aws

Panduan Administrasi

Amazon Chime

Amazon Chime: Panduan Administrasi

Table of Contents

Anda harus menjadi administrator sistem Amazon Chime untuk menyelesaikan langkah-langkah dalam panduan ini. Jika Anda memerlukan bantuan dengan klien desktop Amazon Chime, aplikasi web, atau aplikasi seluler, lihat Mendapatkan dukungan di Panduan Pengguna Amazon Chime.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu Amazon Chime?

Amazon Chime adalah layanan komunikasi yang mengubah rapat online dengan aplikasi yang aman dan komprehensif. Amazon Chime berfungsi di seluruh perangkat Anda sehingga Anda dapat tetap terhubung. Anda dapat menggunakan Amazon Chime untuk rapat online, konferensi video, panggilan, dan obrolan. Anda juga dapat membagikan konten di dalam dan di luar organisasi Anda. Amazon Chime adalah layanan yang dikelola sepenuhnya yang berjalan dengan aman diAWS cloud, yang membebaskan TI dari penerapan dan pengelolaan infrastruktur yang kompleks.

Untuk informasi lebih lanjut, lihat Amazon Chime.

Gambaran Umum Administrasi

Sebagai administrator, Anda menggunakan konsol Amazon Chime untuk melakukan tugas-tugas utama, seperti membuat akun Amazon Chime dan mengelola pengguna dan izin. Untuk mengakses konsol Amazon Chime dan membuat akun administrator Amazon Chime, buatAWS akun terlebih dahulu. Untuk informasi lebih lanjut, lihat Prasyarat untuk administrator sistem Amazon Chime.

Cara memulai

Setelah Anda menyelesaikanPrasyarat untuk administrator sistem Amazon Chime, Anda dapat membuat dan mengkonfigurasi akun administratif Amazon Chime Anda, lalu menambahkan pengguna ke dalamnya. Pilih izin Pro atau Dasar untuk pengguna Anda.

Saat Anda siap memulai sekarang, lihat tutorial berikut:

- Mulai

Untuk informasi lebih lanjut tentang izin dan akses pengguna, lihatMengelola izin dan akses pengguna. Untuk informasi selengkapnya tentang fitur yang dapat diakses pengguna dengan izin Pro dan Dasar, lihat Paket dan harga.

Harga

Amazon Chime menyediakan harga berbasis penggunaan. Anda hanya membayar untuk pengguna dengan izin Pro yang menyelenggarakan rapat, dan hanya pada hari-hari pertemuan tersebut diselenggarakan. Peserta rapat dan pengguna obrolan tidak dikenakan biaya.

Tidak ada biaya untuk pengguna dengan izin Dasar. Pengguna dasar tidak dapat menyelenggarakan rapat, tetapi mereka dapat menghadiri rapat dan menggunakan obrolan. Untuk informasi selengkapnya tentang harga dan fitur yang dapat diakses pengguna dengan izin Pro dan Dasar, lihat Paket dan harga.

Sumber daya

Untuk informasi selengkapnya tentang Amazon Chime, lihat sumber daya berikut:

- Pusat Bantuan Amazon Chime
- Video Pelatihan Amazon Chime

Prasyarat untuk administrator sistem Amazon Chime

Anda harus memiliki AWS akun untuk mengakses konsol Amazon Chime dan membuat akun administrator Amazon Chime.

Membuat akun Amazon Web Services

Sebelum Anda dapat membuat akun administrator untuk Amazon Chime, Anda harus terlebih dahulu membuat AWS akun. lonceng

Topik

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Untuk informasi selengkapnya tentang pengaturan akun administrator Amazon Chime, lihat. Mulai

Mulai

Cara termudah bagi pengguna Anda untuk memulai Amazon Chime adalah mengunduh dan menggunakan versi Amazon Chime Pro secara gratis selama 30 hari. Untuk informasi selengkapnya, lihat Mengunduh Amazon Chime Chime.

Membeli Amazon Chime Chime

Untuk terus menggunakan versi Amazon Chime Pro setelah masa uji coba gratis 30 hari, Anda harus membuat akun administrator Amazon Chime dan menambahkan pengguna Anda ke dalamnya. Untuk memulai, Anda harus terlebih dahulu menyelesaikanPrasyarat untuk administrator sistem Amazon Chime, yang meliputi membuatAWS account. Kemudian, Anda dapat membuat dan mengkonfigurasi akun administrator Amazon Chime dan menambahkan pengguna ke dalamnya dengan menyelesaikan tugas-tugas berikut.

Tugas

- Langkah 1: Membuat akun administrator Amazon Chime
- Langkah 2 (opsional): Mengkonfigurasi pengaturan akun
- Langkah 3: Menambahkan pengguna ke akun Anda
- (Opsional) Menyiapkan nomor telepon untuk akun Amazon Chime Anda

Langkah 1: Membuat akun administrator Amazon Chime

Setelah Anda menyelesaikanPrasyarat untuk administrator sistem Amazon Chime, Anda dapat membuat akun administrator Amazon Chime Chime Chime Chime.

Untuk membuat akun administrator Amazon Chime

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih Akun baru.
3. Untuk Nama Akun, masukkan nama akun dan pilih Buat akun.
4. (Opsional) Pilih apakah akan membiarkan Amazon Chime memilihAWS Wilayah optimal untuk rapat Anda dari semua Wilayah yang tersedia, atau hanya menggunakan Wilayah yang Anda pilih. Untuk informasi selengkapnya, lihat Mengelola pengaturan rapat.

Langkah 2 (opsional): Mengkonfigurasi pengaturan akun

Secara default, akun baru dibuat sebagai akun Tim. Jika Anda lebih suka mengklaim domain dan terhubung ke penyedia identitas Anda sendiri, atau Okta SSO, Anda dapat mengonversi ke akun Enterprise. Untuk informasi selengkapnya tentang jenis akun Tim dan Enterprise, lihatMemilih antara akun Amazon Chime Team atau akun Enterprise.

Mengonversi akun Tim menjadi akun Enterprise

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun.
3. Untuk Identitas, pilih Memulai.
4. Ikuti langkah-langkah di konsol untuk mengklaim domain Anda.
5. (Opsional) Ikuti langkah-langkah di konsol untuk mengatur penyedia identitas Anda dan mengkonfigurasi grup direktori Anda.

Untuk informasi selengkapnya tentang mengklaim domain, lihatMengklaim domain. Untuk informasi selengkapnya tentang pengaturan penyedia identitas, lihatMenghubungkan ke Active Directory danMenyambung ke Okta SSO.

Anda juga dapat mengizinkan atau berhenti mengizinkan kebijakan akun untuk opsi, seperti remote control layar bersama dan fitur Amazon Chime call me.

Cara mengonfigurasi kebijakan akun

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun yang akan dikonfigurasi.
3. Untuk Pengaturan, pilih Rapat.
4. Untuk Kebijakan, pilih atau hapus opsi kebijakan akun yang ingin Anda izinkan atau hentikan izinkan.
5. Pilih Ubah.

Untuk informasi selengkapnya, lihat Mengelola pengaturan rapat.

Langkah 3: Menambahkan pengguna ke akun Anda

Setelah akun Amazon Chime Team Anda dibuat, undang diri Anda dan pengguna Anda untuk bergabung dengannya. Jika Anda meningkatkan akun Anda ke akun Enterprise, Anda tidak perlu mengundang pengguna Anda. Sebagai gantinya, tingkatkan ke akun Enterprise dan klaim domain Anda. Untuk informasi selengkapnya, lihat Langkah 2 (opsional): Mengkonfigurasi pengaturan akun.

Untuk menambahkan pengguna ke akun Amazon Chime Anda

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Anda.
3. Pada halaman Pengguna, pilih Undang pengguna.
4. Masukkan alamat email pengguna yang akan diundang, termasuk diri Anda sendiri, dan pilih Undang pengguna.

Pengguna yang diundang menerima undangan email untuk bergabung dengan akun Amazon Chime Team yang Anda buat. Ketika mereka mendaftarkan akun pengguna Amazon Chime mereka, mereka menerima izin Pro secara default, dan uji coba 30 hari berakhir. Jika mereka telah mendaftar untuk akun pengguna Amazon Chime dengan alamat email pekerjaan mereka, mereka dapat terus menggunakan akun itu. Mereka juga dapat mengunduh aplikasi klien Amazon Chime kapan saja dengan memilih Unduh Amazon Chime dan masuk ke akun pengguna mereka.

Anda hanya dikenai biaya untuk pengguna dengan izin Pro saat mereka menyelenggarakan rapat. Tidak ada biaya untuk pengguna dengan izin Dasar. Pengguna dasar tidak dapat menyelenggarakan rapat, tetapi mereka dapat menghadiri rapat dan menggunakan obrolan. Untuk informasi selengkapnya tentang harga dan fitur yang dapat diakses pengguna dengan izin Pro dan Dasar, lihat Paket dan harga.

Untuk mengubah izin pengguna

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Anda.
3. Pada halaman Pengguna, pilih pengguna atau pengguna untuk mengubah izin untuk.
4. Pilih Tindakan pengguna, Tetapkan izin pengguna.
5. Untuk Izin, pilih Pro atau Basic.
6. PilihTetapkan.

Anda dapat memberikan izin administrator kepada pengguna lain, dan juga mengontrol akses mereka ke konsol Amazon Chime untuk akun Anda. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon Chime.

(Opsional) Menyiapkan nomor telepon untuk akun Amazon Chime Anda

Opsi telepon berikut tersedia untuk akun administratif Amazon Chime:

Panggilan Amazon Chime Bisnis Chime Chime

Memungkinkan pengguna Anda mengirim dan menerima panggilan telepon dan pesan teks langsung dari Amazon Chime. Berikan nomor telepon Anda di konsol atau port Amazon Chime di nomor telepon yang ada. Tetapkan nomor telepon ke pengguna Amazon Chime Anda dan beri mereka izin untuk mengirim dan menerima panggilan telepon dan pesan teks menggunakan Amazon Chime. Untuk informasi selengkapnya, lihat Mengelola nomor telepon di Amazon Chime dan Porting nomor telepon yang ada.

