN이 현재 통신사와 동일한 계정에 있는지 확인할 수 있습니다.
  - BTN을 포팅하고 있는데 현재 통신사의 계정을 폐쇄하고 싶습니다.
  - 내 계정은 현재 각 전화번호가 자체 BTN이 되도록 설정되어 있기 때문에 내 BTN을 포팅하고 있습니다. (현재 통신사의 계정이 이 방법으로 설정된 경우에만 이 옵션을 선택합니다.)
  - 옵션을 선택한 후 요청서에 에이전시 레터 (LOA) 를 첨부하십시오.

국제 번호를 포팅하는 경우:

- 미국 외 전화번호의 경우 SIP 미디어 애플리케이션 다이얼인 제품 유형을 사용해야 합니다.
- 번호 유형(시내전화 또는 수신자 부담)
- 포팅할 기존 전화번호.
- 사용량 추정
- 국가

c. 전화번호 유형 목록에서 비즈니스 전화, SIP 미디어 애플리케이션 다이얼인 또는 음성 커넥터를 선택합니다.

d. 전화 번호에 전화 번호를 하나 이상 입력합니다. 번호를 여러 개 포팅하는 경우에도 마찬가지입니다.

e. 포팅 날짜에 원하는 포팅 날짜를 입력합니다.

f. 포팅 시간에 원하는 시간을 입력합니다.

g. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.

5. 지금 해결 또는 문의하기에서 문의하기를 선택합니다.
6. 기본 연락처 언어 목록에서 언어를 선택합니다.
7. 웹 또는 전화를 선택합니다. 전화를 선택하는 경우 전화번호를 입력합니다. 완료하면 제출을 선택합니다.

AWS Support 기존 이동통신사에서 전화번호를 포팅할 수 있는지 여부를 알 수 있습니다. 가능하면 필요한 서류를 모두 제출해야 합니다. 다음 섹션의 단계에서는 이러한 문서를 제출하는 방법을 설명합니다.

필수 문서 제출

AWS Support에서 전화번호를 포팅할 수 있다고 요청한 후에는 필요한 문서를 모두 제출해야 합니다. 다음 단계에서는 그 방법을 설명합니다.

> **Note**
>
> AWS Support는 요청된 모든 문서를 업로드할 수 있는 안전한 Amazon S3 링크를 제공합니다. 링크를 받을 때까지 진행하지 마십시오.

문서 제출하기

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 계정에 로그인한 다음 AWS 계정용으로 특별히 생성된 Amazon S3 업로드 링크를 엽니다.

   > **Note**
   >
   > 이 링크는 10일 후에 만료되며, 케이스를 생성한 계정에 사용하도록 특별히 생성되는 링크입니다. 링크를 사용하려면 계정의 인증된 사용자가 업로드를 수행해야 합니다.

3. [Add Files] 를 선택한 다음 요청과 관련된 ID 문서를 선택합니다.
4. 권한 섹션을 확장하고 개별 ACL 권한 지정을 선택합니다.
5. 액세스 제어 목록 (ACL) 섹션 끝에서 수혜자 추가를 선택한 다음 AWS Support에서 제공한 키를 수혜자 상자에 붙여넣습니다.
6. 개체에서 읽기 확인란을 선택한 다음 업로드를 선택합니다.

에이전시 레터 (LOA) 를 제공한 후 기존 통신사에 LOA에 있는 정보가 정확한지 AWS Support 확인합니다. LOA에서 제공된 정보가 전화 사업자의 파일에 있는 정보와 일치하지 않으면, AWS Support 가 LOA에서 제공한 정보를 업데이트하도록 연락합니다.

요청 상태 보기

다음 단계는 Amazon Chime 콘솔을 사용하여 포팅 요청 상태를 확인하는 방법을 설명합니다.

상태를 보려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창에서 전화번호 관리를 선택합니다.
3. 주문 탭을 선택합니다.

상태 열에는 요청 상태가 표시됩니다. AWS Support 또한 필요한 경우 업데이트 및 추가 정보 요청과 함께 귀하에게 연락을 취합니다. 자세한 내용은 이 섹션 후반부의 전화번호 포팅 상태 정의 섹션을 참조하세요.

포팅된 번호 지정

이동통신사에서 LOA가 올바른지 확인한 후 요청된 포트를 검토하고 승인합니다. 그런 다음 AWS Support 포트가 실행될 확정 주문 약정 (FOC) 날짜 및 시간을 제공합니다.

FOC 날짜에 포팅된 전화번호를 활성화하여 사용할 수 있습니다. 그런 다음 원하는 계정의 사용자에게 번호를 할당해야 합니다.

전화번호를 할당하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭에서 할당하려는 번호 옆의 확인란을 선택한 다음 할당을 선택합니다.

> **Note**
>
> 한 번에 하나의 번호만 선택할 수 있습니다.

4. 사용자 프로필에 +1 전화번호 할당 페이지에서 해당 번호의 계정을 선택한 후 다음을 선택합니다.
5. 번호를 할당하려는 사용자를 선택한 다음 할당을 선택합니다.

전화번호 포팅 아웃하기

당첨된 배송사를 통해 포팅 요청을 시작하여 Amazon Chime에서 번호를 포팅합니다. 수상한 배송사에 정보를 제출할 때는 포팅되는 전화번호와 연결된 계정 ID로 계정 ID를 포함하십시오 AWS .

포팅 프로세스가 완료되고 당첨된 배송사에 번호가 있으면 해당 번호의 할당을 취소하고 인벤토리에서 삭제해야 합니다. 자세한 내용은 이 설명서의 Amazon Chime 비즈니스 콜링 전화번호 할당 취소 및 전화번호 삭제 단원을 참조하세요.

Important

- 번호를 포팅할 수 있는지 여부는 당첨된 배송사가 해당 번호를 수락할 수 있는지에 따라 달라집니다.
- 대상 통신 사업자의 다른 곳으로 포팅 요청에서 진위 여부를 확인하는 것은 전화번호 보안을 위해 매우 중요합니다. 계정 세부 정보가 정확하지 않은 경우 (예: 계정 ID 불일치) 포팅 요청이 거부되어 지연이 발생하고 요청을 다시 제출해야 할 수 있습니다.

(선택 사항) 번호 보호를 위한 PIN 요청 방법

보안을 강화하기 위해 당사에 문의하여 번호에 PIN을 적용할 수 있습니다. 그러면 우승한 이동 통신사가 해당 PIN을 사용합니다. 다음 단계를 따릅니다.

PIN 요청하기

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 문의처에서 Support를 선택합니다.

   그러면 AWS Support 콘솔로 이동합니다.

   Note

   AWS Support 센터 페이지로 바로 이동할 수도 있습니다. 그럴 경우 사례 만들기를 선택한 다음 아래 단계를 따르세요.

3. 어떻게 도와드릴까요? 에서 다음을 수행하세요.

   a. 계정 및 결제 지원을 선택합니다.

b. 서비스 목록에서 Chime SDK (번호 관리) 를 선택합니다.

c. 범주 목록에서 전화번호 포트 아웃을 선택합니다.

d. 다음 단계: 추가 정보를 선택합니다

4. 추가 정보에서 다음을 수행하십시오.

a. 제목에 **`Porting phone numbers out`**을 입력합니다.

b. 설명에 다음을 입력합니다.

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

> **Note**
>
> 4~10자의 영숫자 PIN을 제공해야 합니다.

AWS Support는 PIN을 전화 번호와 연결합니다. 우승한 배송사에 포트를 요청할 때는 AWS 계정 ID와 PIN을 제공하십시오. 해당 정보를 사용하여 귀하의 번호로 접수된 모든 포트 요청을 확인합니다.

전화번호 포팅 상태 정의

기존 전화번호를 Amazon Chime에 이식하는 요청을 제출한 후 Amazon Chime 콘솔의 통화, 전화번호 관리, 대기 중에서 이식 요청의 상태를 확인할 수 있습니다.

포팅 상태 및 정의는 다음과 같습니다.

취소됨

AWS Support 배송사 또는 고객의 취소 요청 등 포트 관련 문제로 인해 포팅 주문을 취소했습니다. AWS Support 자세한 내용을 안내해 드립니다.

CANCEL_REQUESTED

AWS Support 배송사 또는 고객의 취소 요청과 같은 항구 관련 문제로 인해 포팅 주문 취소를 처리하고 있습니다. AWS Support 자세한 내용을 안내해 드립니다.

CHANGE_REQUESTED

AWS Support 변경 요청을 처리 중이며 배송사 응답이 보류 중입니다. 추가 처리 시간을 허용합니다.

완료됨

이식 주문이 완료되고 전화번호가 활성화됩니다.

EXCEPTION

AWS Support 포트 요청을 완료하는 데 필요한 추가 세부 정보를 문의하기 위해 연락드립니다. 추가 처리 시간을 허용합니다.

FOC

FOC 날짜는 배송사와 확인합니다. AWS Support 날짜를 확인하기 위해 연락을 드립니다.

PENDING DOCUMENTS

AWS Support 포트 요청을 완료하는 데 필요한 추가 문서를 문의하기 위해 연락드립니다. 추가 처리 시간을 허용합니다.

SUBMITTED

이식 주문이 제출되었으며 통신사 응답이 보류 중입니다.

Amazon Chime 비즈니스 콜링 전화번호 할당

전화번호 관리 인벤토리 페이지를 사용하여 Amazon Chime 비즈니스 콜링 전화번호를 개별 사용자에게 할당할 수 있습니다.

Amazon Chime 비즈니스 콜링 전화번호를 할당하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭에서 할당하려는 전화번호를 선택합니다.
4. 할당을 선택합니다.
5. 사용자가 속한 계정을 선택한 후 다음을 선택합니다.
6. 사용자를 선택한 다음 할당을 선택합니다.

전화번호 또는 전화번호 권한을 변경하는 경우 사용자에게 새 정보 또는 권한 정보를 제공하는 것이 좋습니다. 사용자가 새 전화번호 또는 권한 기능에 액세스하려면 먼저 Amazon Chime 계정에서 로그아웃한 후 다시 로그인해야 합니다.

Amazon Chime 비즈니스 콜링 전화번호 할당 취소

다음 절차는 Amazon Chime Business Calling 사용자의 전화번호 할당을 해제합니다.

전화번호 할당을 취소하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭에서 할당을 취소하려는 전화번호를 선택합니다.
4. 할당 해제를 선택합니다.
5. 확인란을 선택하고 할당 해제를 선택합니다.

인벤토리에 있는 번호의 세부 정보를 볼 수 있습니다. 예를 들어 전화 통화 및 문자 메시지가 활성화되었는지 확인할 수 있습니다.

인벤토리 전화번호 세부 정보를 보려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭을 선택한 다음, 보려는 전화번호를 선택합니다.
4. 작업을 열고 세부 정보 보기를 선택합니다.

발신 전화 이름 사용

아웃바운드 전화 이름은 발신자 ID 역할을 합니다. 인벤토리에 있는 하나 이상의 전화번호에 기본 통화 이름을 설정할 수 있습니다. 개별 전화번호에 고유한 전화 이름을 설정할 수도 있습니다. 그러면 해당 전화번호를 사용하여 걸려온 발신 전화의 수신자에게 이름이 표시됩니다. 전화 이름은 모든 전화번호 제품 유형에 적용됩니다. 7일마다 이름을 업데이트할 수 있습니다.

예를 들어, 해당 부서의 모든 전화 번호에 대해 부서 5의 기본 전화 이름을 설정할 수 있습니다. 부서장의 고유한 이름을 Jane Doe로 설정할 수도 있습니다.

다음 단계에서는 기본 발신 전화 이름과 개별 발신 전화 이름을 설정하는 방법을 설명합니다.

통화 이름을 설정하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.

2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭에서 다음 중 하나를 수행하십시오. 업데이트하려는 전화번호 옆의 확인란을 선택합니다.

   - 여러 번호의 기본 발신 이름을 설정하려면 해당 번호 옆의 확인란을 선택합니다.
   - 개별 전화 이름을 설정하려면 원하는 번호를 선택합니다.
4. 작업 목록을 열고 기본 호출 이름 업데이트를 선택합니다.
5. 기본 호출 이름에 15자 이내의 기본 통화 이름을 입력합니다.
6. 저장을 선택합니다.