Amazon Chime Voice Connector

Menyediakan layanan trunking SIP untuk sistem telepon yang ada. Port di nomor telepon yang ada atau berikan nomor telepon baru di konsol Amazon Chime. Untuk informasi selengkapnya, lihat Mengelola Konektor Suara Amazon Chime di Panduan Administrasi Amazon Chime SDK.

Mengelola akun Amazon Chime Anda

Anda dapat menggunakan Amazon Chime sebagai pengguna individu atau sebagai grup tanpa administrator. Tetapi jika Anda ingin menambahkan fungsionalitas administrator atau membeli Amazon Chime Pro, Anda harus membuat akun Amazon Chime di. AWS Management Console Untuk mempelajari cara membuat akun administrator Amazon Chime, atau untuk informasi selengkapnya tentang membeli Amazon Chime Pro, lihat. Mulai

Untuk informasi selengkapnya tentang berbagai jenis akun administrator Amazon Chime, lihat. Memilih antara akun Amazon Chime Team atau akun Enterprise Untuk informasi selengkapnya tentang mengelola akun administrator yang ada, lihat topik berikut.

Topik

Memilih antara akun Amazon Chime Team atau akun Enterprise

Saat membuat akun administrator Amazon Chime, Anda memilih apakah akan membuat akun Tim atau akun Enterprise. Untuk informasi selengkapnya tentang membuat akun administrator Amazon Chime, lihat. Mulai

Akun tim

Dengan akun Tim, Anda dapat mengundang pengguna dan memberi mereka izin Amazon Chime Pro tanpa mengklaim domain email. Untuk informasi selengkapnya tentang izin Pro dan Dasar, lihat Paket dan harga.

Anda dapat mengundang pengguna dari domain email apa pun yang belum diklaim oleh organisasi lain. Anda hanya membayar untuk pengguna saat mereka menyelenggarakan rapat. Pengguna di akun Tim Anda dapat menggunakan aplikasi Amazon Chime untuk mencari dan menghubungi pengguna Amazon Chime lainnya yang terdaftar ke akun yang sama. Kami juga merekomendasikan akun Tim untuk membayar pengguna Pro di luar organisasi Anda.

Akun perusahaan

Dengan akun Enterprise, Anda memiliki kontrol lebih besar atas pengguna dari domain organisasi Anda. Anda dapat memilih untuk terhubung ke penyedia identitas Anda sendiri atau Okta SSO untuk mengautentikasi dan menetapkan izin Pro atau Dasar. Amazon Chime juga mendukung Microsoft Active Directory.

Untuk membuat akun Enterprise, Anda harus mengklaim setidaknya satu domain email. Ini memastikan bahwa semua pengguna yang masuk ke Amazon Chime menggunakan domain yang diklaim disertakan dalam akun Amazon Chime yang dikelola secara terpusat. Akun perusahaan diperlukan untuk mengelola pengguna Anda melalui integrasi direktori yang didukung. Lihat informasi yang lebih lengkap di Mengklaim domain dan Menghubungkan ke Active Directory.

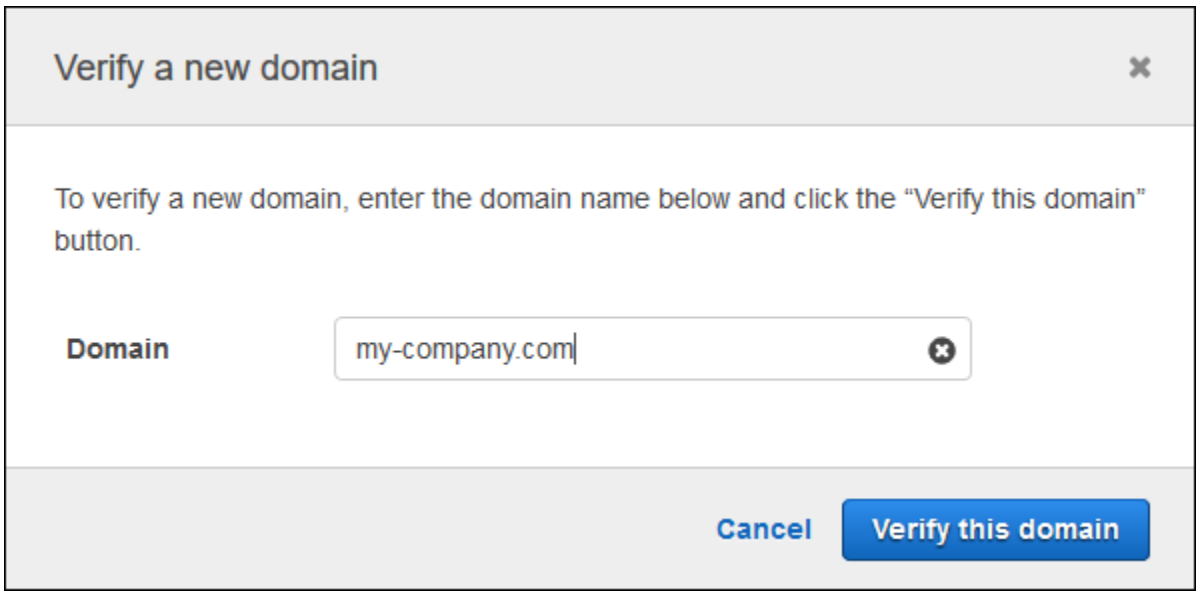
Anda juga dapat mengelola aktivasi dan penangguhan pengguna dari akun Enterprise Anda. Untuk informasi selengkapnya, lihat Mengelola izin dan akses pengguna.

Mengklaim domain

Untuk membuat akun Enterprise dan mendapatkan manfaat dari kontrol yang lebih besar yang diberikannya atas akun dan pengguna Anda, Anda harus mengklaim setidaknya satu domain email.

Untuk mengklaim domain

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Tim.
3. Di panel navigasi, pilih Identitas, Domain.
4. Pada halaman Domain, pilih Klaim domain baru.
5. Untuk Domain, ketik domain yang digunakan organisasi Anda untuk alamat email. Pilih Verifikasi domain ini.



6. Ikuti petunjuk di layar untuk menambahkan catatan TXT ke server DNS untuk domain Anda. Secara umum, prosesnya melibatkan masuk ke akun domain Anda, menemukan catatan DNS untuk domain Anda, dan menambahkan catatan TXT dengan nama dan nilai yang disediakan oleh Amazon Chime. Untuk informasi selengkapnya tentang memperbarui catatan DNS untuk domain Anda, lihat dokumentasi untuk penyedia DNS atau pencatat nama domain Anda.

   Amazon Chime memeriksa keberadaan catatan ini untuk memverifikasi bahwa Anda memiliki domain. Setelah domain diverifikasi, statusnya berubah dari Verifikasi Tertunda ke Verified.

   > **Note**
   >
   > Propagasi perubahan DNS dan verifikasi oleh Amazon Chime dapat memakan waktu hingga 24 jam.

7. Jika organisasi Anda menggunakan domain atau subdomain tambahan untuk alamat email, ulangi prosedur ini untuk setiap domain.

Untuk informasi selengkapnya tentang pemecahan masalah klaim domain, lihat Mengapa permintaan klaim domain saya tidak diverifikasi? .

Mengonversi akun Tim ke akun Enterprise

Untuk mengonversi akun Tim yang ada ke akun Enterprise, klaim satu atau beberapa domain email di konsol Amazon Chime. Untuk informasi selengkapnya tentang perbedaan antara akun Tim dan

Perusahaan, lihatMemilih antara akun Amazon Chime Team atau akun Enterprise. Untuk informasi selengkapnya tentang mengklaim domain, lihatMengklaim domain.

Untuk mengonversi akun Team ke akun Enterprise

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun.
3. Untuk Identitas, pilih Memulai.
4. Ikuti langkah-langkah di konsol untuk mengklaim domain Anda.
5. (Opsional) Ikuti langkah-langkah di konsol untuk mengatur penyedia identitas Anda dan mengonfigurasi grup direktori Anda.

Setelah akun Anda dikonversi ke akun Enterprise, Anda dapat memutuskan apakah akan menghubungkan instans Active Directory melalui AWS Directory Service. Menghubungkan ke instans Active Directory memungkinkan pengguna Anda untuk masuk ke Amazon Chime menggunakan kredenal Direktori Aktif mereka. Untuk informasi selengkapnya, lihat Menghubungkan ke Active Directory.

Jika Anda tidak terhubung ke instans Direktori Aktif, pengguna Anda dapat terus masuk ke Amazon Chime menggunakan Login with Amazon (LWA) atau kredenal akun Amazon.com mereka.

Mengganti nama akun Anda

Langkah-langkah berikut menjelaskan cara mengganti nama tim Amazon Chime dan akun perusahaan yang Anda kelola. Nama yang Anda pilih muncul di email yang mengundang pengguna untuk bergabung dengan Amazon Chime.

Untuk mengganti nama akun Anda

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.

   Halaman Akun muncul secara default.
2. Di kolom Nama akun, pilih akun yang ingin Anda ganti namanya.
3. Di panel sebelah kiri, di bawah Pengaturan, pilih Akun.

   Halaman ringkasan Akun akan muncul.
4. Buka daftar Tindakan akun dan pilih Ganti nama akun.

Kotak dialog Ganti nama akun muncul.

5. Masukkan nama akun baru dan pilih Simpan.

Menghapus akun Anda

Jika Anda menghapus AWS akun Anda di AWS Management Console, akun Amazon Chime Anda akan dihapus secara otomatis. Atau, Anda dapat menggunakan konsol Amazon Chime untuk menghapus akun Amazon Chime Team atau Enterprise.