기본 통화 이름을 업데이트하는 데는 72시간 정도 소요됩니다.

전화번호 삭제

> **Important**
>
> Amazon Chime 시스템 관리자만 이 단계를 완료할 수 있습니다. 전화번호를 삭제하려면 우선 모든 전화번호를 할당 해제해야 합니다.

전화번호를 프로비저닝할 경우, Amazon Chime에서 유지 관리하는 번호 풀에서 전화번호를 주문합니다. 전화번호를 삭제하면 전화번호가 풀로 다시 이동합니다. 전화번호를 삭제하면 해당 전화번호는 먼저 삭제 대기열로 이동하여 7일 동안 보관됩니다. 이 기간에는 전화번호를 인벤토리로 다시 이동할 수 있습니다. 7일이 지나면 대기 중인 대기열에서 전화번호가 자동으로 삭제되고 계정에서 해당 전화번호의 연결이 해제됩니다. 그러면 번호가 번호 풀에 반환됩니다. 대기 중인 대기열에서 전화번호가 삭제된 후 전화번호를 회수해야 할 경우 전화번호 프로비저닝의 단계를 따르되, 해당 전화번호를 사용하지 못할 수도 있다는 점에 유의하시기 바랍니다.

할당 해제된 전화번호를 삭제하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 인벤토리 탭을 선택한 다음, 삭제하려는 전화번호를 선택합니다.
4. 작업 목록을 열고 전화번호 삭제를 선택합니다.
5. 확인란을 선택한 다음 삭제를 선택합니다.

삭제된 전화번호는 삭제 대기열에 7일 동안 보관된 후 인벤토리에서 영구적으로 삭제됩니다.

삭제된 전화번호 복원

전화번호를 삭제한 후 최대 7일 동안 삭제 대기열에서 삭제된 전화번호를 복원할 수 있습니다. 전화번호를 복원하면 전화번호는 인벤토리로 다시 이동합니다.

삭제된 전화번호를 복원하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 탐색 창의 통화에서 전화번호 관리를 선택합니다.
3. 삭제 대기열 탭을 선택한 다음, 복원할 전화번호를 선택합니다.
4. 인벤토리로 이동을 선택합니다.

Amazon Chime에서 글로벌 설정 관리

Amazon Chime 콘솔을 사용하여 통화 세부 기록 설정을 관리합니다.

호출 세부 정보 레코드 구성

Amazon Chime 관리 계정에 대한 통화 세부 정보 레코드 설정을 구성하려면 먼저 Amazon Simple Storage Service 버킷을 생성해야 합니다. Amazon S3 버킷은 통화 세부 기록에 대한 로그 대상으로 사용됩니다. 호출 세부 정보 레코드 설정을 구성할 때는 데이터를 저장하고 관리할 수 있도록 Amazon Chime 읽기 및 쓰기 액세스 권한을 Amazon S3 버킷에 부여합니다. Amazon S3 버킷을 생성하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon Simple Storage Service 시작하기를 참조하세요.

Amazon Chime Business Calling에 대한 통화 세부 기록 설정을 구성할 수 있습니다. Amazon Chime Business Calling에 대한 자세한 내용은 Amazon Chime에서 전화번호 관리 섹션을 참조하세요.

호출 세부 정보 레코드 설정을 구성하려면

1. Amazon Simple Storage Service 사용 설명서의 Amazon Simple Storage Service 시작하기의 단계에 따라 Amazon S3 버킷을 생성합니다.
2. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
3. 글로벌 설정에서 호출 세부 정보 레코드를 선택합니다.
4. 비즈니스 통화 구성을 선택합니다.
5. 로그 대상에서 Amazon S3 버킷을 선택합니다.
6. 저장을 선택합니다.

언제든지 호출 세부 정보 레코드의 로깅을 중지할 수 있습니다.

호출 세부 정보 레코드의 로깅을 중지하려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 글로벌 설정에서 호출 세부 정보 레코드를 선택합니다.
3. 해당 구성에 대한 로깅 비활성화를 선택합니다.

Amazon Chime Business Calling 통화 세부 기록

Amazon Chime Business Calling에 대한 통화 세부 기록을 수신하기로 선택하면 해당 기록이 사용자의 Amazon S3 버킷으로 전송됩니다. 다음 예제에서는 Amazon Chime Business Calling 통화 세부 기록 이름의 일반 형식을 보여줍니다.

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

다음 예제에서는 호출 세부 정보 레코드 이름에 표시되는 데이터를 보여줍니다.

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

다음 예제에서는 Amazon Chime Business Calling 통화 세부 기록의 일반 형식을 보여줍니다.

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

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

    "DestinationPhoneNumber": "+12065550101",
    "DestinationCountry": "US",

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

```
}
```

회의실 구성

Amazon Chime은 Cisco, Tandberg, Polycom, Lifesize, Vidyo 또는 기타 공급업체(SIP 또는 H.323 프로토콜을 사용하는 경우)의 채팅룸 비디오 하드웨어와 통합됩니다.

SIP를 지원하는 회의실 VTC 디바이스를 사용하여 Amazon Chime에 연결하려면 다음 옵션 중 하나를 입력합니다.

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- 10자리수 회의 ID 다음에 **`@meet.chime.in`**

`meet.chime.in`은 SIP 회의실 디바이스를 가장 가까운 Amazon Chime 리전에 연결합니다. 특정 리전에 연결하려면 SIP 회의실 시스템에 리전별 DNS 항목을 사용합니다. 자세한 내용은 SIP(Session Initiation Protocol) 회의실 시스템 섹션을 참조하세요.

> **Note**
>
> SIP 회의실 디바이스가 TLS를 지원하지 않는데 TCP 연결이 필요한 경우, AWS 지원 센터에 문의하세요.

H.323만 지원하는 장치를 사용하는 경우 다음 중 하나로 전화를 걸어야 합니다.

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

방화벽이 VTC 디바이스와 Amazon Chime 간의 트래픽을 필터링하는 경우 사용된 프로토콜에 대한 범위를 여세요. 자세한 내용은 네트워크 구성 및 대역폭 요구 사항 섹션을 참조하세요.

Amazon Chime 시작 화면에서 10자리수 또는 13자리수 회의 ID를 입력하여 참가합니다. Amazon Chime 클라이언트 또는 웹 앱에서 13자리수 회의 ID를 검색하거나 전화 접속 옵션을 선택할 수 있습니다.

중재 회의 참가

중재 회의에서 주최자 또는 대리인은 자신의 13자리수 회의 ID를 입력해야 중재자로 회의에 참여할 수 있습니다. 중재자는 다이얼 패드에 중재자 암호 뒤에 파운드 기호(#)를 입력해야만 회의에 참여하여 시작할 수 있습니다. 주최자, 대리인 또는 중재자가 아닌 사람은 중재자가 회의에 참여하여 시작한 후에 회의에 연결됩니다.

중재자는 주최자 컨트롤이 있어 추가적인 회의 작업을 수행할 수 있습니다. 이러한 작업에는 녹음 시작과 정지, 회의 잠금 및 잠금 해제, 다른 모든 참가자의 음소거, 회의 종료가 포함됩니다. 자세한 내용은 Amazon Chime 사용 설명서의 회의실 내 비디오 시스템을 사용하는 중재자 작업을 참조하세요.

> **Note**
>
> Alexa for Business를 사용하여 Amazon Chime 회의에 참여할 경우에는 회의실 내 비디오 시스템에 사용자의 디바이스가 연결되어 있고, 디바이스의 다이얼 패드를 사용하여 전화 접속할 경우에만 중재자로 참여할 수 있습니다.

호환되는 VTC 디바이스

다음 표에는 호환되는 VTC 디바이스 목록의 일부가 나와 있습니다.

디바이스	SIP	H.323	Comment
Cisco SX20	예	예	오디오/비디오/스크린: 양방향 연결 가능
Cisco DX80	예	예	오디오/비디오/스크린: 양방향 연결 가능
Lifesize 아이콘	예	아니요	오디오/비디오/스크린: 양방향 연결 가능

디바이스	SIP	H.323	Comment
Polycom Debut	예	예	오디오/비디오/스크린: 양방향 연결 가능
Polycom RealPresence Desktop	아니요	예	오디오/비디오: 가능, 스크린: 시작 디바이스 가능
Polycom Trio	예	예	오디오/비디오/스크린: 양방향 연결 가능
Tandberg C40	예	예	오디오/비디오/스크린: 양방향 연결 가능

네트워크 구성 및 대역폭 요구 사항

Amazon Chime에서 다양한 서비스를 지원하려면 이 주제에 설명된 대상 및 포트가 필요합니다. 인바운드 또는 아웃바운드 트래픽이 차단되면 오디오, 비디오, 화면 공유, 채팅 등 다양한 서비스의 사용에 영향을 줄 수 있습니다.

Amazon Chime은 TCP/443 포트에서 Amazon Elastic Compute Cloud(Amazon EC2) 및 기타 AWS 서비스를 사용합니다. 방화벽이 포트 TCP/443을 차단할 경우 `*.amazonaws.com`을 허용 목록에 넣거나, 아래의 서비스에 대해 AWS 일반 참조에 AWS IP 주소 범위를 넣어야 합니다.

- Amazon EC2
- 아마존 CloudFront
- Amazon Route 53

목적지, 포트 및 대역폭에 대한 자세한 내용은 다음 섹션을 확장하십시오.

필수 대상 및 포트

Amazon Chime을 실행하려면 다음과 같은 대상 및 포트가 필요합니다.

대상	포트
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com을 위한 CNAME 별칭으로 구성해야 합니다	TCP/443
99.77.128.0/18	TCP/443

미팅 및 텔레포니 포트

Amazon Chime은 회의 및 Amazon Chime Business Calling을 위해 다음과 같은 대상과 포트를 사용합니다.

대상	Port
99.77.128.0/18	UDP/3478

H.323 회의실 시스템

Amazon Chime은 H.323 회의실 내 비디오 시스템에 대해 다음과 같은 대상 및 포트를 사용합니다.

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

SIP(Session Initiation Protocol) 회의실 시스템

현재 환경에서 SIP 회의실 내 비디오 시스템에 대해 Amazon Chime을 실행하는 경우 다음과 같은 대상 및 포트를 사용하는 것이 좋습니다.

AWS 지역	대상	포트
글로벌(가장 가까운 리전)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS 지역	대상	포트
	52.55.63.0/25	
전 세계	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
미국 동부(버지니아 북부)	meet.ue1.chime.in	TCP/5061
미국 서부(오레곤)	meet.uw2.chime.in	TCP/5061
아시아 태평양(싱가포르)	meet.as1.chime.in	TCP/5061
아시아 태평양(시드니)	meet.as2.chime.in	TCP/5061
아시아 태평양(도쿄)	meet.an1.chime.in	TCP/5061
유럽(아일랜드)	meet.ew1.chime.in	TCP/5061
남아메리카(상파울루)	meet.se1.chime.in	TCP/5061

대역폭 요구 사항

Amazon Chime의 오디오, 비디오 및 화면 공유에 대한 대역폭 요구 사항은 다음과 같습니다.

- 오디오
  - 1:1 통화: 54kbps 업/다운
  - 대규모 통화: 50명의 경우 추가로 32kbps 다운
- 비디오
  - 1:1 통화: 650kbps 업/다운
  - HD 모드: 1400kbps 업/다운
  - 3~4명: 450kbps 업, (N-1)*400kbps 다운
  - 5~16명: 184kbps 업, (N-1)*134kbps 다운
  - 업/다운 대역폭은 네트워크 상태에 따라 낮게 조정됩니다.
- 화면 공유

- 고품질의 경우 1.2mbps 업(프레젠테이션)/다운(보기). 네트워크 상태에 따라 320kbps까지 하향 조정됩니다.
- 원격 제어: 800kbps 고정

보고서 보기

정보에 기초한 의사 결정을 내리고 조직의 생산성을 높이기 위해 콘솔에서 사용량 및 피드백 데이터를 직접 확인할 수 있습니다. 보고서 데이터는 매일 업데이트되며, 최대 48시간 정도의 지연이 있을 수 있습니다.

사용량 및 피드백 보고서를 보려면

1. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
2. 보고서, 대시보드를 선택합니다.
3. 사용량 및 피드백 대시보드 보고서 페이지에서 다음 데이터를 볼 수 있습니다.

> **Note**
>
> 사용 가능한 데이터에 대한 자세한 내용은 Amazon Chime 보고서 대시보드 및 사용자 활동 정보를 참조하세요.

- 날짜 범위(UTC) - 보고서의 날짜 범위.
- 등록된 사용자 - Amazon Chime에 등록한 사용자의 수.
- 활성 사용자 - Amazon Chime을 사용하여 회의에 참석하거나 메시지를 보낸 사용자의 수.
- 회의 개최 - 종료된 총 회의 수. 특정 회의를 선택하여 회의 ID, 시작 시간, 유형, 조직자, 기간, 참석자 수 등을 비롯한 세부 정보를 볼 수 있습니다. 참석자, 회의 명단 이벤트, 클라이언트 유형, 회의 피드백 등의 추가 세부 정보를 보려면 특정 회의 ID 또는 회의 조직자를 선택합니다.
- 회의 만족도 - 회의 종료 후 설문 조사에서 제공된 긍정적 응답의 비율입니다.
- 채팅 메시지 전송됨 - 사용자가 보낸 채팅 메시지 수입니다.

Amazon Chime 데스크톱 클라이언트 확장

챗봇, 프록시 전화 세션, 웹후크를 추가하여 Amazon Chime 데스크톱 클라이언트의 기능을 확장할 수 있습니다. 챗봇을 통해 사용자는 내부 시스템에 정보를 쿼리하는 등의 작업을 수행할 수 있습니다. 프록시 전화 세션을 통해 사용자는 전화번호를 표시하지 않고도 전화를 걸고 문자를 전송할 수 있습니다. 웹후크는 채팅룸에 메시지를 자동으로 전송할 수 있습니다. 예를 들어 웹후크는 회의 링크와 함께 회의 알림을 팀에 전송할 수 있습니다.

주제

사용자 관리

다음과 같은 코드 스니펫은 Amazon Chime 사용자를 관리하는 데 도움이 될 수 있습니다. 이 주제의 모든 예제에서는 Java를 사용합니다.

주제

여러 사용자 초대

아래의 예제에서는 Amazon Chime Team 계정에 여러 사용자를 초대하는 방법을 보여줍니다.

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

```
chime.inviteUsers(inviteUsersRequest);
```

사용자 목록 다운로드

아래의 예제에서는 Amazon Chime 관리 계정과 연결된 사용자 목록을 `.csv` 형식으로 다운로드하는 방법을 보여줍니다.

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

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

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

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

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

printer.close();
```

여러 사용자 로그아웃

아래의 예제에서는 Amazon Chime 관리 계정에서 여러 사용자를 로그아웃하는 방법을 보여줍니다.

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

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

    chime.logoutUser(logoutUserRequest);
}
```

사용자 개인 PIN 업데이트

아래의 예제에서는 지정된 Amazon Chime 사용자의 개인 회의 PIN을 재설정하는 방법을 보여줍니다.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

Amazon Chime 데스크톱 클라이언트에 챗봇 통합

AWS Command Line Interface(AWS CLI), Amazon Chime API 또는 AWS SDK를 사용하여 챗봇을 Amazon Chime과 통합할 수 있습니다. 챗봇을 사용하면 Amazon Lex, AWS Lambda 및 기타 AWS 서비스의 기능을 사용하여 지능적인 대화형 인터페이스를 통해 일반 작업을 간소화할 수 있습니다. 이 인터페이스는 Amazon Chime 채팅룸의 사용자가 액세스할 수 있습니다.

Amazon Chime 엔터프라이즈 계정 관리자인 경우, 챗봇을 사용하여 사용자가 다음과 같은 태스크를 수행하도록 허용할 수 있습니다.

- 정보를 위해 내부 시스템에 쿼리 작성
- 자동화 작업
- 심각한 문제에 대한 알림 수신
- 지원 티켓 생성

Amazon Chime 엔터프라이즈 계정 유형에 대한 자세한 내용은 Amazon Chime 계정 관리 섹션을 참조하세요.

Amazon Chime Enterprise 계정을 관리하는 경우 최대 10개의 채팅 봇을 생성하여 Amazon Chime과 통합할 수 있습니다. 챗봇은 사용자 계정의 멤버가 생성한 채팅룸에서만 사용할 수 있습니다. 채팅룸 관리자만 채팅룸에 챗봇을 추가할 수 있습니다. 채팅룸에 챗봇을 추가하면 채팅룸의 멤버는 봇 생성자가 제공한 명령을 사용하여 봇과 상호 작용할 수 있습니다. 자세한 내용은 이 주제의 다음 섹션을 참조하세요.

Linux 및 macOS 사용자는 샘플 사용자 지정 챗봇을 만들 수 있습니다. 자세한 내용은 Amazon Chime 사용자 지정 챗봇 만들기를 참조하세요.

Content

Amazon Chime에서 챗봇 사용

Amazon Chime Enterprise 계정을 관리하는 경우 최대 10개의 채팅 봇을 생성하여 Amazon Chime과 통합할 수 있습니다. 챗봇은 사용자 계정의 멤버가 생성한 채팅룸에서만 사용할 수 있습니다. 채팅룸 관리자만 채팅룸에 챗봇을 추가할 수 있습니다. 채팅룸에 챗봇을 추가하면 채팅룸의 멤버는 봇 생성자가 제공한 명령을 사용하여 봇과 상호 작용할 수 있습니다. 자세한 내용을 알아보려면 Amazon Chime 사용 설명서의 챗봇 사용하기를 참조하세요.

Amazon Chime API를 사용하여 Amazon Chime 계정에 대한 챗봇을 활성화하거나 중지할 수도 있습니다. 자세한 내용은 챗봇 업데이트 섹션을 참조하세요.

> **Note**
>
> 챗봇은 삭제할 수 없습니다. 계정에서 챗봇 사용을 중지하려면 Amazon Chime API 참조에서 Amazon Chime UpdateBot API 작업을 사용하세요. 챗봇을 중지하면 채팅룸 관리자가 채팅룸에서 챗봇을 제거할 수 있지만, 채팅룸에 추가할 수는 없습니다. 채팅룸에서 중단된 챗봇을 @언급한 사용자에게는 오류 메시지가 표시됩니다.

필수 조건

챗봇을 Amazon Chime과 통합하는 절차를 시작하려면 우선 다음과 같은 사전 조건을 완료하세요.

- 챗봇을 생성합니다.

- Amazon Chime에 대한 아웃바운드 엔드포인트를 생성하여 이벤트를 봇에 전송합니다. AWS Lambda 함수 ARN 또는 HTTPS 엔드포인트 중에서 선택합니다. Lambda에 대한 자세한 내용은 AWS Lambda 개발자 설명서를 참조하세요.

HTTPS 엔드포인트 대한 DNS 모범 사례

HTTPS 엔드포인트에 대해 DNS를 할당할 때 다음 모범 사례를 따르는 것이 좋습니다.

- 봇 엔드포인트 전용 DNS 하위 도메인을 사용합니다.
- A 레코드를 사용하여 봇 엔드포인트를 가리킵니다.
- 도메인 탈취를 방지하기 위해 DNS 서버 및 DNS 등록 대행자 계정을 보호합니다.
- 공개적으로 유효한 봇 엔드포인트 전용 TLS 중간 인증서를 사용합니다.
- 봇 메시지에 대해 작업하기 전에 봇 메시지 서명을 암호화 방식으로 검증합니다.

챗봇을 생성한 후 AWS Command Line Interface(AWS CLI) 또는 Amazon Chime API 작업을 사용하여 다음 섹션에 설명된 태스크를 완료하세요.

작업

- 1단계: 챗봇을 Amazon Chime과 통합
- 2단계: Amazon Chime 챗봇에 대한 아웃바운드 엔드포인트 구성
- 3단계: Amazon Chime 채팅룸에 챗봇 추가
- 챗봇 요청 인증
- 챗봇 업데이트

1단계: 챗봇을 Amazon Chime과 통합

사전 조건을 완료한 후 AWS CLI 또는 Amazon Chime API를 사용하여 챗봇을 Amazon Chime과 통합합니다.

> **Note**
>
> 이 절차를 수행하면 챗봇의 이름과 이메일 주소가 생성됩니다. 생성 후에는 챗봇 이름과 이메일 주소를 변경할 수 없습니다.

AWS CLI

AWS CLI를 사용하여 챗봇을 통합하려면

1. 챗봇을 Amazon Chime과 통합하려면 AWS CLI의 create-bot 명령을 사용하세요.

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

   a. 최대 55자의 영숫자 또는 특수 문자(예: +, -, %)로 구성된 챗봇 표시 이름을 입력합니다.

   b. Amazon Chime 엔터프라이즈 계정에 대해 등록된 도메인 이름을 입력합니다.

2. Amazon Chime에서 봇 ID가 포함된 응답을 반환합니다.

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

3. 다음 절차에 사용할 봇 ID와 봇 이메일 주소를 복사한 후 저장합니다.

Amazon Chime API

Amazon Chime API를 사용하여 챗봇을 통합하려면

1. 챗봇을 Amazon Chime과 통합하려면 Amazon Chime API 참조의 CreateBot API 작업을 사용하세요.

   a. 최대 55자의 영숫자 또는 특수 문자(예: +, -, %)로 구성된 챗봇 표시 이름을 입력합니다.

   b. Amazon Chime 엔터프라이즈 계정에 대해 등록된 도메인 이름을 입력합니다.

2. Amazon Chime에서 봇 ID가 포함된 응답을 반환합니다. 봇 ID와 이메일 주소를 복사한 후 저장합니다. 봇 이메일 주소는 *exampleBot*-chimebot@*example.com* 같은 형식입니다.

Java용 AWS SDK

아래의 샘플 코드는 Java용 AWS SDK를 사용하여 챗봇을 통합하는 방법을 보여줍니다.

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

chime.createBot(createBotRequest);
```

Amazon Chime에서 봇 ID가 포함된 응답을 반환합니다. 봇 ID와 이메일 주소를 복사한 후 저장합니다. 봇 이메일 주소는 *exampleBot*-chimebot@*example.com* 같은 형식입니다.

2단계: Amazon Chime 챗봇에 대한 아웃바운드 엔드포인트 구성

Amazon Chime 엔터프라이즈 계정에 대한 챗봇 ID를 생성한 후에는 Amazon Chime이 봇에 메시지를 전송하는 데 사용할 아웃바운드 엔드포인트를 구성합니다. 아웃바운드 엔드포인트는 사용자가 사전 조건의 일부로 생성한 AWS Lambda 함수 ARN 또는 HTTPS 엔드포인트일 수 있습니다. Lambda에 대한 자세한 내용은 AWS Lambda 개발자 설명서를 참조하세요.

> **Note**
>
> 봇에 대한 아웃바운드 HTTPS 엔드포인트가 구성되지 않았거나 비어 있는 경우 채팅룸 관리자는 채팅룸에 봇을 추가할 수 없습니다. 또한 채팅룸 사용자는 봇과 상호 작용할 수 없습니다.

AWS CLI

챗봇에 대한 아웃바운드 엔드포인트를 구성하려면 AWS CLI의 put-events-configuration 명령을 사용하세요. Lambda 함수 ARN 또는 아웃바운드 HTTPS 엔드포인트를 구성합니다.

Lambda ARN

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

HTTPS endpoint

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

Amazon Chime은 봇 ID 및 HTTPS 엔드포인트로 응답합니다.

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

Amazon Chime API

챗봇에 대한 아웃바운드 엔드포인트를 구성하려면 Amazon Chime API 참조에서 Amazon Chime PutEventsConfiguration API 작업을 사용하세요. Lambda 함수 ARN 또는 아웃바운드 HTTPS 엔드포인트를 구성합니다.

- Lambda 함수 ARN을 구성할 경우 - Amazon Chime은 Lambda를 직접 호출하여 Amazon Chime 관리자의 AWS 계정이 제공된 Lambda 함수 ARN을 간접 호출할 수 있는 권한을 추가합니다. 이후 Amazon Chime에서 함수를 간접 호출할 권한이 있는지 확인하는 모의 실습 호출이 수행됩니다. 권한 추가에 실패하거나 모의 실습 호출이 실패하면 `PutEventsConfiguration` 요청에서는 HTTP 4xx 오류가 반환됩니다.
- 아웃바운드 HTTPS 엔드포인트를 구성할 경우 - Amazon Chime에서는 Challenge JSON 페이로드가 있는 HTTP Post 요청을 이전 단계에서 제공한 아웃바운드 HTTPS 엔드포인트로 전송하여 엔드포인트를 확인합니다. 아웃바운드 HTTPS 엔드포인트에서는 Challenge 파라미터를 JSON 형식으로 되풀이하여 응답해야 합니다. 다음은 요청 및 유효한 응답을 보여주는 예입니다.

  Request

```
HTTPS POST

JSON Payload:
{
   "Challenge":"00000000000000000000",
```

```
    "EventType" : "HTTPSEndpointVerification"
}
```

Response

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

{
    "Challenge":"0000000000000000000"
}
```

Challenge 핸드셰이크가 실패하면 PutEventsConfiguration 요청에서는 HTTP 4xx 오류가 반환됩니다.