> **Note**
>
> Pengguna yang tidak dikelola di akun Tim atau Perusahaan dapat meminta untuk dihapus menggunakan perintah “Hapus saya” Amazon Chime Assistant. Untuk informasi selengkapnya, lihat Menggunakan Asisten Lonceng Amazon.

Untuk menghapus akun Tim

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pilih akun di kolom Nama akun dan pilih Akun di bawah Pengaturan.
3. Di panel navigasi, halaman Pengguna ditampilkan.
4. Pilih pengguna dan pilih Tindakan pengguna, Hapus pengguna.
5. Di panel navigasi, pilih Akun, Tindakan akun, dan Hapus akun.
6. Konfirmasikan bahwa Anda ingin menghapus akun Anda.

Amazon Chime menghapus semua data pengguna saat Anda menghapus akun Anda. Ini termasuk penghentian akun, AWS akun Amazon Chime individual, atau pengguna Amazon Chime yang tidak dikelola. Ini tidak termasuk data non-konten yang terkait dengan akun pengguna dan penggunaan Amazon Chime (Atribut Layanan yang tercakup dalam Perjanjian Pelanggan) yang dihasilkan oleh Amazon Chime.

Untuk menghapus akun Enterprise

1. Hapus domain.

> **Note**
>
> Saat Anda menghapus domain, hal berikut terjadi:
>
> - Pengguna yang terkait dengan domain segera keluar dari semua perangkat dan kehilangan akses ke semua kontak, percakapan obrolan, dan ruang obrolan.
> - Rapat yang dijadwalkan oleh pengguna dari domain ini tidak lagi dimulai.
> - Pengguna yang ditangguhkan terus ditampilkan sebagai status Ditangguhkan pada halaman detail Pengguna dan Pengguna dan tidak dapat mengakses data mereka. Mereka tidak dapat membuat akun Amazon Chime baru dengan alamat email mereka.
> - Pengguna terdaftar ditampilkan sebagai Dirilis di halaman detail Pengguna dan Pengguna dan tidak dapat mengakses data mereka. Mereka dapat membuat akun Amazon Chime baru dengan alamat email mereka.
> - Jika Anda memiliki akun Direktori Aktif, dan Anda menghapus domain yang dikaitkan dengan alamat email utama pengguna, pengguna tidak dapat mengakses Amazon Chime dan profil mereka dihapus. Jika Anda menghapus domain yang dikaitkan dengan alamat email sekunder pengguna, mereka tidak dapat masuk dengan alamat email tersebut, tetapi mereka tetap memiliki akses ke kontak dan data Amazon Chime mereka.
> - Jika Anda memiliki akun Enterprise OpenID Connect (OIDC), dan Anda menghapus domain yang dikaitkan dengan alamat email utama pengguna, pengguna tidak dapat lagi mengakses Amazon Chime dan profilnya dihapus.

2. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
3. Pada halaman Akun, pilih nama akun Tim.
4. Di panel navigasi, pilih Pengaturan, Domain.
5. Pada halaman Domain, pilih Hapus domain.
6. Di panel navigasi, pilih Akun, Tindakan akun, dan Hapus akun.
7. Konfirmasikan bahwa Anda ingin menghapus akun Anda.

Amazon Chime menghapus semua data pengguna saat Anda menghapus akun Anda. Ini termasuk penghentian akun, AWS akun Amazon Chime individual, atau pengguna Amazon Chime yang tidak dikelola. Ini tidak termasuk data non-konten yang terkait dengan akun pengguna dan penggunaan

Amazon Chime (Atribut Layanan yang tercakup dalam Perjanjian Pelanggan) yang dihasilkan oleh Amazon Chime.

Mengelola pengaturan rapat

Kelola setelan rapat Anda dari konsol Amazon Chime.

Pengaturan kebijakan rapat

Kelola kebijakan akun di konsol Amazon Chime di bawah Pengaturan, Rapat. Pilih dari opsi kebijakan berikut.

Aktifkan kontrol bersama dalam berbagi layar

> Pilih apakah pengguna di organisasi Anda dapat memberikan kontrol bersama atas komputer mereka saat berada dalam rapat. Peserta yang meminta kontrol bersama komputer pengguna Anda menerima pesan kesalahan yang menunjukkan bahwa remote control tidak tersedia.

Aktifkan panggilan keluar untuk bergabung dengan rapat

> Mengaktifkan fitur Amazon Chime call me. Menyediakan opsi bagi peserta rapat untuk bergabung dengan rapat dengan menerima panggilan telepon dari Amazon Chime.

Pengaturan aplikasi rapat

Kelola akses aplikasi rapat di bawah Pengaturan, Rapat di konsol Amazon Chime. Anda dapat memilih opsi berikut:

Izinkan pengguna masuk ke Amazon Chime menggunakan Aplikasi Amazon Chime Meetings untuk Slack

> Opsi ini memungkinkan pengguna di organisasi Anda masuk ke Amazon Chime dari Aplikasi Rapat Amazon Chime untuk Slack. Untuk informasi selengkapnya, lihat Menyiapkan Aplikasi Amazon Chime Meetings untuk Slack.

Pengaturan Wilayah Rapat

Untuk meningkatkan kualitas rapat dan mengurangi latensi, Amazon Chime memproses rapat di Wilayah AWS optimal untuk semua peserta. Anda dapat memilih apakah akan mengizinkan

Amazon Chime memilih Wilayah optimal untuk rapat dari semua Wilayah yang tersedia, atau hanya menggunakan Wilayah yang Anda pilih.

Anda dapat memperbarui pengaturan ini dari pengaturan Rapat akun Anda kapan saja. Dari pengaturan Rapat, Anda juga dapat melihat persentase rapat Amazon Chime yang sedang diproses di setiap Wilayah.

Untuk memperbarui pengaturan Wilayah rapat

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Anda.
3. Di panel navigasi, pilih Pengaturan, Rapat.
4. Untuk Wilayah, pilih salah satu opsi berikut:
   - Gunakan semua Wilayah yang tersedia untuk memastikan kualitas rapat — Memungkinkan Amazon Chime mengoptimalkan pemrosesan rapat untuk Anda.
   - Gunakan hanya Wilayah yang saya pilih - Memungkinkan Anda memilih Wilayah dari menu tarik-turun.
5. Pilih Simpan.

Mengelola kebijakan retensi obrolan

Jika Anda mengelola satu atau beberapa akun Amazon Chime Enterprise, Anda dapat menetapkan kebijakan penyimpanan obrolan untuk hal-hal berikut:

- Percakapan obrolan yang hanya mencakup anggota akun Enterprise Anda.
- Ruang obrolan yang dibuat oleh anggota akun Enterprise Anda.

Kebijakan penyimpanan secara otomatis menghapus pesan berdasarkan periode waktu yang Anda tetapkan. Anda dapat mengatur periode waktu yang berlangsung dari satu hari hingga 15 tahun.

> **Note**
>
> Akun Amazon Chime Enterprise memiliki periode retensi 90 hari. Kebijakan ini berlaku untuk percakapan yang melibatkan pengguna yang termasuk dalam akun, dan untuk pengguna yang bukan milik akun.
> Kebijakan retensi tidak berlaku untuk hal-hal berikut:

- Percakapan obrolan yang tidak menyertakan anggota akun Amazon Chime Enterprise
- Ruang obrolan yang dibuat oleh pengguna yang bukan milik akun Amazon Chime Enterprise

Bagaimana kebijakan retensi memengaruhi pengguna Amazon Chime

Kebijakan penyimpanan yang ditetapkan administrator akun Enterprise memengaruhi pengguna Amazon Chime secara berbeda, bergantung pada apakah pengguna merupakan bagian dari akun Enterprise yang sama, akun Enterprise yang berbeda, akun Tim, atau apakah pengguna bukan anggota akun apa pun.

Percakapan obrolan anggota perusahaan

Tabel berikut menunjukkan bagaimana kebijakan retensi memengaruhi percakapan obrolan untuk anggota akun Enterprise.

Jika percakapan obrolan mencakup...	Kebijakan retensi adalah...
Hanya anggota lain dari akun Enterprise pengguna	Ditetapkan oleh administrator pengguna
Siapa pun di luar akun Enterprise pengguna	Secara otomatis diatur ke 90 hari

Ruang obrolan anggota perusahaan

Tabel berikut menunjukkan bagaimana kebijakan retensi memengaruhi ruang obrolan untuk anggota akun Enterprise.

Jika ruang obrolan dibuat oleh...	Kebijakan retensi adalah...
Anggota akun Enterprise pengguna	Ditetapkan oleh administrator pengguna
Anggota akun Enterprise lainnya	Ditetapkan oleh administrator akun lain
Anggota akun non-Enterprise	Tidak berlaku

Percakapan obrolan anggota tim

Tabel berikut menunjukkan bagaimana kebijakan retensi memengaruhi percakapan obrolan untuk anggota akun Tim.

Jika percakapan obrolan mencakup...	Kebijakan retensi adalah...
Hanya pengguna yang bukan anggota akun Enterprise	Tidak berlaku
Setidaknya satu anggota akun Enterprise	Secara otomatis diatur ke 90 hari

Ruang obrolan anggota tim

Tabel berikut menunjukkan bagaimana kebijakan retensi memengaruhi ruang obrolan untuk anggota akun Tim.

Jika ruang obrolan dibuat oleh...	Kebijakan retensi adalah...
Pengguna akun Tim	Tidak berlaku
Siapa pun yang bukan anggota akun Enterprise	Tidak berlaku
Anggota akun Enterprise	Ditetapkan oleh administrator akun Enterprise

Pengguna Amazon Chime yang bukan anggota akun Perusahaan atau Tim hanya tunduk pada kebijakan penyimpanan ruang obrolan di ruang obrolan yang dibuat oleh anggota akun Perusahaan.

Mengobrol percakapan dengan penerima yang bukan milik akun Perusahaan atau Tim

Tabel berikut menunjukkan bagaimana kebijakan penyimpanan memengaruhi percakapan obrolan untuk pengguna yang bukan anggota akun Amazon Chime Enterprise atau Tim.