Java용 AWS SDK

아래의 샘플 코드는 Java용 AWS SDK를 사용하여 엔드포인트를 구성하는 방법을 보여줍니다.

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

 chime.putEventsConfiguration(putEventsConfigurationRequest):
```

3단계: Amazon Chime 채팅룸에 챗봇 추가

채팅룸 관리자만 채팅룸에 챗봇을 추가할 수 있습니다. 채팅룸 관리자는 1단계에서 생성된 챗봇 이메일 주소를 사용합니다.

채팅룸에 챗봇을 추가하려면

1. Amazon Chime 데스크톱 클라이언트 또는 웹 애플리케이션을 엽니다.
2. 오른쪽 상단 모서리에 있는 기어 모양 아이콘을 선택하고 웹후크 및 봇 관리를 선택합니다.

3. 봇 추가을 선택합니다.
4. 이메일 주소에 봇 이메일 주소를 입력합니다.
5. 추가를 선택합니다.

봇 이름이 채팅 룸 명단에 표시됩니다. 채팅룸에 챗봇을 추가하는 데 필요한 추가 작업이 있을 경우 해당 작업을 채팅룸 관리자에게 제공하세요.

채팅룸에 챗봇을 추가한 후 채팅룸 사용자에게 챗봇 명령을 제공합니다. 이를 위한 한 가지 방법은 채팅룸 초대를 받았을 때 명령 도움말을 채팅룸에 전송하도록 챗봇을 프로그래밍하는 것입니다. 또한 챗봇 사용자가 사용할 도움말 명령을 생성하는 것이 좋습니다.

챗봇 요청 인증

Amazon Chime 채팅룸에서 챗봇에 전송된 요청을 인증할 수 있습니다. 이렇게 하려면 요청에 따라 서명을 계산합니다. 그런 다음, 계산된 서명이 요청 헤더의 서명과 일치하는지 확인합니다. Amazon Chime은 HMAC SHA256 해시를 사용하여 서명을 생성합니다.

아웃바운드 HTTPS 엔드포인트를 사용하여 Amazon Chime에 대해 챗봇을 구성한 경우 아래의 인증 단계를 따르세요.

아웃바운드 HTTPS 엔드포인트가 구성된 챗봇에 대해 Amazon Chime의 서명된 요청을 검증하려면

1. HTTP 요청에서 Chime-Signature 헤더를 가져옵니다.
2. Chime-Request-Timestamp 헤더와 요청 본문을 가져옵니다. 그런 다음 세로 막대를 두 요소 간의 구분 기호로 사용하여 문자열을 작성합니다.
3. CreateBot 응답의 SecurityToken을 HMAC_SHA_256의 초기 키로 사용하고 2단계에서 생성한 문자열을 해싱합니다.
4. Base64 인코더로 해싱한 바이트를 서명 문자열에 인코딩합니다.
5. 계산된 이 서명을 Chime-Signature 헤더에 있는 서명과 비교합니다.

다음은 Java를 사용하여 서명을 생성하는 방법을 설명하는 코드 샘플입니다.

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

        private String generateSignature(String securityToken, String requestTime,
String requestBody)
```

```
        {
            try {
                final Mac mac = Mac.getInstance(HMAC_SHA_256);
                SecretKeySpec key = new SecretKeySpec(securityToken.getBytes(UTF_8),
HMAC_SHA_256);
                mac.init(key);
                String data = requestTime + DELIMITER + requestBody;
                byte[] rawHmac = mac.doFinal(data.getBytes(UTF_8));

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

아웃바운드 HTTPS 엔드포인트는 2초 이내에 Amazon Chime의 `200 OK` 요청에 응답해야 합니다. 그렇지 않으면 요청이 실패합니다. 연결 또는 읽기 제한 시간으로 인해 2초 후 아웃바운드 HTTPS 엔드포인트를 사용할 수 없거나, Amazon Chime이 5xx 응답 코드를 수신하는 경우 Amazon Chime에서는 요청을 두 번 재시도합니다. 첫 번째 재시도는 초기 요청이 실패한 후 200밀리초에 전송되며, 두 번째 재시도는 이전 재시도가 실패한 후 400밀리초에 전송됩니다. 두 번째 재시도 이후에도 아웃바운드 HTTPS 엔드포인트를 계속 사용할 수 없으면 요청이 실패한 것입니다.

> **Note**
>
> Chime-Request-Timestamp는 요청이 재시도될 때마다 변경됩니다.

Lambda 함수 ARN을 사용하여 Amazon Chime에 대해 챗봇을 구성한 경우 아래의 인증 단계를 따르세요.

Lambda 함수 ARN이 구성된 챗봇에 대해 Amazon Chime의 서명된 요청을 확인하려면

1. Lambda 요청 ClientContext에서 Chime-Signature 및 Chime-Request-Timestamp를 Base64 인코딩 JSON 형식으로 가져옵니다.

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

2. 요청 페이로드에서 요청의 본문을 가져옵니다.
3. `CreateBot` 응답의 SecurityToken을 HMAC_SHA_256의 초기 키로 사용하고, 생성한 문자열을 해싱합니다.
4. Base64 인코더로 해싱한 바이트를 서명 문자열에 인코딩합니다.
5. 계산된 이 서명을 Chime-Signature 헤더에 있는 서명과 비교합니다.

Lambda 간접 호출 중 `com.amazonaws.SdkClientException`이 발생하면 Amazon Chime에서는 요청을 두 번 재시도합니다.

챗봇 업데이트

Amazon Chime 계정 관리자는 Amazon Chime API를 AWS SDK 또는 AWS CLI와 함께 사용하여 챗봇 세부 정보를 볼 수 있습니다. 계정에서 챗봇 사용을 활성화하거나 중지할 수도 있습니다. 챗봇에 대한 보안 토큰도 생성할 수 있습니다.

자세한 내용은 Amazon Chime API 참조의 다음 주제를 참조하세요.

- GetBot – 봇 이메일 주소, 봇 유형 등 챗봇 세부 정보를 가져옵니다.
- UpdateBot – 사용자의 계정에서 챗봇 사용을 활성화하거나 중지합니다.
- RegenerateSecurityToken – 챗봇에 대한 보안 토큰을 재생성합니다.

챗봇에 대해 `PutEventsConfiguration`을 변경하도록 선택할 수도 있습니다. 예를 들어, 초기에 챗봇이 아웃바운드 HTTPS 엔드포인트를 사용하도록 구성된 경우 이전 이벤트 구성을 삭제하고 Lambda 함수 ARN에 대한 새 이벤트 구성을 배치할 수 있습니다.

자세한 내용은 Amazon Chime API 참조의 다음 주제를 참조하세요.

- DeleteEventsConfiguration
- PutEventsConfiguration

챗봇으로 전송된 Amazon Chime 이벤트

Amazon Chime에서 챗봇으로 전송된 이벤트는 다음과 같습니다.

- Invite – 챗봇이 Amazon Chime 채팅룸에 추가된 경우 전송됩니다.
- Mention – 채팅룸의 사용자가 챗봇을 @언급한 경우 전송됩니다.
- Remove – Amazon Chime 채팅룸에서 챗봇이 제거된 경우 전송됩니다.

다음은 이러한 각 이벤트에 대해 챗봇에 전송된 JSON 페이로드를 보여주는 예입니다.

Example : Invite 이벤트

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

Example : Mention 이벤트

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

```
                                    },
        "EventTimestamp": "2019-04-04T21:30:43.181Z",
        "Message": "@botDisplayName@example.com Hello Chatbot"
    }
```

> **Note**
>
> Mention 이벤트에 대한 InboundHttpsEndpoint URL은 전송 2분 후에 만료됩니다.

Example : Remove 이벤트

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

Amazon Chime에 사용할 웹후크 생성

웹후크를 사용하면 웹 애플리케이션이 서로 실시간으로 통신할 수 있습니다. 일반적으로 웹후크는 작업이 발생할 때 알림을 보냅니다. 예를 들어, 온라인 쇼핑 사이트를 운영한다고 가정해 보겠습니다. 웹후크는 고객이 장바구니에 품목을 추가하거나, 주문 상품을 결제하거나, 의견을 전송할 경우 알림을 보낼 수 있습니다. 웹후크는 기존 애플리케이션만큼 많은 프로그래밍이 필요하지 않으며 처리 능력도 많이 사용하지 않습니다. 웹후크가 없으면 프로그램에서 데이터를 실시간으로 가져오기 위해 데이터를 자주 폴링해야 합니다. 웹후크가 있으면 전송 애플리케이션이 데이터를 즉시 게시합니다.

수신되는 웹후크는 프로그래밍 방식으로 Amazon Chime 채팅룸에 메시지를 전송합니다. 예를 들어 웹후크는 고객 서비스 팀에 우선순위가 높은 새로운 티켓이 생성된 것을 알리고 채팅룸에 해당 티켓에 대한 링크를 추가할 수 있습니다.

Webhook 메시지는 마크다운으로 서식 지정할 수 있으며 이모티콘을 포함할 수 있습니다. HTTP 링크와 이메일 주소는 활성 링크로 표시됩니다. 또한 메시지에 @All 및 @Present 주석을 포함시켜 모든 구성원과 현재 채팅룸 구성원에게 알림을 보낼 수 있습니다. 채팅룸 참가자를 직접 @mention하려면 별칭 또는 전체 이메일 주소를 사용하십시오. 예: `@alias` 또는 `@alias@domain.com`.

웹후크는 채팅룸에서만 사용할 수 있으며 공유할 수 없습니다. Amazon Chime 채팅룸 관리자는 각 채팅룸에 최대 10개의 웹후크를 추가할 수 있습니다.

웹후크를 생성한 후에는 다음 절차에 나온 것처럼 Amazon Chime 채팅룸에 웹후크를 통합할 수 있습니다.

웹후크를 채팅룸에 통합하려면

1. 채팅룸 관리자에게서 웹후크 URL을 얻습니다. 자세한 내용은 Amazon Chime 사용 설명서의 채팅룸에 웹후크 추가를 참조하세요.
2. 생성한 스크립트 또는 애플리케이션의 웹후크 URL을 사용하여 채팅룸에 메시지를 전송합니다.

   a. URL은 HTTP POST 요청을 수락합니다.

   b. Amazon Chime 웹후크는 JSON 페이로드와 단일 키 콘텐츠를 수락합니다. 다음은 curl 명령과 페이로드의 예입니다.

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/
json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
sample.com email test: marymajor@example.com All member callout: @All All
 Present member callout: @Present"}'
```

   다음은 Windows 사용자를 위한 예제 PowerShell 명령입니다.

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

외부 프로그램이 Webhook URL로 HTTP POST를 보내면 서버는 Webhook이 유효하며 할당된 채팅룸이 있는지 확인합니다. Webhook은 webhook 명단에 이름 옆에 있는 webhook 아이콘으로 표시됩니다. Webhook에 전송된 채팅룸 메시지는 (Webhook)라는 이름으로 채팅룸에 표시됩니다.

> **Note**
>
> CORS는 현재 Webhook에 대해 활성화되어 있지 않습니다.

웹후크 오류 해결

다음은 Webhook 관련 오류 목록입니다.