Jika percakapan obrolan mencakup...	Kebijakan retensi adalah...
Hanya pengguna yang bukan anggota akun Enterprise	Tidak berlaku

Jika percakapan obrolan mencakup...	Kebijakan retensi adalah...
Setidaknya satu anggota akun Enterprise	Secara otomatis diatur ke 90 hari

Ruang obrolan yang dibuat oleh pengguna yang bukan milik akun Perusahaan atau Tim

Tabel berikut menunjukkan bagaimana kebijakan penyimpanan memengaruhi ruang obrolan bagi pengguna yang bukan anggota akun Amazon Chime Enterprise atau Tim.

Jika ruang obrolan dibuat oleh...	Kebijakan retensi adalah...
Pengguna yang bukan anggota akun Perusahaan atau Tim	Tidak berlaku
Pengguna akun Tim	Tidak berlaku
Anggota akun Enterprise	Ditetapkan oleh administrator akun Enterprise

Mengaktifkan retensi obrolan

Administrator akun Amazon Chime Enterprise dapat menggunakan konsol Amazon Chime untuk mengaktifkan retensi obrolan untuk percakapan obrolan dan ruang obrolan di akun mereka. Anda juga dapat menggunakan konsol untuk memperbarui periode retensi obrolan atau mematikan retensi obrolan kapan saja.

Untuk mengaktifkan retensi obrolan

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun.
3. Di panel navigasi, di bawah Pengaturan, pilih Retensi.
4. Pada halaman Retensi, di bawah Retensi percakapan obrolan, pindahkan slider ke Aktif.
5. Di bawah Periode penyimpanan, masukkan nomor di kotak pertama, lalu buka daftar di sebelah kotak dan pilih Hari, Minggu, atau Tahun.
6. Di bawah Retensi ruang obrolan, ulangi langkah 4-5. Setelah selesai, silakan pilih Simpan.

Dalam satu hari setelah menetapkan periode retensi, pengguna di akun Anda kehilangan akses ke pesan yang dikirim di luar periode penyimpanan.

Memulihkan pesan obrolan

> **Note**
>
> Anda harus menjadi administrator akun Amazon Chime Enterprise untuk menyelesaikan langkah-langkah ini.

Anda dapat memulihkan pesan obrolan dalam waktu 30 hari setelah menetapkan periode retensi obrolan. Saat memulihkan pesan obrolan, Anda memulihkan semua pesan yang dikirim oleh semua pengguna di akun Amazon Chime Anda.

Dalam periode 30 hari itu, Anda dapat melakukan salah satu dari hal berikut untuk memulihkan pesan:

- Gunakan Amazon Chime Console untuk menonaktifkan retensi data.

  — ATAU —

- Memperpanjang periode retensi.

Setelah masa tenggang 30 hari, semua pesan obrolan yang termasuk dalam periode retensi akan dihapus secara permanen. Pesan obrolan baru dihapus secara permanen segera setelah melewati periode penyimpanan.

Untuk informasi tentang pengaturan atau perubahan periode retensi, lihatMengaktifkan retensi obrolan, sebelumnya di bagian ini.

Pesan obrolan juga dihapus secara permanen dari Amazon Chime saat Anda atau anggota akun melakukan salah satu tindakan berikut:

- Hapus ruang obrolan Amazon Chime. Untuk informasi selengkapnya tentang menghapus ruang obrolan, lihat Menghapus ruang obrolan, di Panduan Pengguna Amazon Chime.
- Akhiri rapat Amazon Chime di mana pesan obrolan hadir.

> **Note**
>
> Jika diperlukan, Anda dapat menyalin dan menyimpan pesan obrolan secara manual dari rapat, tetapi Anda harus melakukannya sebelum rapat berakhir. Untuk informasi selengkapnya, lihat Menggunakan obrolan dalam rapat, di Panduan Pengguna Amazon Chime.

Menghapus pesan obrolan

Untuk mematuhi kebijakan penyimpanan data, Amazon Chime menyimpan semua pesan obrolan, dan mencegah pengguna akhir menghapus pesan yang mereka kirim. Namun, administrator sistem Amazon Chime dapat menggunakan sepasang API untuk menghapus pesan individual dari percakapan dan ruang obrolan. Pesan harus berada di akun Amazon Chime administrator.

Pengguna dapat meminta penghapusan pesan dengan mengirimi Anda ID pesan dan ID percakapan atau ruang obrolan yang sesuai. Topik Menggunakan fitur obrolan, di Panduan Pengguna Amazon Chime, menjelaskan caranya.

Ketika Anda mendapatkan permintaan penghapusan, Anda dapat menulis kode atau menggunakan AWS CLI untuk memanggil API berikut.

Untuk menghapus pesan

- Lakukan salah satu hal berikut:
  - Untuk pesan percakapan — Gunakan RedactConversationMessageAPI.

    Di CLI, jalankan perintah berikut:

    ```
    aws chime redact-conversation-message --conversation-id id_string --message-id id_string
    ```
  - Untuk pesan ruang obrolan — Gunakan RedactRoomMessageAPI.

    Di CLI, jalankan perintah berikut:

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

Menghubungkan ke Active Directory

Saat Anda menghubungkan akun administratif Amazon Chime Anda ke Direktori Aktif, Anda bisa mendapatkan keuntungan dari kemampuan berikut:

- Pengguna Amazon Chime Anda dapat masuk dengan kredenal Direktori Aktif mereka.
- Sebagai administrator Amazon Chime, Anda memilih fitur keamanan kredenal mana yang akan ditambahkan, termasuk rotasi kata sandi, aturan kompleksitas kata sandi, dan otentikasi multi-faktor.
- Saat Anda menghapus akun pengguna dari Active Directory, akun Amazon Chime mereka juga akan dihapus.
- Anda dapat menentukan grup Active Directory mana yang menerima izin Amazon Chime Pro.
  - Beberapa grup dapat dikonfigurasi untuk menerima izin Dasar atau Pro.
  - Pengguna harus menjadi anggota dari salah satu grup untuk masuk ke Amazon Chime.
  - Pengguna di kedua grup menerima lisensi Pro.

Untuk informasi selengkapnya tentang mengelola izin pengguna, lihatMengelola izin dan akses pengguna.

Prasyarat

Sebelum Anda dapat terhubung ke Direktori Aktif Anda di Amazon Chime, Anda harus menyelesaikan prasyarat berikut:

- Pastikan Anda memiliki AWS Identity and Access Management izin yang benar untuk mengonfigurasi domain, direktori aktif, dan grup direktori. Untuk informasi selengkapnya, lihat Manajemen identitas dan akses untuk Amazon Chime.
- Buat direktori dengan AWS Directory Service yang dikonfigurasi di Wilayah AS Timur (Virginia N.). Untuk informasi selengkapnya, lihat Panduan Administrasi AWS Directory Service. Amazon Chime dapat terhubung menggunakan AD Connector, Microsoft AD, atau Simple AD.
- Klaim domain untuk membuat akun Amazon Chime Enterprise, atau mengonversi akun Tim Anda yang ada ke akun Enterprise. Jika pengguna Anda memiliki alamat email kantor dari lebih dari satu domain, pastikan untuk mengklaim semua domain tersebut. Lihat informasi yang lebih lengkap di Mengklaim domain dan Mengonversi akun Tim ke akun Enterprise.

Menghubungkan ke Direktori Aktif Anda di Amazon Chime

Setelah Anda menghubungkan Active Directory ke Amazon Chime, pengguna akan diminta untuk masuk dengan kredensialnya ketika mereka menggunakan alamat email dari salah satu domain yang Anda klaim di akun Amazon Chime Enterprise Anda.

Untuk terhubung ke Direktori Aktif Anda di Amazon Chime

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, untuk Identity, pilih Active directory.
3. Untuk ID direktori Cloud, pilih AWS Directory Service direktori yang akan digunakan untuk Amazon Chime, lalu pilih Connect.

   > **Note**
   >
   > Anda dapat menemukan ID direktori Anda menggunakan AWS Directory Service konsol.

4. Setelah direktori Anda terhubung, pilih Tambahkan grup baru.
5. Untuk Grup, masukkan nama grup. Nama harus sama persis dengan grup Active Directory di direktori target. Unit Organisasi Direktori Aktif (OU) tidak didukung.
6. Untuk Izin, pilih Basic atau Pro.
7. Pilih Tambah grup.
8. (Opsional) Ulangi prosedur ini untuk membuat grup direktori tambahan.

Mengkonfigurasi beberapa alamat email

Setelah Anda terhubung ke Direktori Aktif di Amazon Chime, pengguna dapat masuk ke Amazon Chime menggunakan kredenal Direktori Aktif mereka. Pengguna Anda dapat memiliki beberapa alamat email yang ditetapkan untuk mereka di Direktori Aktif Anda. Untuk mengizinkan pengguna Anda masuk ke Amazon Chime menggunakan kredensi Direktori Aktif mereka, Anda harus mengklaim setiap domain email yang berlaku di akun administratif Amazon Chime Anda. Untuk informasi selengkapnya, lihat Mengklaim domain.

> **Note**
>
> Jika pengguna Anda mencoba masuk menggunakan alamat email dari domain yang tidak diklaim, mereka akan diminta untuk masuk menggunakan Masuk dengan Amazon. Mereka

tidak dapat masuk ke akun administratif Anda saat menggunakan alamat email dari domain yang tidak diklaim.

Saat melihat detail pengguna di konsol Amazon Chime, Amazon Chime menggunakan alamat email tunggal dalam `EmailAddress` atribut dari Direktori Aktif Anda sebagai alamat email utama setiap pengguna. Ini adalah satu-satunya alamat email yang dapat Anda lihat untuk pengguna di konsol Amazon Chime. Namun, pengguna dapat masuk dengan alamat tambahan apa pun yang tercantum dalam `ProxyAddress` atribut, selama Anda mengklaim domain tersebut di akun Amazon Chime Anda.