- 각 Webhook의 수신 Webhook 속도 한도는 채팅룸당 1TPS입니다. 조절(throttling)을 수행하면 HTTP 429 오류가 발생합니다.
- Webhook이 게시하는 메시지는 4KB 미만이어야 합니다. 메시지 페이로드가 이보다 크면 HTTP 413 오류가 발생합니다.
- @All and @Present 주석을 포함하는 Webhook에 의해 게시된 메시지는 멤버가 50명 이하인 채팅룸에서만 작동합니다. 멤버가 50명을 초과하면 HTTP 400 오류가 발생합니다.
- Webhook URL이 다시 생성된 경우 이전 URL을 사용하면 HTTP 404 오류가 발생합니다.
- 채팅룸의 Webhook URL이 삭제된 경우 이전 URL을 사용하면 HTTP 404 오류가 발생합니다.
- Webhook URL이 유효하지 않으면 HTTP 403 오류가 발생합니다.
- 서비스를 사용할 수 없는 경우 사용자는 응답에 HTTP 503 오류를 받습니다.

Amazon Chime에 대한 관리 지원

> **Note**
>
> 아마존 쇼핑 계정에 대한 도움이 필요하면 amazon.com의 고객 서비스로 이동하십시오.

Amazon Chime 지원 부서에 문의해야 하는 경우 다음 옵션 중 하나를 선택하십시오.

- AWS Support 계정이 있는 경우 Support 센터로 이동하여 티켓을 제출하세요.
- 그렇지 않으면 AWS Management Console을 열고 Amazon Chime, 지원, 요청 제출을 차례로 선택합니다.

다음 정보를 최대한 많이 제공하십시오.

- 문제에 대한 자세한 설명
- 문제가 발생한 시간과 해당 표준시간대
- 사용자의 Amazon Chime 버전. 버전 번호를 확인하려면 다음과 같이 합니다.
  - Windows에서 도움말, Amazon Chime 정보를 선택합니다.
  - macOS에서는 Amazon Chime, Amazon Chime 정보를 선택합니다.
  - iOS 및 Android에서는 설정, 정보를 선택합니다.
- 로그 참조 ID. 이 ID를 확인하려면 다음과 같이 합니다.
  - Windows 및 macOS에서 도움말, 진단 로그 전송을 선택합니다.
  - iOS 및 Android에서는 설정, 진단 로그 전송을 선택합니다.
- 회의와 관련된 문제인 경우 회의 ID

Amazon Chime의 보안

클라우드 AWS 보안은 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. Amazon Chime에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon Chime을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Amazon Chime을 구성하는 방법을 보여줍니다. 또한 Amazon Chime 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS AWS 서비스를 사용하는 방법도 배웁니다.

주제

- Amazon Chime의 인프라 보안
- Amazon Chime 자동 업데이트에 대한 이해

Amazon Chime용 Identity and Access Management

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 있도록 AWS 서비스 AWS 도와주는 도구입니다. IAM 관리자는 어떤 사용자가 Amazon Chime 리소스를 사용할 수 있도록 인증(로그인)되고 권한이 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리

고객

Amazon Chime에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 – Amazon Chime 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 다른 Amazon Chime 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Amazon Chime의 기능에 액세스할 수 없다면 Amazon Chime 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 – 회사에서 Amazon Chime 리소스를 책임지고 있다면 Amazon Chime에 대한 모든 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Amazon Chime 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Amazon Chime에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Chime에서 IAM을 사용하는 방법 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Amazon Chime에 대한 액세스 권한을 관리하는 정책을 작성하는 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Amazon Chime 자격 증명 기반 정책의 예제를 확인하려면 Amazon Chime 자격 증명 기반 정책 예제를 참조하세요. 섹션을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 Tasks that require root user credentials를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 자격 증명입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.
- 서비스 간 액세스 — 일부는 다른 기능을 사용합니다. AWS 서비스 AWS 서비스예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.

- 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

AWS Amazon Chime에 대한 관리형 정책

사용자, 그룹 또는 역할에 권한을 추가할 때 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더욱 편리합니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하려면 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이러한 정책은 일반적인 사용 사례에 적용되며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스가 새 기능을 지원하기 위해 AWS 관리형 정책에 권한을 추가하는 경우가 있습니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새 기능이 출시되거나 새 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스에서 새 기능을 시작하면 AWS (이)가 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하십시오.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.

- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

Amazon Chime에서 IAM을 사용하는 방법

IAM을 사용하여 Amazon Chime에 대한 액세스를 관리하기 전에 Amazon Chime에서 사용할 수 있는 IAM 기능을 이해해야 합니다. Amazon Chime 및 AWS 기타 서비스가 IAM과 연동되는 방식을 개괄적으로 살펴보려면 IAM 사용 설명서의 IAM과 연동되는 서비스를AWS 참조하십시오.

주제

- Amazon Chime 자격 증명 기반 정책
- 리소스
- 예

Amazon Chime 자격 증명 기반 정책

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. Amazon Chime은 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는

권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

조건 키

Amazon Chime은 서비스별 조건 키를 제공하지 않습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

리소스

Amazon Chime은 정책에서 리소스 ARN 지정을 지원하지 않습니다.

예

Amazon Chime 자격 증명 기반 정책 예제를 보려면 Amazon Chime 자격 증명 기반 정책 예제를 참조하세요. 섹션을 참조하세요.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티를 호출하여 작업을 수행하도록 하는 경우에 발생합니다. 이를 통해 악의적인 공격자는 실행 또는 액세스할 수 있는 권한이 없는 명령을 실행하거나 리소스를 수정할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 혼동된 대리자 문제를 참조하세요.

AWS에서는 크로스 서비스 사칭으로 인해 부정 시나리오가 혼동될 수 있습니다. 교차 서비스 가장은 한 서비스(직접적으로 호출하는 서비스)가 다른 서비스(직접적으로 호출되는 서비스)를 직접적으로 호출할 때 발생합니다. 악의적인 공격자는 호출 서비스를 활용해 평소에는 없는 권한을 사용하여 다른 서비스의 리소스를 변경할 수 있습니다.

AWS 서비스 주체에게 계정의 리소스에 대한 관리 액세스 권한을 제공하여 리소스의 보안을 보호하는 데 도움을 줍니다. 리소스 정책에는 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하는 것이 좋습니다. 이러한 키는 Amazon Chime이 해당 리소스에 대해 다른 서비스에 주는 권한을 제한합니다.

아래의 예제에서는 혼동된 대리인 문제를 방지하는 데 도움이 되는 `aws:SourceAccount` S3 버킷에 구성된 `CallDetailRecords` 전역 조건 컨텍스트 키를 사용하는 S3 버킷 정책을 보여줍니다.

```
{
```

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

Amazon Chime 리소스 기반 정책

Amazon Chime은 리소스 기반 정책을 지원하지 않습니다.

Amazon Chime 태그 기반 권한 부여

Amazon Chime은 리소스 태그 지정 또는 태그 기반 액세스 제어를 지원하지 않습니다.

Amazon Chime IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

Amazon Chime에서 임시 보안 인증 사용

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole또는 GetFederation토큰과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Amazon Chime은 임시 보안 인증을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 표시되며, 서비스가 해당 역할을 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

Amazon Chime은 서비스 연결 역할을 지원합니다. Amazon Chime 서비스 연결 역할 생성 또는 관리에 대한 자세한 정보는 Amazon Chime에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Amazon Chime은 서비스 역할을 지원하지 않습니다.

Amazon Chime 자격 증명 기반 정책 예제를 참조하세요.

기본적으로 IAM 사용자 및 역할은 Amazon Chime 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Amazon Chime 콘솔 사용

- 사용자에게 Amazon Chime에 대한 전체 액세스 권한 허용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 사용자가 사용자 관리 작업에 액세스하도록 허용
- AWS 관리형 정책: AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- 관리형 정책에 대한 AWS Amazon Chime 업데이트

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Amazon Chime 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하십시오.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하십시오.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하십시오.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

Amazon Chime 콘솔 사용

Amazon Chime 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한을 통해 계정의 Amazon Chime 리소스에 대한 세부 정보를 나열하고 볼 수 AWS 있어야 합니다. 최소 필수 권한보다 더 제한적인 보안 인증 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 엔티티가 Amazon Chime 콘솔을 계속 사용할 수 있도록 하려면 다음 AWS 관리형 AmazonChimeReadOnly정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

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

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자에게 Amazon Chime에 대한 전체 액세스 권한 허용

다음 AWS 관리형 AmazonChimeFullAccess정책은 IAM 사용자에게 Amazon Chime 리소스에 대한 전체 액세스 권한을 부여합니다. 이 정책은 모든 Amazon Chime 작업뿐만 아니라, Amazon Chime에서 사용자를 대신해 수행할 수 있어야 하는 다른 작업에 대한 액세스 권한을 사용자에게 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