Contoh konfigurasi salah

Pengguna dengan nama pengguna shirley.rodriguez adalah anggota akun Amazon Chime yang telah mengklaim dua domain: example.com dan example.org. Di Active Directory, pengguna ini memiliki tiga alamat email berikut:

- Alamat email utama: shirley.rodriguez@example.com
- Alamat email proxy 1: shirley.rodriguez@example2.com
- Alamat email proxy 2: srodriguez@example.org

Pengguna ini dapat masuk ke Amazon Chime menggunakan shirley.rodriguez@example.com atau srodriguez@example.org dan shirley.rodriguez. Jika mereka mencoba masuk menggunakan shirley.rodriguez@example2.com, mereka diminta untuk Masuk dengan Amazon, dan mereka bukan bagian dari akun terkelola Anda. Inilah sebabnya mengapa penting untuk mengklaim semua domain email pengguna Anda.

Pengguna Amazon Chime lainnya dapat menambahkan pengguna ini sebagai kontak, mengundang mereka ke rapat, atau menambahkannya sebagai delegasi menggunakan alamat email shirley.rodriguez@example.com atau srodriguez@example.org.

Contoh konfigurasi yang benar

Pengguna dengan nama pengguna shirley.rodriguez adalah anggota akun Amazon Chime yang telah mengklaim tiga domain: example.com, example2.com, dan example.org. Di Active Directory, pengguna ini memiliki tiga alamat email berikut:

- Alamat email utama: shirley.rodriguez@example.com

- Alamat email proxy 1: shirley.rodriguez@example2.com
- Alamat email proxy 2: srodriguez@example.org

Pengguna ini dapat masuk ke Amazon Chime menggunakan salah satu alamat email kantor mereka. Pengguna lain juga dapat menambahkannya sebagai kontak, mengundang mereka ke rapat, atau menambahkannya sebagai delegasi menggunakan alamat email kantor mereka.

Menyambung ke Okta SSO

Jika Anda memiliki akun Enterprise, Anda dapat terhubung ke Okta SSO untuk mengautentikasi dan menetapkan izin pengguna.

> **Note**
>
> Jika Anda perlu membuat akun Enterprise, yang memungkinkan Anda mengelola semua pengguna dalam satu set domain alamat email tertentu, lihatMengklaim domain.

Menghubungkan Amazon Chime ke Okta memerlukan konfigurasi dua aplikasi di Konsol Administrasi Okta. Aplikasi pertama dikonfigurasi secara manual, dan menggunakan OpenID Connect untuk mengautentikasi pengguna ke layanan Amazon Chime. Aplikasi kedua tersedia sebagai Amazon Chime SCIM Provisioning di Okta Integration Network (OIN). Ini dikonfigurasi untuk mendorong pembaruan ke Amazon Chime tentang perubahan pada pengguna dan grup.

Untuk terhubung ke Okta SSO

1. Buat aplikasi Amazon Chime (OpenID Connect) di Konsol Administrasi Okta:

    1. Masuk ke Dasbor Administrasi Okta, lalu pilih Tambah Aplikasi. Di kotak dialog Create New Application, pilih Web, Next.
    2. Konfigurasikan Pengaturan Aplikasi:
        a. Beri nama aplikasi**`Amazon Chime`**.
        b. Untuk Login Redirect URI, masukkan nilai berikut: **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
        c. Di bagian Jenis Hibah yang Diizinkan, pilih semua opsi untuk mengaktifkannya.
        d. Pada menu tarik-turun Login yang dimulai oleh, pilih Either (Okta atau App), dan pilih semua opsi terkait.

e. Untuk URI Initiate Login, masukkan nilai berikut: **`https://signin.id.ue1.app.chime.aws/auth/okta`**

f. Pilih Simpan.

g. Biarkan halaman ini tetap terbuka, karena Anda memerlukan informasi Client ID, Client secret, dan Issuer URI untuk Langkah 2.

2. Di konsol Amazon Chime, ikuti langkah-langkah ini:

1. Pada halaman konfigurasi tanda tunggal Okta, di bagian atas halaman, pilih Siapkan kunci masuk.
2. Dalam kotak dialog Pengaturan kunci Okta yang masuk:
   a. Rekatkan ID Klien dan informasi rahasia Klien dari halaman Pengaturan Aplikasi Okta.
   b. Rekatkan URI Penerbit yang sesuai dari halaman Okta API. URI Penerbit harus berupa domain Okta, seperti. `https://example.okta.com`

3. Siapkan aplikasi Penyediaan Amazon Chime SCIM di Konsol Administrasi Okta untuk bertukar identitas tertentu dan informasi keanggotaan grup dengan Amazon Chime:

1. Di Okta Administration Console, pilih Applications, Add Application, cari Amazon Chime SCIM Provisioning, dan tambahkan aplikasi.

> **Important**
>
> Selama pengaturan awal, pilih keduanya Jangan tampilkan aplikasi ke pengguna dan Jangan tampilkan ikon aplikasi di Aplikasi Seluler Okta, lalu pilih Selesai.

2. Pada tab Provisioning, pilih Configure API Integration, dan pilih Enable API Integration. Biarkan halaman ini tetap terbuka, karena Anda harus menyalin kunci akses API untuk langkah berikut.
3. Di konsol Amazon Chime, pilih Buat kunci akses untuk membuat kunci akses API. Salin ke bidang Okta API Token di kotak dialog Konfigurasi Integrasi API, pilih Uji Integrasi, lalu pilih Simpan.
4. Konfigurasikan tindakan dan atribut yang akan digunakan Okta untuk memperbarui Amazon Chime. Pada tab Penyediaan, di bawah bagian Ke Aplikasi, pilih Edit, pilih dari Aktifkan Pengguna, Perbarui Atribut Pengguna, dan Nonaktifkan Pengguna, lalu pilih Simpan.
5. Pada tab Penugasan, berikan izin pengguna ke aplikasi SCIM baru.

> **Important**
>
> Sebaiknya berikan izin melalui grup yang berisi semua pengguna yang seharusnya memiliki akses ke Amazon Chime, terlepas dari lisensinya. Grup harus sama dengan grup yang digunakan untuk menetapkan aplikasi OIDC yang dihadapi pengguna pada langkah 1 sebelumnya. Jika tidak, pengguna akhir tidak akan dapat masuk.

6. Pada tab Push Groups, konfigurasikan grup dan keanggotaan mana yang disinkronkan ke Amazon Chime. Kelompok-kelompok ini digunakan untuk membedakan antara pengguna Basic dan Pro.

4. Konfigurasikan grup direktori di Amazon Chime:

   1. Di konsol Amazon Chime, navigasikan ke halaman konfigurasi tanda tunggal Okta.
   2. Di bawah Grup direktori, pilih Tambahkan grup baru.
   3. Masukkan nama grup direktori untuk ditambahkan ke Amazon Chime. Nama harus sama persis dengan salah satu Grup Push yang dikonfigurasi sebelumnya pada langkah 3-f.
   4. Pilih apakah pengguna dalam grup ini harus menerima kemampuan Dasar atau Pro, dan pilih Simpan. Ulangi proses ini untuk mengkonfigurasi grup tambahan.

   > **Note**
   >
   > Jika Anda menerima pesan galat yang menyatakan bahwa grup tidak ditemukan, kedua sistem mungkin belum menyelesaikan sinkronisasi. Tunggu beberapa menit, dan pilih Tambahkan grup baru lagi.

Memilih kemampuan Dasar atau Pro untuk pengguna di grup direktori Anda memengaruhi lisensi, kemampuan, dan biaya pengguna tersebut di akun Amazon Chime Enterprise Anda. Untuk informasi selengkapnya, silakan lihat Harga .

Menerapkan Amazon Chime Add-In untuk Outlook

Amazon Chime menyediakan dua add-in untuk Microsoft Outlook: Amazon Chime Add-In untuk Outlook di Windows dan Amazon Chime Add-In untuk Outlook. Add-in ini menawarkan fitur penjadwalan yang sama, tetapi mendukung berbagai jenis pengguna. Pelanggan dan organisasi Microsoft Office 365 yang menggunakan Microsoft Exchange 2013 atau yang lebih baru lokal dapat

menggunakan Amazon Chime Add-In untuk Outlook. Pengguna Windows dengan server Exchange lokal yang menjalankan Exchange Server 2010 atau yang lebih lama dan pengguna Outlook 2010 harus menggunakan Amazon Chime Add-in untuk Outlook di Windows.

Pengguna Windows yang tidak memiliki izin untuk menginstal Amazon Chime Add-in untuk Outlook harus memilih Amazon Chime Add-in untuk Outlook di Windows.

Untuk informasi tentang add-in mana yang tepat untuk Anda dan organisasi Anda, lihat Memilih Add-In Outlook yang Tepat.

Jika Anda memilih Amazon Chime Add-In untuk Outlook untuk organisasi Anda, Anda dapat menerapkannya ke pengguna dengan penerapan terpusat. Untuk informasi selengkapnya, lihat Panduan Instalasi Amazon Chime Add-In untuk Outlook untuk Administrator.

Menyiapkan Aplikasi Amazon Chime Meetings untuk Slack

Jika Anda menggunakan Slack Enterprise Grid Organizations, dan Anda memiliki atau mengelola organisasi Slack, Anda dapat menyiapkan Aplikasi Amazon Chime Meetings untuk Slack untuk organisasi Anda. Jika Anda administrator ruang kerja Slack, Anda dapat mengatur Aplikasi Amazon Chime Meetings untuk Slack untuk ruang kerja Anda.

Langkah-langkah di bagian berikut menjelaskan cara melakukan kedua jenis pengaturan, dan cara menyelesaikan tugas tambahan seperti memigrasikan ruang kerja ke organisasi.