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

```
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:CreateQueue"
            ],
            "Resource": [
                "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
            ]
        }
    ]
}
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS

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

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

사용자가 사용자 관리 작업에 액세스하도록 허용

AWS 관리형 AmazonChimeUserManagement정책을 사용하여 Amazon Chime 콘솔에서 사용자에게 사용자 관리 작업에 대한 액세스 권한을 부여합니다.

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

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

AWS 관리형 정책: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`는 이를 사용하여 Amazon Chime Voice Connector가 Amazon Kinesis Video Streams로 미디어를 스트리밍하고, 스트리밍 알림을 제공하고, Amazon Polly를 사용하여 음성을 합성할 수 있습니다. 이 정책은 고객의 Amazon Kinesis Video Streams에 액세스하고, Amazon Simple Notification Service 및 Amazon Simple Queue Service에 알림 이벤트를 전송하고, Amazon Chime SDK 음성 애플리케이션 `Speak` 및 `SpeakAndGetDigits` 작업을 사용할 때 Amazon Polly를 사용하여 음성을 합성할 수 있는 권한을 Amazon Chime Voice Connector 서비스에 부여합니다. 자세한 내용은 Amazon Chime SDK 관리자 안내서의 Amazon Chime SDK 자격 증명 기반 정책을 참조하세요.

관리형 정책에 대한 AWS Amazon Chime 업데이트

아래 표에는 Amazon Chime IAM 정책에 적용된 업데이트 목록 및 그에 대한 설명이 나열되어 있습니다.

변경 사항	설명	날짜
`AmazonChimeVoiceConnectorServiceLink`	Amazon Chime Voice Connector가 Amazon Polly를 사용하여 음성을 합성할 수 있	2022년 3월 15일

변경 사항	설명	날짜
edRolePolicy - 기존 정책에 대한 업데이트	는 새로운 권한을 추가했습니다. Amazon Chime SDK 음성 애플리케이션에서 Speak 및 SpeakAndGetDigits 작업을 사용하려면 이러한 권한이 필요합니다.	
AmazonChimeVoiceConnectorServiceLinkedRolePolicy -기존 정책 업데이트	Amazon Chime Voice Connector가 Amazon Kinesis Video Streams에 대한 액세스를 허용하고, SNS 및 SQS에 알림 이벤트를 전송할 수 있는 새로운 권한을 추가했습니다. 이러한 권한은 Amazon Chime Voice Connector가 Amazon Kinesis Video Streams로 미디어를 스트리밍하고 스트리밍 알림을 제공하려는 경우에 필요합니다.	2021년 12월 20일
기존 정책에 대한 변경 사항. Chime SDK 정책을 사용하여 IAM 사용자 또는 역할 생성.	Amazon Chime이 확장된 검증을 지원하기 위해 새로운 작업을 추가했습니다. 참석자 및 회의 리소스를 나열하고 태그를 지정하며, 회의 트랜스크립션을 시작 및 중지할 수 있는 여러 작업이 추가되었습니다.	2021년 9월 23일
Amazon Chime에서 변경 사항 추적 시작	Amazon Chime은 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 9월 23일

Amazon Chime 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Amazon Chime 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Amazon Chime에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사용자가 내 Amazon Chime 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Amazon Chime에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojacksonIAM 사용자가 콘솔을 사용하여 가상 *my-example-widget*리소스에 대한 세부 정보를 보려고 하지만 가상 chime:*GetWidget*권한이 없을 때 발생합니다.

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

이 경우 chime:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하십시오. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Amazon Chime에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 AWS 서비스 수 있는 기능도 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Amazon Chime에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사용자가 내 Amazon Chime 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- Amazon Chime에서 이러한 기능을 지원하는지 알아보려면 Amazon Chime에서 IAM을 사용하는 방법 섹션을 참조하세요.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Amazon Chime에 대해 서비스 연결 역할 사용

Amazon Chime은 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon Chime에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon Chime에서 사전 정의하며, 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Amazon Chime을 더 효율적으로 설정할 수 있습니다. Amazon Chime에서 서비스 연결 역할의 권한을 정의하므로 다르게

정의되지 않은 한, Amazon Chime만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 삭제할 수 없기 때문에 Amazon Chime 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스 단원을 참조하세요. 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

주제

공유 Alexa for Business 디바이스에서 역할 사용

다음 섹션의 정보에서는 서비스 연결 역할을 사용하고 Amazon Chime에 AWS 계정의 Alexa for Business 리소스에 대한 액세스 권한을 부여하는 방법을 설명합니다.

주제

Amazon Chime에 대한 서비스 연결 역할 권한

Amazon Chime은 AWSServiceRoleForAmazonChime이라는 서비스 연결 역할을 사용합니다. 이 역할은 Alexa for Business 공유 디바이스 같은 Amazon Chime에서 사용하거나 관리하는AWS 서비스 및 리소스에 액세스할 수 있도록 허용합니다.

AWSServiceRoleForAmazonChime 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- chime.amazonaws.com

역할 권한 정책은 Amazon Chime이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime에 대한 iam:CreateServiceLinkedRole

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Amazon Chime에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI, 또는 AWS API에서 Amazon Chime에 있는 공유 디바이스에 대해 Alexa for Business를 활성화할 경우, Amazon Chime에서는 서비스 연결 역할을 자동으로 생성합니다.

또한 IAM 콘솔을 사용해 Amazon Chime 사용 사례로 서비스 연결 역할을 생성할 수도 있습니다. AWS CLI 또는 AWS API에서 chime.amazonaws.com 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성을 참조하세요. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Amazon Chime에 대한 서비스 연결 역할 편집

Amazon Chime은 AWSServiceRoleForAmazonChime 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon Chime에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능이나 서비스가 더 이상 필요하지 않으면 그 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 연결 역할을 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제할 때 Amazon Chime이 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForAmazonChime(콘솔)에서 사용하는 Amazon Chime 리소스를 삭제하려면

- Amazon Chime 계정의 모든 공유 디바이스에 대해 Alexa for Business를 끕니다.
  a. https://chime.aws.amazon.com/에서 Amazon Chime 콘솔을 엽니다.
  b. 사용자, 공유 디바이스를 선택합니다.
  c. 디바이스를 선택합니다.
  d. [작업]을 선택합니다.
  e. Alexa for Business 비활성화를 선택합니다.

수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForAmazonChime 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

Amazon Chime 서비스 연결 역할에 대해 지원되는 리전

Amazon Chime은 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 Amazon Chime 엔드포인트 및 할당량을 참조하세요.

실시간 대화 기록을 통한 역할 사용

다음 섹션에서는 Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할을 생성하고 관리하는 방법을 설명합니다. 실시간 대화 기록 서비스에 대한 자세한 내용은 Amazon Chime SDK 실시간 대화 기록 사용을 참조하세요.

주제

- Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 권한
- Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 생성
- Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 편집
- Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 삭제

- Amazon Chime 서비스 연결 역할에 대해 지원되는 리전

Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 권한

Amazon Chime 실시간 대화 기록은 AWSServiceRoleForAmazonChimeTranscription이라는 서비스 연결 역할을 사용합니다. 이 서비스 연결 역할은 Amazon Chime이 사용자를 대신하여 Amazon Transcribe 및 Amazon Transcribe Medical에 액세스할 수 있도록 허용합니다.

AWSServiceRoleForAmazonChimeTranscription 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `transcription.chime.amazonaws.com`

역할 권한 정책은 Amazon Chime이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: `all AWS resources`에 대한 `transcribe:StartStreamTranscription`
- 작업: `all AWS resources`에 대한 `transcribe:StartMedicalStreamTranscription`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 생성

IAM 콘솔을 사용하여 실시간 대화 기록 사용 사례에서 서비스 연결 역할을 생성할 수 있습니다.

> **Note**
>
> 이 단계를 완료하려면 IAM 관리자 권한이 있어야 합니다. 그렇지 않은 경우 시스템 관리자에게 문의하세요.

역할 생성

1. AWS 관리 콘솔에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. AWS 서비스 역할 유형을 선택한 다음, Chime을 선택한 후 Chime 대화 기록을 선택합니다.
4. 다음을 선택합니다.

5. 다음을 선택합니다.
6. 필요에 따라 설명을 편집한 다음 역할 생성을 선택합니다.

AWS CLI 또는 AWS API를 사용하여 transcription.chime.amazonaws.com이라는 서비스 연결 역할을 생성할 수도 있습니다.

CLI에서 `aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com` 명령을 실행합니다.

자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성 섹션을 참조하세요. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 편집

Amazon Chime은 AWSServiceRoleForAmazonChimeTranscription 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할 설명을 편집할 수는 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon Chime 실시간 대화 기록에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForAmazonChimeTranscription 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

Amazon Chime 서비스 연결 역할에 대해 지원되는 리전

Amazon Chime은 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 Amazon Chime 엔드포인트 및 할당량 및 Amazon Chime SDK 미디어 리전 사용을 참조하세요.

Amazon Chime SDK 미디어 파이프라인과 함께 역할 사용

다음 섹션에서는 Amazon Chime SDK 미디어 파이프라인에 대한 서비스 연결 역할을 생성하고 관리하는 방법을 설명합니다.

주제

Amazon Chime SDK에 대한 서비스 연결 역할 권한

Amazon Chime은 AWSServiceRoleForAmazonChimeSDKMediaPipelines라는 서비스 연결 역할을 사용합니다. 이 역할은 Amazon Chime SDK 미디어 파이프라인이 사용자를 대신하여 Amazon Chime SDK 회의에 액세스할 수 있도록 허용합니다.

AWSServiceRoleForAmazonChimeSDKMediaPipelines 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `mediapipelines.chime.amazonaws.com`

역할은 Amazon Chime이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: `all AWS resources`에 대한 `chime:CreateAttendee`
- 작업: `all AWS resources`에 대한 `chime:DeleteAttendee`
- 작업: `all AWS resources`에 대한 `chime:GetMeeting`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

Amazon Chime SDK 미디어 파이프라인에 대한 서비스 연결 역할 생성

IAM 콘솔을 사용하여 Amazon Chime SDK 미디어 파이프라인*에서 사용할 수 있도록 서비스 연결 역할을 생성합니다.

> **Note**
>
> 이 단계를 완료하려면 IAM 관리자 권한이 있어야 합니다. 그렇지 않은 경우 시스템 관리자에게 문의하세요.

역할 생성

1. AWS 관리 콘솔에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. AWS 서비스 역할 유형을 선택한 다음 Chime을 선택하고 Chime SDK 미디어 파이프라인을 선택합니다.
4. 다음을 선택합니다.
5. 다음을 선택합니다.
6. 필요에 따라 설명을 편집한 다음 역할 생성을 선택합니다.

AWS CLI 또는 AWS API를 사용하여 mediapipelines.chime.amazonaws.com이라는 서비스 연결 역할을 생성할 수도 있습니다.

AWS CLI에서 `aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com` 명령을 실행합니다.

자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성 섹션을 참조하세요. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Amazon Chime SDK 미디어 파이프라인에 대한 서비스 연결 역할 편집

Amazon Chime은 AWSServiceRoleForAmazonChimeSDKMediaPipelines 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon Chime SDK 미디어 파이프라인에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForAmazonChimeSDKMediaPipelines 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

Amazon Chime SDK 미디어 파이프라인 서비스 연결 역할에 대해 지원되는 리전

Amazon Chime SDK는 서비스가 사용 가능한 모든 AWS 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 Amazon Chime 엔드포인트 및 할당량을 참조하세요.

Amazon Chime의 로깅 및 모니터링

Amazon Chime 및 다른 AWS 솔루션의 안정성, 가용성, 성능을 유지하려면 모니터링이 중요합니다. AWS는 Amazon Chime을 모니터링하고, 문제를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 도구를 제공합니다.

- Amazon CloudWatch는 AWS에서 실행하는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.
- Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. EventBridge는 자동화된 이벤트 중심 컴퓨팅을 지원합니다. 특정 이벤트를 감시하는 규칙을 작성하고 이러한 이벤트가 발생할 때 다른 AWS 서비스에서 자동화된 작업을 트리거할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.
- Amazon CloudWatch Logs로 Amazon EC2 인스턴스, CloudTrail, 기타 소스의 로그 파일을 모니터링, 저장, 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임계값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.
- AWS CloudTrail은 AWS 계정에서 또는 이 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처합니다. 그리고 나서 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- Amazon CloudWatch를 사용한 Amazon Chime 모니터링
- EventBridge를 통한 Amazon Chime 자동화
- AWS CloudTrail을 사용하여 Amazon Chime API 호출 로깅

Amazon CloudWatch를 사용한 Amazon Chime 모니터링

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 Amazon Chime을 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

Amazon Chime의 CloudWatch 지표

Amazon Chime은 CloudWatch에 다음 지표를 전송합니다.

AWS 계정 및 Amazon Chime Voice Connector에 할당된 전화번호에 대해 다음과 같은 지표가 `AWS/ChimeVoiceConnector` 네임스페이스에 포함됩니다.

지표	설명
`InboundCallAttempts`	시도한 인바운드 통화 수입니다. 단위: 개수
`InboundCallFailures`	인바운드 통화 실패 수입니다. 단위: 개수
`InboundCallsAnswered`	응답된 인바운드 통화 수입니다. 단위: 개수
`InboundCallsActive`	현재 활성 상태인 인바운드 통화 수입니다. 단위: 개수
`OutboundCallAttempts`	시도한 아웃바운드 통화 수입니다. 단위: 개수
`OutboundCallFailures`	아웃바운드 통화 실패 수입니다. 단위: 개수
`OutboundCallsAnswered`	응답된 아웃바운드 통화 수입니다.

지표	설명
	단위: 개수
OutboundCallsActive	현재 활성화된 아웃바운드 통화 수입니다. 단위: 개수
Throttles	전화를 걸려고 할 때 계정에 스로틀이 발생한 수입니다. 단위: 개수
Sip1xxCodes	1xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수
Sip2xxCodes	2xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수
Sip3xxCodes	3xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수
Sip4xxCodes	4xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수
Sip5xxCodes	5xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수
Sip6xxCodes	6xx 레벨 상태 코드가 있는 SIP 메시지 수입니다. 단위: 개수

지표	설명
CustomerToVcRtpPackets	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 RTP 패킷의 수입니다. 단위: 개수
CustomerToVcRtpBytes	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTP 패킷 단위)입니다. 단위: 개수
CustomerToVcRtcpPackets	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 RTCP 패킷의 수입니다. 단위: 개수
CustomerToVcRtcpBytes	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTCP 패킷 단위)입니다. 단위: 개수
CustomerToVcPacketsLost	고객으로부터 Amazon Chime Voice Connector 인프라로 전송되는 동안 손실된 패킷의 수입니다. 단위: 개수
CustomerToVcJitter	고객으로부터 Amazon Chime Voice Connector 인프라로 전송되는 패킷의 평균 지터입니다. 단위: 밀리초
VcToCustomerRtpPackets	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 RTP 패킷의 수입니다. 단위: 개수

지표	설명
VcToCustomerRtpBytes	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 바이트 수(RTP 패킷 단위)입니다. 단위: 개수
VcToCustomerRtcpPackets	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 RTCP 패킷의 수입니다. 단위: 개수
VcToCustomerRtcpBytes	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 바이트 수(RTCP 패킷 단위)입니다. 단위: 개수
VcToCustomerPacketsLost	Amazon Chime Voice Connector 인프라로부터 고객으로 전송되는 동안 손실된 패킷의 수입니다. 단위: 개수
VcToCustomerJitter	Amazon Chime Voice Connector 인프라로부터 고객으로 전송되는 패킷의 평균 지터입니다. 단위: 밀리초
RTTBetweenVcAndCustomer	고객과 Amazon Chime Voice Connector 인프라 간의 평균 왕복 시간입니다. 단위: 밀리초

지표	설명
MOSBetweenVcAndCustomer	고객과 Amazon Chime Voice Connector 인프라 간의 음성 스트림과 관련된 예상 MOS(평균 평가점)입니다. 단위: 1.0-4.4의 점수. 점수가 높을수록 오디오 음질이 뛰어납니다.
RemoteToVcRtpPackets	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 RTP 패킷의 수입니다. 단위: 개수
RemoteToVcRtpBytes	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTP 패킷 단위)입니다. 단위: 개수
RemoteToVcRtcpPackets	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 RTCP 패킷의 수입니다. 단위: 개수
RemoteToVcRtcpBytes	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTCP 패킷 단위)입니다. 단위: 개수
RemoteToVcPacketsLost	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송되는 동안 손실된 패킷의 수입니다. 단위: 개수

지표	설명
RemoteToVcJitter	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송되는 패킷의 평균 지터입니다. 단위: 밀리초
VcToRemoteRtpPackets	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 RTP 패킷의 수입니다. 단위: 개수
VcToRemoteRtpBytes	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 바이트 수(RTP 패킷 단위)입니다. 단위: 개수
VcToRemoteRtcpPackets	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 RTCP 패킷의 수입니다. 단위: 개수
VcToRemoteRtcpBytes	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 바이트 수(RTCP 패킷 단위)입니다. 단위: 개수
VcToRemotePacketsLost	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송되는 동안 손실된 패킷의 수입니다. 단위: 개수
VcToRemoteJitter	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송되는 패킷의 평균 지터입니다. 단위: 밀리초

지표	설명
RTTBetweenVcAndRemote	원격 엔드와 Amazon Chime Voice Connector 인프라 간의 평균 왕복 시간입니다. 단위: 밀리초
MOSBetweenVcAndRemote	원격 엔드와 Amazon Chime Voice Connector 인프라 간의 음성 스트림과 관련된 예상 MOS(평균 평가점)입니다. 단위: 단위: 1.0~4.4의 점수. 점수가 높을수록 오디오 음질이 뛰어납니다.

Amazon Chime에 사용되는 CloudWatch 차원

Amazon Chime과 사용할 수 있는 CloudWatch 차원은 다음과 같습니다.

차원	설명
VoiceConnectorId	지표를 표시할 Amazon Chime Voice Connector의 식별자입니다.
Region	이벤트와 연관된 AWS 지역입니다.

Amazon Chime에 사용되는 CloudWatch Logs

Amazon Chime Voice Connector 지표를 CloudWatch Logs로 전송할 수 있습니다. 자세한 내용은 Amazon Chime SDK 관리 안내서의 Amazon Chime Voice Connector 설정 편집을 참조하세요.

미디어 품질 메트릭 로그

Amazon Chime Voice Connector에 대한 미디어 품질 지표 로그를 수신하도록 선택할 수 있습니다. 이를 선택하면 Amazon Chime에서는 사용자를 위해 생성된 CloudWatch Logs 로그 그룹에 대한 모든 Amazon Chime Voice Connector 통화의 상세한 1분당 지표를 전송합니다. 로그 그룹 이름은 /aws/ChimeVoiceConnectorLogs/${*VoiceConnectorID*}입니다. 로그에 다음과 같은 필드가 JSON 형식으로 포함됩니다.

필드	설명
voice_connector_id	통화를 전달하는 Amazon Chime Voice Connector ID입니다.
event_timestamp	UTC 기준 메트릭이 UTC Epoch(1970년 1월 1일 자정) 이후 밀리초 단위로 내보냈을 때 시간입니다.
call_id	거래 ID에 해당합니다.
from_sip_user	호출하는 시작 사용자입니다.
from_country	호출하는 시작 국가입니다.
to_sip_user	호출하는 수신 사용자입니다.
to_country	호출하는 수신 국가입니다.
endpoint_id	호출의 다른 엔드포인트를 나타내는 불투명 식별자입니다. CloudWatch Logs Insights와 함께 사용합니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 CloudWatch Logs Insights를 사용한 로그 데이터 분석을 참조하세요.
aws_region	호출하는 AWS 리전입니다.
cust2vc_rtp_packets	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 RTP 패킷의 수입니다.
cust2vc_rtp_bytes	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTP 패킷 단위)입니다.
cust2vc_rtcp_packets	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 RTCP 패킷의 수입니다.

필드	설명
cust2vc_rtcp_bytes	고객으로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTCP 패킷 단위)입니다.
cust2vc_packets_lost	고객으로부터 Amazon Chime Voice Connector 인프라로 전송되는 동안 손실된 패킷의 수입니다.
cust2vc_jitter	고객으로부터 Amazon Chime Voice Connector 인프라로 전송되는 패킷의 평균 지터입니다.
vc2cust_rtp_packets	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 RTP 패킷의 수입니다.
vc2cust_rtp_bytes	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 바이트 수(RTP 패킷 단위)입니다.
vc2cust_rtcp_packets	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 RTCP 패킷의 수입니다.
vc2cust_rtcp_bytes	Amazon Chime Voice Connector 인프라로부터 고객으로 전송된 바이트 수(RTCP 패킷 단위)입니다.
vc2cust_packets_lost	Amazon Chime Voice Connector 인프라로부터 고객으로 전송되는 동안 손실된 패킷의 수입니다.
vc2cust_jitter	Amazon Chime Voice Connector 인프라로부터 고객으로 전송되는 패킷의 평균 지터입니다.
rtt_btwn_vc_and_cust	고객과 Amazon Chime Voice Connector 인프라 간의 평균 왕복 시간입니다.

필드	설명
mos_btwn_vc_and_cust	고객과 Amazon Chime Voice Connector 인프라 간의 음성 스트림과 관련된 예상 MOS(평균 평가점)입니다.
rem2vc_rtp_packets	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 RTP 패킷의 수입니다.
rem2vc_rtp_bytes	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTP 패킷 단위)입니다.
rem2vc_rtcp_packets	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 RTCP 패킷의 수입니다.
rem2vc_rtcp_bytes	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송된 바이트 수(RTCP 패킷 단위)입니다.
rem2vc_packets_lost	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송되는 동안 손실된 패킷의 수입니다.
rem2vc_jitter	원격 엔드로부터 Amazon Chime Voice Connector 인프라로 전송되는 패킷의 평균 지터입니다.
vc2rem_rtp_packets	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 RTP 패킷의 수입니다.
vc2rem_rtp_bytes	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 바이트 수(RTP 패킷 단위)입니다.
vc2rem_rtcp_packets	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 RTCP 패킷의 수입니다.

필드	설명
vc2rem_rtcp_bytes	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송된 바이트 수(RTCP 패킷 단위)입니다.
vc2rem_packets_lost	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송되는 동안 손실된 패킷의 수입니다.
vc2rem_jitter	Amazon Chime Voice Connector 인프라로부터 원격 엔드로 전송되는 패킷의 평균 지터입니다.
rtt_btwn_vc_and_rem	원격 엔드와 Amazon Chime Voice Connector 인프라 간의 평균 왕복 시간입니다.
mos_btwn_vc_and_rem	원격 엔드와 Amazon Chime Voice Connector 인프라 간의 음성 스트림과 관련된 예상 MOS(평균 평가점)입니다.

SIP 메시지 로그

Amazon Chime Voice Connector에 대한 SIP 메시지 로그를 수신하도록 선택할 수 있습니다. 메시지 로그를 수신하면 Amazon Chime에서는 인바운드 및 아웃바운드 SIP 메시지를 캡처한 후 생성된 CloudWatch Logs 로그 그룹에 이를 전송합니다. 로그 그룹 이름은 `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`입니다. 로그에 다음과 같은 필드가 JSON 형식으로 포함됩니다.

필드	설명
voice_connector_id	Amazon Chime Voice Connector ID입니다..
aws_region	이벤트와 연관된 AWS 지역입니다.
event_timestamp	UTC 기준 UNIX Epoch(1970년 1월 1일 자정) 이후 밀리초 단위로 표기되는 메시지가 캡처된 시간입니다.

필드	설명
call_id	Amazon Chime Voice Connector 통화 ID입니다.
sip_message	캡처된 전체 SIP 메시지입니다.

EventBridge를 통한 Amazon Chime 자동화

Amazon EventBridge를 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제나 리소스 변경 같은 시스템 이벤트에 자동으로 대응할 수 있습니다. 회의 이벤트에 대한 자세한 내용은 Amazon Chime 개발자 안내서의 회의 이벤트를 참조하세요.

Amazon Chime에서는 이벤트가 생성되면 최선의 작업 전달을 위해 EventBridge에 해당 이벤트를 전송합니다. 이는 Amazon Chime에서는 모든 이벤트를 EventBridge에 전송하려고 시도하지만, 드물게 이벤트가 전달되지 않는 경우가 발생할 수 있음을 뜻합니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 AWS 서비스의 이벤트를 참조하세요.

> **Note**
>
> 데이터를 암호화해야 하는 경우 Amazon S3 관리형 키를 사용해야 합니다. AWS Key Management Service에 저장된 고객 마스터 키를 사용하는 서버 측 암호화는 지원하지 않습니다.

EventBridge를 사용하여 Amazon Chime Voice Connector 자동화

Amazon Chime Voice Connector에 대해 자동으로 트리거할 수 있는 작업은 다음과 같습니다.

- AWS Lambda 함수 호출
- Amazon Elastic Container Service 태스크 시작
- Amazon Kinesis Video Streams로 이벤트 릴레이
- AWS Step Functions 상태 머신 활성화
- Amazon SNS 주제 또는 Amazon SQS 대기열 알림

다음은 EventBridge를 Amazon Chime Voice Connector에 사용하는 몇 가지 예입니다.

- Lambda 함수를 활성화하여 통화 종료 후 통화 오디오를 다운로드합니다.
- Amazon ECS 태스크를 시작하여 통화 시작 후 실시간 트랜스크립션을 활성화합니다.

자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.

Amazon Chime Voice Connector 스트리밍 이벤트

Amazon Chime Voice Connector는 이 섹션에 설명된 이벤트가 발생할 경우 EventBridge에 이벤트 전송을 지원합니다.

Amazon Chime Voice Connector 스트리밍 시작

Amazon Chime Voice Connector는 Kinesis Video Streams로 미디어 스트리밍이 시작될 때 이 이벤트를 전송합니다.

Example 이벤트 데이터

다음은 이 이벤트의 예제 데이터입니다.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "direction": "Outbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>;",
            "content-type": "application/sdp",
            "content-length": "246"
        },
```