Topik

- Menginstal Aplikasi Amazon Chime Meetings untuk Slack di organisasi
- Menginstal Aplikasi Amazon Chime Meetings untuk Slack di ruang kerja
- Migrasi ruang kerja ke organisasi
- Mengaitkan ruang kerja dengan akun Amazon Chime Team

Menginstal Aplikasi Amazon Chime Meetings untuk Slack di organisasi

Menginstal Aplikasi Amazon Chime Meetings untuk Slack di organisasi Slack memungkinkan pengguna untuk memulai rapat instan dan panggilan dengan pengguna lain di berbagai ruang kerja di organisasi tersebut. Ini juga memungkinkan administrator ruang kerja untuk menginstal Aplikasi Amazon Chime Meetings untuk aplikasi rapat Slack secara otomatis di ruang kerja baru. Langkah-langkah berikut menjelaskan caranya.

> **Note**
>
> Langkah-langkah berikut mengasumsikan bahwa Anda adalah pemilik atau administrator organisasi, dan Anda dapat masuk ke konsol manajemen Slack.

Untuk menyiapkan Aplikasi Amazon Chime Meetings untuk Slack di organisasi

1. Di panel sebelah kiri konsol manajemen Slack, pilih Aplikasi.

   Halaman Aplikasi muncul dan mencantumkan aplikasi yang diinstal organisasi, jika ada.
2. Pilih Kelola Aplikasi, yang terletak di sudut kanan atas halaman, lalu pilih Instal aplikasi.

   Kotak dialog Find an app to install akan muncul.
3. Cari di**`Amazon Chime Meetings`**, lalu pilih di hasil pencarian.

   Kotak dialog Tambahkan Amazon Chime Meetings ke ruang kerja muncul dan mencantumkan ruang kerja di organisasi.
4. Pilih ruang kerja atau ruang kerja tempat Anda ingin menginstal Aplikasi Amazon Chime Meetings untuk Slack.
5. Secara opsional, pilih Default untuk ruang kerja future jika Anda ingin menginstal Aplikasi Amazon Chime Meetings secara otomatis untuk Slack di semua ruang kerja baru, lalu pilih Berikutnya.

   Kotak dialog Tinjau izin yang diminta aplikasi ini muncul dan menampilkan izin dan tindakan untuk Aplikasi Rapat Amazon Chime untuk Slack.
6. Pilih Berikutnya.
7. Jika Anda memilih untuk menginstal Aplikasi Amazon Chime Meetings untuk Slack di ruang kerja baru secara default, pilih I'm ready to set this app as a default for future workspaces, lalu pilih Save. Jika tidak, pilih saja Simpan.

> **Note**
>
> Anda juga dapat menggunakan OAuth untuk menginstal aplikasi di organisasi Anda. Untuk informasi selengkapnya, lihat Menginstal dengan OAuth di bantuan Slack.

Menginstal Aplikasi Amazon Chime Meetings untuk Slack di ruang kerja

Menginstal Aplikasi Amazon Chime Meetings untuk Slack di ruang kerja memungkinkan pengguna untuk memulai rapat instan dan panggilan dengan pengguna lain di ruang kerja tersebut. Pengguna tidak memerlukan profil pengguna Amazon Chime untuk menggunakan Aplikasi Amazon Chime Meetings untuk Slack. Mereka dapat masuk dengan profil pengguna Slack mereka dan memulai panggilan atau rapat kapan saja. Jika pengguna perlu melakukan rapat dengan lebih dari satu orang lain, Anda harus menyiapkan akun Amazon Chime Team dan memberikan izin Pro kepada pengguna tambahan tersebut. Untuk informasi selengkapnya tentang memulai panggilan dan rapat Amazon Chime, lihat Menggunakan Aplikasi Amazon Chime Meetings untuk Slack di Panduan Pengguna Amazon Chime. Untuk informasi selengkapnya tentang menyiapkan akun Amazon Chime Team, lihat Mengaitkan ruang kerja dengan akun Amazon Chime Team di panduan ini.

Untuk menginstal Aplikasi Amazon Chime Meetings untuk Slack untuk ruang kerja Slack

1. Arahkan ke Direktori Aplikasi Slack dan temukan Aplikasi Amazon Chime Meetings.
2. Pilih Tambahkan ke Slack untuk menginstal Aplikasi Amazon Chime Meetings untuk Slack dari Direktori Aplikasi Slack.
3. Konfigurasikan setelan Panggilan ruang kerja Slack Anda untuk Aktifkan panggilan di Slack, menggunakan Amazon Chime.

Migrasi ruang kerja ke organisasi

Jika Anda memiliki organisasi Slack, Anda dapat memigrasikan ruang kerja ke organisasi tersebut. Untuk informasi selengkapnya tentang memigrasi ruang kerja, lihat Memigrasi ruang kerja ke Enterprise Grid di bantuan Slack.

Mengaitkan ruang kerja dengan akun Amazon Chime Team

Kaitkan ruang kerja Anda dengan akun Amazon Chime Team untuk mengelola izin pengguna. Anda dapat memutakhirkan host rapat ke Amazon Chime Pro sehingga mereka dapat memulai rapat dengan hingga 250 peserta dan 25 ubin video, dan menyertakan nomor telepon untuk dipanggil untuk audio. Tetapkan izin Amazon Chime Basic kepada pengguna sehingga mereka dapat one-on-one memulai rapat atau bergabung dengan rapat Amazon Chime. Untuk informasi selengkapnya, lihat Harga Amazon Chime.

> **Note**
>
> Jika Anda mengaitkan akun Amazon Chime Team dengan ruang kerja Slack, pengguna dapat masuk ke Amazon Chime dari Aplikasi Rapat Amazon Chime untuk Slack. Anda dapat mengubah pengaturan ini kapan saja. Untuk informasi selengkapnya, lihat Mengelola pengaturan rapat.

Sebelum Anda dapat mengaitkan ruang kerja Slack Anda dengan akun Amazon Chime Team, Anda harus membuat akun. AWS Untuk informasi selengkapnya tentang cara membuat AWS akun, lihatPrasyarat untuk administrator sistem Amazon Chime.

Untuk mengaitkan ruang kerja Slack Anda dengan akun Amazon Chime Team saat menginstal Aplikasi Amazon Chime Meetings untuk Slack

1. Segera setelah menginstal Aplikasi Amazon Chime Meetings untuk Slack di ruang kerja Slack Anda, pilih Tingkatkan sekarang.
2. Ikuti petunjuk untuk masuk ke konsol Amazon Chime menggunakan kredenal akun AWS Anda.
3. Ikuti petunjuk untuk membuat akun Tim baru di Amazon Chime atau pilih yang sudah ada.

    - Buat akun baru — Buat akun Amazon Chime baru untuk mengundang pengguna Slack Anda. Masukkan nama akun, pilih apakah akan mengundang pengguna Slack Anda, lalu pilih Buat.
    - Pilih akun yang sudah ada — Pilih akun Amazon Chime yang ada untuk mengundang pengguna Slack Anda. Pilih akun, lalu pilih Undang.

Saat Anda mengundang pengguna Slack untuk bergabung dengan Amazon Chime, mereka menerima undangan email. Ketika mereka menerima undangan, mereka secara otomatis ditingkatkan ke Amazon Chime Pro.

Jika Anda tidak mengaitkan ruang kerja Slack Anda dengan akun Amazon Chime Team saat menginstal Aplikasi Amazon Chime Meetings untuk Slack, Anda dapat melakukannya setelah fakta dengan menggunakan langkah-langkah berikut.

Untuk mengaitkan ruang kerja Slack Anda dengan akun Amazon Chime Team setelah menginstal Aplikasi Amazon Chime Meetings for Slack

1. Masuk ke AWS akun Anda.
2. Masuk ke ruang kerja Slack Anda sebagai administrator.

3. Pergi ke https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Ikuti petunjuk untuk membuat akun Tim baru di Amazon Chime atau pilih akun yang sudah ada.

   - Buat akun baru — Buat akun Amazon Chime baru untuk mengundang pengguna Slack Anda. Masukkan nama akun, pilih apakah akan mengundang pengguna Slack Anda, lalu pilih Buat.
   - Pilih akun yang sudah ada — Pilih akun Amazon Chime yang ada untuk mengundang pengguna Slack Anda. Pilih akun, lalu pilih Undang.

Mengelola pengguna

> **Note**
>
> Langkah-langkah di bagian ini mengasumsikan bahwa Anda memiliki satu set alamat email pengguna, atau bahwa Anda telah menghubungkan akun administrator Anda ke Active Directory. Untuk informasi lebih lanjut, lihatMenghubungkan ke Active Directory, dalam panduan ini.

Anda menggunakan konsol Amazon Chime untuk menambah dan mengelola pengguna. Anda menambahkan pengguna dengan mengundang mereka. Saat mereka menerima undangan Anda, mereka muncul di bawah Pengguna, yang mencantumkan semua pengguna di akun Anda dan detail pengguna mereka. Untuk informasi selengkapnya, lihat Melihat detail pengguna.

Administrator akun yang menggunakan Login with Amazon (LWA) juga melihat opsi untuk mengelola tingkatan izin dan menghapus pengguna dari akun. Tindakan ini dikelola melalui Active Directory atau Okta, tergantung pada yang mana Anda mengonfigurasi akun untuk digunakan. Untuk informasi selengkapnya, lihat Mengelola izin dan akses pengguna.

Daftar Isi

Menambahkan pengguna

Anda menambahkan pengguna ke akun Amazon Chime dengan mengundang mereka untuk bergabung dengan akun tersebut. Anda mengirim undangan ke calon pengguna dari konsol Amazon Chime, dan langkah-langkah ini menjelaskan caranya.

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.

   Daftar akun yang Anda kelola muncul.
2. Pilih akun yang ingin Anda tambahkan anggota, lalu pilih Undang pengguna.

   Kotak dialog Undang pengguna baru muncul.
3. Masukkan alamat email pengguna yang ingin Anda undang. Pisahkan setiap alamat dengan titik koma (;).
4. Pilih Undang pengguna.