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

Amazon Chime Voice Connector 스트리밍 종료

Amazon Chime Voice Connector는 Kinesis Video Streams로 미디어 스트리밍이 종료될 때 이 이벤트를 전송합니다.

Example 이벤트 데이터

다음은 이 이벤트의 예제 데이터입니다.

```
{
    "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"
    }
}
```

Amazon Chime Voice Connector 스트리밍 업데이트

Amazon Chime Voice Connector는 Kinesis Video Streams로 미디어 스트리밍이 업데이트될 때 이 이벤트를 전송합니다.

Example 이벤트 데이터

다음은 이 이벤트의 예제 데이터입니다.

```
{
    "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"
    }
}
```

Amazon Chime Voice Connector 스트리밍 실패

Amazon Chime Voice Connector는 Kinesis Video Streams로 미디어 스트리밍이 실패할 때 이 이벤트를 전송합니다.

Example 이벤트 데이터

다음은 이 이벤트의 예제 데이터입니다.

```
{
  "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"
    }
}
```

AWS CloudTrail을 사용하여 Amazon Chime API 호출 로깅

Amazon Chime은 Amazon Chime에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Amazon Chime 콘솔의 호출과 Amazon Chime API에 대한 코드 호출을 포함하여, Amazon Chime에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면 Amazon Chime 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon Chime에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Amazon Chime 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. API 호출이 Amazon Chime 관리 콘솔에서 수행되면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트 로그에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amazon Chime에 대한 이벤트를 포함하여 AWS 계정의 이벤트의 지속적인 레코드의 경우, 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성

- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 Amazon Chime 작업은 CloudTrail에서 로깅되며 Amazon Chime API 참조에 설명되어 있습니다. 예를 들어 `CreateAccount`, `InviteUsers`, `ResetPersonalPIN` 섹션을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다. 모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 IAM 사용자 보안 인증 정보로 했는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청했는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Amazon Chime 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함하고 있습니다. CloudTrail 로그 파일은 퍼블릭 API 호출에 대한 순서 지정된 스택 추적이 아니기 때문에 특정 순서로 표시되지 않습니다.