Pengguna baru muncul dalam daftar. Saat Anda mengundang pengguna ke akun Tim, detail mereka tidak akan muncul sampai mereka menerima undangan Anda.

Melihat detail pengguna

Di konsol Amazon Chime, di bawah Pengguna, Anda dapat melihat daftar semua pengguna di akun Anda dan melihat detail pengguna mereka. Cari pengguna tertentu berdasarkan alamat email mereka dan pilih nama mereka untuk melihat detail pengguna mereka. Di bawah rincian Pengguna, Anda dapat melihat informasi rinci tentang pengguna, dan membuat pembaruan ke akun pengguna mereka.

Tabel berikut mencantumkan detail pengguna yang muncul di konsol.

> **Note**
>
> Detail pengguna lengkap tidak muncul untuk pengguna akun Tim sampai setelah mereka menerima undangan mereka.

Bidang	Deskripsi	Contoh
Nama tampilan	Nama pengguna yang muncul di Amazon Chime. Untuk pengguna Login with Amazon (LWA), ini adalah nama lengkapnya. Untuk pengguna	Mayor, Mary

Bidang	Deskripsi	Contoh
	Active Directory, DISPLAY_NAME_ATTRIBUTE digunakan.	
Alamat email	Untuk pengguna LWA, alamat email yang digunakan untuk pendaftaran. Untuk pengguna Active Directory, alamat email utama dari Active Directory akan muncul.	mary.major@example.com
Registrasi	Status pendaftaran pengguna saat ini. Nilai yang mungkin berbeda antara akun Enterprise, di mana undangan tidak dikirim, dan akun Tim, tempat undangan dikirim.	Terdaftar, Tidak Terdaftar (untuk akun Tim), atau Ditangguhkan (untuk akun Perusahaan)
Tingkat izin	Setel ke Pro secara default, untuk memungkinkan pengguna menyelenggarakan rapat. Hal ini dapat diubah menjadi Basic.	Pro, Dasar
Diundang	Untuk akun Tim, tanggal ketika pengguna diundang ke akun.	01/05/2020
Bergabung	Tanggal ketika pengguna pertama kali masuk ke Amazon Chime. Untuk pengguna uji coba Pro, ini juga merupakan tanggal uji coba Pro mereka dimulai.	01/10/2020

Bidang	Deskripsi	Contoh
PIN pribadi	PIN rapat pribadi yang dapat digunakan pengguna untuk menjadwalkan rapat.	0123456789
Pengaturan privasi	Pengaturan kehadiran yang dipilih pengguna.	Publik atau Pribadi
Pertemuan yang dihadiri	Jumlah pertemuan yang telah dihadiri pengguna.	87
Pertemuan diselenggarakan	Jumlah pertemuan yang telah diselenggarakan pengguna.	12
Kepuasan pertemuan	Persentase tanggapan positif yang diberikan pada end-of-meeting survei.	92%
Tanggal aktif terakhir	Tanggal ketika pengguna terakhir aktif.	06/12/2020
Pesan obrolan terkirim	Jumlah pesan obrolan yang dikirim pengguna.	1025
Nomor telepon	Nomor telepon yang ditetapkan untuk pengguna, jika ada.	+12065550100

Mengelola izin dan akses pengguna

Kelola fitur mana yang dapat diakses pengguna Amazon Chime Anda dengan memberi mereka izin Pro atau Dasar. Pengguna dengan izin Dasar tidak dapat menyelenggarakan rapat, tetapi mereka dapat menghadiri rapat dan menggunakan obrolan. Untuk informasi selengkapnya tentang fitur yang dapat diakses pengguna dengan izin Pro dan Dasar, lihat Paket dan harga.

Kelola siapa yang dapat masuk ke akun administratif Amazon Chime Anda dengan mengundang atau menangguhkan pengguna. Hanya administrator akun Enterprise yang dapat menangguhkan pengguna. Administrator akun tim dapat menghapus pengguna dari akun mereka sehingga

mereka tidak lagi membayar izin pengguna. Namun, mereka tidak dapat menangguhkan pengguna untuk mencegah mereka masuk. Untuk informasi selengkapnya tentang perbedaan antara akun Perusahaan dan Tim, lihatMengelola akun Amazon Chime Anda.

Mengelola izin pengguna

Sebagai administrator Amazon Chime, Anda dapat mengelola izin Pro dan Dasar untuk pengguna di akun Amazon Chime Anda.

Jika Active Directory atau Okta dikonfigurasi untuk akun Amazon Chime Anda, kelola izin pengguna melalui keanggotaan grup direktori mereka. Jika Anda tidak memiliki Direktori Aktif atau Okta yang dikonfigurasi, kelola izin pengguna dari konsol Amazon Chime.

Akun tim dan Enterprise Login with Amazon

Jika Anda mengelola akun Amazon Chime Team atau akun Enterprise LWA, tempat pengguna masuk dengan akun Login with Amazon (LWA) mereka, Anda dapat mengelola izin Pro dan Dasar di konsol Amazon Chime.

Untuk mengelola izin pengguna untuk akun LWA Tim dan Perusahaan

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun Amazon Chime.
3. Pilih Pengguna.
4. Pilih pengguna dan pilih Tindakan, Tetapkan izin.
5. Pilih salah satu izin berikut:
   - Pro
   - Basic
6. PilihTetapkan.

Akun Enterprise Active Directory atau Enterprise OpenID Connect (Okta)

Jika pengguna Anda masuk dengan kredensyal Active Directory atau Okta, kelola izin mereka dengan menjadikannya anggota grup direktori yang memiliki izin Pro atau Dasar yang ditetapkan padanya.

Untuk menetapkan izin Pro kepada pengguna, jadikan mereka anggota Active Directory atau grup Okta yang telah Anda tetapkan izin Pro. Untuk menetapkan izin Dasar kepada pengguna, jadikan

mereka anggota grup yang telah Anda tetapkan izin Dasar. Pengguna yang tidak memiliki izin Pro atau Dasar tidak dapat masuk ke Amazon Chime.

Mengelola akses pengguna

Jika Anda mengelola akun Amazon Chime, Anda dapat mengundang pengguna untuk mengizinkan mereka masuk ke akun Anda. Administrator akun perusahaan dapat menangguhkan akses pengguna untuk mencegah mereka masuk ke akun.

Mengundang dan menghapus pengguna akun Tim

Jika Anda mengelola akun Tim, gunakan konsol Amazon Chime untuk mengundang pengguna dari domain email apa pun.

> **Note**
>
> Uji coba Pro 30 hari gratis pengguna berakhir ketika mereka menerima undangan Anda.

Mengundang pengguna ke akun Team

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun Tim.
3. Pilih Pengguna, Undang pengguna.
4. Masukkan alamat email pengguna yang akan diundang, pisahkan beberapa alamat email dengan titik koma (). **;**
5. Pilih Undang pengguna.

Prosedur berikut memisahkan pengguna dari akun Tim Anda dengan menghapus izin Pro atau Dasar apa pun yang diberikan kepada mereka. Pengguna yang dihapus masih dapat masuk ke Amazon Chime, tetapi mereka bukan lagi anggota berbayar dari akun Amazon Chime Anda.

Untuk menghapus pengguna dari akun Tim

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun Tim.
3. Pilih Pengguna.
4. Pilih pengguna yang akan dihapus dan pilih Tindakan, Hapus pengguna.

Izin Pro atau Dasar apa pun yang diberikan kepada pengguna akan dihapus. Pengguna tidak dapat lagi menggunakan pelengkapan otomatis untuk menemukan pengguna Tim baru di Kontak mereka.

Mengundang dan menangguhkan pengguna akun Enterprise

Jika Anda mengelola akun Enterprise, setiap pengguna yang mendaftar untuk Amazon Chime dengan alamat email dari domain yang diklaim secara otomatis ditambahkan ke akun Anda. Jika Anda mengonfigurasi Active Directory atau Okta, pengguna juga harus menjadi anggota grup direktori yang Anda konfigurasikan untuk Amazon Chime.

Mengundang pengguna ke akun Enterprise

- Kirim email undangan ke pengguna di organisasi Anda dan instruksikan mereka untuk mengikuti langkah-langkah dalam Membuat akun Amazon Chime di Panduan Pengguna Amazon Chime.

Pengguna masuk dengan alamat email dari salah satu domain yang Anda klaim untuk akun Anda. Setelah mereka menyelesaikan langkah-langkah untuk membuat akun pengguna Amazon Chime mereka, akun tersebut secara otomatis muncul di bawah Pengguna akun Enterprise Anda di konsol Amazon Chime.

Prosedur berikut menangguhkan pengguna dari akun Enterprise yang tidak memiliki Active Directory atau Okta dikonfigurasi. Ini mencegah pengguna masuk ke Amazon Chime.

Untuk menangguhkan pengguna dari akun Enterprise

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Akun, pilih nama akun Enterprise.
3. Pilih Pengguna.
4. Pilih pengguna yang akan ditangguhkan dan pilih Tindakan, Tangguhkan pengguna.
5. Pilih kotak centang dan pilih Tangguhkan.

Jika Anda memiliki Active Directory atau Okta yang dikonfigurasi untuk akun Enterprise Anda, gunakan prosedur berikut untuk menangguhkan pengguna.

Untuk menangguhkan pengguna dari akun Enterprise Active Directory atau OpenID Connect (Okta)

- Lakukan salah satu hal berikut:

- Dari Active Directory atau Okta Administrator Dashboard, tangguhkan pengguna atau tandai mereka tidak aktif.
- Hapus pengguna dari grup Active Directory yang memiliki izin Dasar atau Pro yang ditetapkan padanya.

Mengubah PIN Rapat Pribadi

PIN rapat pribadi adalah ID statis yang dihasilkan saat pengguna mendaftar. PIN memudahkan pengguna Amazon Chime untuk menjadwalkan pertemuan dengan pengguna Amazon Chime lainnya. Menggunakan PIN rapat pribadi berarti penyelenggara rapat tidak perlu mengingat detail rapat untuk setiap rapat baru yang mereka jadwalkan.