Amazon Chime에 대한 항목은 chime.amazonaws.com 이벤트 소스로 식별됩니다.

해당 Amazon Chime 계정에 대해 Active Directory를 구성한 경우 CloudTrail을 사용하여 AWS Directory Service API 호출 로깅 섹션을 참조하세요. 여기에서는 Amazon Chime 사용자의 로그인 기능에 영향을 줄 수 있는 문제를 모니터링하는 방법을 설명합니다.

다음 예제는 Amazon Chime에 대한 CloudTrail 로그 항목을 표시합니다.

```
{"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"
       }
```


Amazon Chime에 대한 규정 준수 검증

제3자 감사자는 SOC, PCI, FedRAMP, HIPAA와 같은 여러 AWS 규정 준수 프로그램의 일환으로 AWS 서비스의 보안 및 규정 준수를 평가합니다.

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의 범위별 범위 내 규정 준수 프로그램별 규정을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon Chime의 복원력

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복

성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

Amazon Chime은 AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 다양한 기능을 제공합니다. 자세한 내용은 Amazon Chime SDK 관리자 안내서의 Amazon Chime Voice Connector 그룹 관리 및 Amazon Chime Voice Connector 미디어를 Kinesis로 스트리밍을 참조하세요.

Amazon Chime의 인프라 보안

관리형 서비스인 Amazon Chime은 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amazon Chime 자동 업데이트에 대한 이해

Amazon Chime은 클라이언트를 업데이트하는 다양한 방법을 제공합니다. Amazon Chime을 브라우저에서 실행하는지, 데스크톱에서 실행하는지, 모바일 장치에서 실행하는지에 따라 방법이 달라집니다.

Amazon Chime 웹 애플리케이션(https://app.chime.aws)은 항상 최신 기능 및 보안 수정 사항과 함께 로드됩니다.

Amazon Chime 데스크톱 클라이언트는 사용자가 종료 또는 로그아웃을 선택할 때마다 업데이트가 있는지 확인합니다. 이는 Windows 및 macOS 시스템에 적용됩니다. 사용자가 클라이언트를 실행하면 3시간마다 업데이트가 있는지 확인합니다. 사용자는 Windows 도움말 메뉴 또는 macOS Amazon Chime 메뉴에서 업데이트 확인을 선택하여 업데이트가 있는지 확인할 수도 있습니다.

데스크톱 클라이언트가 업데이트를 감지하면 Amazon Chime에서는 사용자에게 업데이트를 설치하라는 메시지를 표시합니다. 단, 회의가 진행 중인 경우는 예외입니다. 회의가 진행 중인 경우는 다음과 같습니다.

- 사용자가 회의에 참석 중인 경우.
- 아직 진행 중인 회의에 초대된 경우.

Amazon Chime에 최신 버전을 설치하라는 메시지가 표시되며, 설치를 연기할 수 있도록 15초 카운트다운이 제공됩니다. 사용자는 나중에 다시 시도를 선택합니다.

사용자가 업데이트를 연기했고 진행 중인 회의에 참석하고 있지 않은 경우, 클라이언트에서는 3시간 후에 업데이트를 확인하고 설치하라는 메시지를 다시 표시합니다. 카운트다운이 끝나면 설치가 시작됩니다.

> **Note**
>
> macOS 시스템에서는 사용자가 지금 다시 시작을 선택하여 업데이트를 시작해야 합니다.

모바일 디바이스에서 - Amazon Chime 모바일 애플리케이션은 App Store 및 Google Play에서 제공하는 업데이트 옵션을 사용하여 Amazon Chime 클라이언트의 최신 버전을 제공합니다. 모바일 디바이스 관리 시스템을 통해 업데이트를 배포할 수도 있습니다. 이번 주제에서는 여러분이 방법을 알고 있다는 것을 전제로 합니다.

Amazon Chime 문서 기록

다음 표에서는 2018년 3월을 시작으로 Amazon Chime 관리자 안내서에 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
Amazon Chime SDK 관리 안내서 게시	이제 Amazon Chime SDK 주제가 Amazon Chime SDK 관리 안내서에 게시되었습니다. 자세한 내용은 Amazon Chime 관리 안내서를 참조하세요.	2022년 3월 24일
IAM 정책 업데이트	에서 관리하는 IAM 정책의 변경 AWS 사항은 이제 이 관리자 안내서에서 추적됩니다. Amazon Chime 자격 증명 기반 정책 예시를 참조하세요.	2021년 9월 23일
서비스 연결 역할	이제 관리자는 Amazon Live Transcription에 대한 서비스 연결 역할을 생성할 수 있으며, Amazon Chime 실시간 대화 기록 작업이 시작 및 종료될 때 이벤트 메시지를 볼 수 있습니다. 자세한 내용은 실시간 트랜스크립션을 통한 역할 사용 및 이벤트를 통한 Amazon CloudWatch Chime 자동화를 참조하십시오.	2021년 8월 12일
SIP 미디어 애플리케이션 및 규칙	관리자는 Amazon Chime 음성 커넥터 AWS Lambda 및 기능과 함께 사용할 SIP 미디어 애플리케이션 및 규칙을 만들 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서	2020년 11월 18일

	의 SIP 애플리케이션 및 규칙 관리를 참조하십시오.	
Amazon Chime Voice Connector 긴급 통화 라우팅 번호	Amazon Chime 관리자는 Amazon Chime Voice Connector에 대한 긴급 통화 라우팅 번호를 설정할 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Amazon Chime 음성 커넥터에 대한 긴급 통화 라우팅 번호 설정을 참조하십시오.	2020년 7월 1일
Dolby Voice Huddle에서 Amazon Chime	Amazon Chime은 Dolby Voice Huddle 오디오 및 비디오 회의 하드웨어에 관계자 회의 환경을 제공합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Dolby 하드웨어에 Amazon Chime 설정을 참조하십시오.	2020년 6월 3일
채팅 보존 정책 설정	Amazon Chime 관리자는 엔터프라이즈 계정에 대한 채팅 보존 정책을 설정할 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 채팅 보존 정책 관리를 참조하십시오.	2020년 5월 21일
채팅 메시지 제거	프로그래밍할 수 있는 경우 Amazon Chime API 쌍을 사용하여 계정의 채팅방 및 대화에서 메시지를 제거할 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 개별 메시지 삭제를 참조하십시오.	2020년 5월 18일

CloudWatch Amazon Chime 보이스 커넥터의 미디어 품질 메트릭	Amazon Chime은 Amazon Chime 음성 커넥터에 대한 미디어 품질 지표 전송을 지원합니다. CloudWatch 자세한 내용은 Amazon Chime 관리자 안내서의 를 사용하여 CloudWatch Amazon Chime 모니터링을 참조하십시오.	2020년 1월 23일
Amazon Chime Meetings App for Slack	Amazon Chime은 Amazon Chime Meetings App for Slack을 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Slack용 Amazon Chime 미팅 앱 설정을 참조하십시오.	2019년 12월 4일
회의 리전 설정	Amazon Chime은 모든 참가자를 위한 최적의 AWS 지역에서의 회의 처리를 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 회의 지역 설정을 참조하십시오.	2019년 12월 3일
SIP 기반 미디어 레코딩 (SIPREC) 호환성	Amazon Chime Voice Connector는 SIPREC 호환 음성 인프라에서 Kinesis Video Streams로 미디어 스트리밍을 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 SIP 기반 미디어 녹화 (SIPREC) 호환성을 참조하십시오.	2019년 11월 25일

Dolby Voice Room에서 Amazon Chime	사용자가 회의에 편하게 참여하기를 원하는 경우 Amazon Chime은 Dolby Voice Room 오디오 및 비디오 회의 하드웨어에 관계자 회의 환경을 제공합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Dolby Voice Room에 Amazon Chime 설정을 참조하십시오.	2019년 10월 29일
발신 통화 이름 업데이트	Amazon Chime 인벤토리에 있는 전화번호를 사용하여 건 발신 통화의 수신자에게 표시되는 기본 통화 이름을 설정합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 아웃바운드 전화 이름 업데이트를 참조하십시오.	2019년 10월 24일
Amazon Kinesis로 미디어 스트리밍	분석, 기계 학습 및 그 밖의 처리를 위해 Amazon Chime Voice Connector에서 Kinesis Video Streams로 전화 통화 오디오를 스트리밍합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Amazon Chime 음성 커넥터 미디어를 Kinesis로 스트리밍하고 Amazon Chime 음성 커넥터 서비스 연결 역할 사용을 참조하십시오.	2019년 10월 24일

아마존을 통한 아마존 Chime 모니터링 CloudWatch	원시 데이터를 수집하여 읽기 쉬운 거의 CloudWatch 실시간 지표로 처리하는 기능을 사용하여 Amazon Chime을 모니터링합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 를 사용하여 CloudWatch Amazon Chime 모니터링을 참조하십시오.	2019년 10월 24일
Amazon Chime Voice Connector 그룹	여러 지역에서 만든 Amazon Chime 음성 커넥터를 포함하는 Amazon Chime 음성 커넥터 그룹을 생성하십시오. AWS 그러면 수신 통화가 리전 간에 장애 조치를 수행할 수 있으며 가용성 이벤트가 발생할 경우 대체할 내결함성 메커니즘이 생성됩니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Amazon Chime 음성 커넥터 그룹 사용을 참조하십시오.	2019년 10월 24일
네트워크 구성 업데이트	Amazon Chime의 방화벽 요구 사항이 간소화되고 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 네트워크 구성 및 대역폭 요구 사항을 참조하십시오.	2019년 9월 6일
중재 회의	Amazon Chime은 중재 회의를 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 조정된 회의 참여를 참조하십시오.	2019년 7월 25일

Amazon Chime에 대한 규정 준수 검증	Amazon Chime은 HIPAA 적격 서비스입니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Amazon Chime에 대한 규정 준수 검증을 참조하세요.	2019년 6월 11일
수신자 부담 전화번호 이식	Amazon Chime은 Amazon Chime Voice Connector에 사용할 수 있도록 수신자 부담 미국 전화번호 이식을 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 기존 전화번호 포팅을 참조하십시오.	2019년 5월 28일
Amazon Chime에서 전화번호 관리	Amazon Chime Business Calling을 사용하여 전화번호를 프로비저닝하고 Amazon Chime 사용자에게 전화번호를 할당할 수 있습니다. Amazon Chime Voice Connector를 기존 전화 시스템과 통합합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Amazon Chime에서 전화번호 관리를 참조하세요.	2019년 3월 18일

Outlook용 Amazon Chime 추가	Amazon Chime은 두 가지 Microsoft Outlook용 추가 기능, 즉 Windows용 Outlook용 Amazon Chime 추가 기능과 Outlook용 Amazon Chime 추가 기능을 제공합니다. 이러한 추가 기능은 동일한 예약 기능을 제공하지만, 다른 유형의 사용자를 지원합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Outlook용 추가 기능 배포를 참조하십시오.	2019년 3월 12일
다양한 업데이트	주제 레이아웃과 조직에 대한 다양한 업데이트입니다.	2019년 2월 11일
Amazon Chime 내게 전화 걸기 기능	관리자는 회의 설정에서 Amazon Chime 내게 전화 걸기 기능을 활성화할 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 회의 설정 관리를 참조하십시오.	2018년 8월 22일
Okta SSO 연결	엔터프라이즈 계정이 있는 경우 Okta SSO에 연결하여 사용자 권한을 인증하고 할당할 수 있습니다. 자세한 내용은 Amazon Chime 관리자 안내서의 Okta SSO에 연결 섹션을 참조하십시오.	2018년 8월 1일
사용자 첨부 파일 요청	사용자별로 Amazon Chime에 업로드된 첨부 파일을 수신합니다. 자세한 내용은 Amazon Chime 관리자 안내서의 사용자 첨부 파일 요청을 참조하십시오.	2018년 4월 23일

추가 보고서 데이터 보기	추가 보고서 데이터를 봅니다. 자세한 내용은 Amazon Chime 관리자 안내서의 보고서 보기를 참조하십시오.	2018년 3월 30일
사용자에게 프로 또는 기본 권한 할당	사용자에게 프로 또는 기본 권한 할당. 자세한 내용은 Amazon Chime 관리자 안내서의 사용자 액세스 및 권한 관리를 참조하십시오.	2018년 3월 29일