Jika pengguna merasa bahwa PIN rapat pribadi mereka telah dikompromikan, Anda dapat mengatur ulang PIN mereka dan membuat ID baru. Setelah memperbarui PIN rapat pribadi, pengguna harus memperbarui semua rapat yang dijadwalkan menggunakan PIN rapat pribadi lama.

Mengubah PIN Rapat Pribadi

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Amazon Chime.
3. Di panel navigasi, pilih Pengguna.
4. Cari pengguna yang membutuhkan PIN mereka diubah.
5. Untuk membuka halaman detail Pengguna, pilih nama pengguna.
6. Pilih Tindakan pengguna, Setel ulang PIN pribadi, Konfirmasi.

Mengelola uji coba Pro

Ketika pengguna menerima undangan Amazon Chime Team atau ditambahkan ke akun Enterprise, uji coba gratis mereka berakhir dan mereka memiliki izin Pro. Hal ini memungkinkan mereka untuk terus menyelenggarakan pertemuan yang dijadwalkan. Mengubah tingkat izin pengguna ke Basic mencegah mereka bertindak sebagai host rapat.

Dengan harga berbasis penggunaan Amazon Chime, Anda hanya membayar untuk pengguna yang menyelenggarakan rapat pada hari-hari mereka menyelenggarakannya. Peserta rapat dan pengguna obrolan tidak dikenakan biaya.

Pengguna Pro dianggap Pro Aktif jika mereka menyelenggarakan rapat yang berakhir pada hari kalender dan setidaknya salah satu dari yang berikut terjadi:

- Pertemuan itu dijadwalkan.
- Pertemuan tersebut melibatkan lebih dari dua peserta.
- Pertemuan itu memiliki setidaknya satu acara rekaman.
- Pertemuan itu termasuk seorang peserta yang menelepon.
- Pertemuan tersebut termasuk peserta yang bergabung dengan H.323 atau SIP.

Untuk informasi selengkapnya, lihat Paket dan Harga.

Meminta lampiran pengguna

Jika Anda mengelola akun Enterprise dan memiliki izin yang sesuai, Anda dapat meminta dan menerima lampiran yang diunggah pengguna ke Amazon Chime. Anda bisa mendapatkan lampiran yang diunggah pengguna ke percakapan 1:1 dan grup, atau ke ruang obrolan yang mereka buat.

> **Note**
>
> Jika Anda mengelola akun Amazon Chime Team, Anda dapat meningkatkan ke akun Enterprise dengan mengklaim satu atau beberapa domain. Atau, Anda dapat menghapus pengguna dari akun Tim, yang memungkinkan pengguna yang tidak dikelola tersebut untuk mendapatkan lampiran mereka menggunakan Amazon Chime Assistant.

Untuk meminta lampiran pengguna

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada halaman Akun, pilih nama akun Amazon Chime.
3. Di bawah Pengaturan, pilih Akun, Tindakan akun, Permintaan lampiran.
4. Dalam waktu sekitar 24 jam, halaman ringkasan Akun menyediakan tautan ke file yang berisi daftar URL yang telah ditetapkan sebelumnya yang Anda gunakan untuk mengakses setiap lampiran.
5. Unduh filenya.

> **Note**
>
> Pastikan untuk mempertahankan tingkat kontrol akses yang sesuai pada file. Setiap pengguna yang memperoleh file dapat menggunakan daftar URL yang disediakan untuk mengunduh lampiran terkait.
> URL yang ditetapkan sebelumnya akan kedaluwarsa setelah 6 hari. Anda dapat mengirimkan permintaan satu kali setiap 7 hari.

Untuk menggunakan kebijakan AWS Identity and Access Management (IAM) untuk mengelola akses ke konsol administrasi Amazon Chime dan tindakan Minta lampiran, gunakan salah satu kebijakan FullAccess terkelola Amazon Chime (,, atau). UserManagement ReadOnly Atau, Anda dapat memperbarui kebijakan khusus untuk menyertakan `StartDataExport` tindakan dan `RetrieveDataExport` tindakan. Untuk informasi selengkapnya tentang tindakan ini, lihat Tindakan yang ditentukan oleh Amazon Chime di Panduan Pengguna IAM.

Bagaimana Amazon Chime mengelola pembaruan otomatis

Amazon Chime menyediakan berbagai cara untuk memperbarui kliennya. Metodenya bervariasi, tergantung pada apakah Anda menjalankan Amazon Chime di browser, di desktop, atau di perangkat seluler.

Aplikasi web Amazon Chime - https://app.chime.aws - selalu memuat dengan fitur terbaru dan perbaikan keamanan.

Klien desktop Amazon Chime memeriksa pembaruan setiap kali Anda memilih Keluar atau Keluar. Ini berlaku untuk mesin Windows dan macOS. Saat Anda menjalankan klien, ia memeriksa pembaruan setiap tiga jam. Anda juga dapat memeriksa pembaruan dengan memilih Periksa Pembaruan di menu Bantuan Windows atau di menu MacOS Amazon Chime.

Saat klien desktop mendeteksi pembaruan, Amazon Chime meminta pengguna untuk menginstalnya kecuali mereka sedang dalam rapat yang sedang berlangsung. Mereka sedang dalam pertemuan yang sedang berlangsung ketika:

- Mereka menghadiri pertemuan.
- Mereka diundang ke pertemuan yang masih berlangsung.

Amazon Chime meminta mereka untuk menginstal versi terbaru, dan menyediakan hitungan mundur 15 detik sehingga mereka dapat menunda instalasi. Pengguna memilih Coba Nanti untuk menunda pembaruan.

Jika pengguna menunda pembaruan, dan mereka tidak dalam rapat yang sedang berlangsung, klien memeriksa pembaruan setelah tiga jam dan meminta mereka untuk menginstal lagi. Instalasi dimulai ketika hitungan mundur berakhir.

> **Note**
>
> Pada mesin macOS, pengguna harus memilih Restart Now untuk memulai pembaruan.

Di perangkat seluler - Aplikasi seluler Amazon Chime menggunakan opsi pembaruan yang disediakan oleh App Store dan Google Play untuk menghadirkan versi terbaru klien Amazon Chime. Anda juga dapat menggunakan sistem manajemen perangkat seluler untuk menyebarkan pembaruan.

Migrasi pengguna ke akun Tim lain

Anda memigrasikan pengguna ke akun Tim lain dengan membuat dan mengonfigurasi akun tujuan, jika akun tersebut belum ada. Kemudian Anda menambahkan pengguna ke akun tujuan. Langkah-langkah berikut membawa Anda ke informasi tentang menyelesaikan setiap bagian migrasi.

Untuk memigrasikan pengguna

1. Jika Anda tidak memiliki akun Tim tujuan, buat satu. Untuk informasi selengkapnya, lihat Langkah 1: Membuat akun administrator Amazon Chime.
2. Sesuai kebutuhan, konfigurasikan akun. Untuk informasi selengkapnya, lihat Langkah 2 (opsional): Mengkonfigurasi pengaturan akun.
3. Tambahkan pengguna ke akun. Untuk informasi selengkapnya, lihat Langkah 3: Menambahkan pengguna ke akun Anda.

Mengelola nomor telepon di Amazon Chime

Anda menggunakan Gunakan konsol Amazon Chime untuk menyediakan nomor telepon. Saat Anda memberikan nomor, Anda memintanya dari kumpulan nomor yang dikelola oleh Amazon Chime. Ketika Anda membatalkan penetapan dan kemudian menghapus nomor, mereka kembali ke kolam. Saat Anda mem-port nomor, Anda memindahkannya ke dalam dan keluar dari Amazon Chime.

> **Note**
>
> Saat menggunakan konsol Amazon Chime, Anda hanya dapat menyediakan nomor Panggilan Bisnis Amazon Chime. Jika Anda memerlukan nomor internasional, Anda menggunakan Amazon Chime Voice Connectors dan aplikasi media SIP. Untuk melakukan itu, Anda harus terlebih dahulu membuat akun administratif Amazon Chime SDK. Untuk informasi selengkapnya, lihat topik berikut di Panduan Administrator SDK Amazon Chime:
>
> - Prasyarat
> - Mengelola inventaris nomor telepon
> - Mengelola Konektor Suara
> - Mengelola aplikasi media SIP

Topik di bagian berikut menjelaskan cara menyediakan dan mengelola nomor telepon Amazon Chime.

Daftar Isi

Menyediakan nomor telepon

Gunakan konsol Amazon Chime untuk menyediakan nomor telepon untuk akun Amazon Chime Anda. Angka-angka tersebut berasal dari kumpulan yang dikelola oleh Amazon Chime. Pilih Panggilan Bisnis Amazon Chime untuk menyediakan dan menetapkan nomor telepon ke pengguna Amazon Chime yang ada.

Saat penyediaan selesai, nomor telepon akan muncul di Inventaris Anda. Anda kemudian menetapkannya ke pengguna individu.

Untuk memberikan nomor telepon

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pilih Pesanan, Nomor telepon Penyediaan.
4. Pilih Panggilan Bisnis, lalu pilih Berikutnya.
5. Cari nomor telepon yang tersedia. Pilih nomor telepon yang Anda inginkan, lalu pilih Ketentuan.

Nomor telepon muncul di daftar Pesanan dan Pending Anda saat penyediaan terjadi.

Porting nomor telepon yang ada

Selain menyediakan nomor telepon, Anda juga dapat mem-port nomor dari operator telepon ke inventaris Anda. Ini termasuk nomor bebas pulsa.

> **Note**
>
> Jika Anda perlu mem-port nomor internasional, menggunakan Amazon Chime Voice Connector, atau menggunakan aplikasi media SIP, Anda harus membuat akun administrator Amazon Chime SDK dan menggunakan konsol Amazon Chime SDK. Untuk informasi selengkapnya tentang melakukan itu, lihat Prasyarat, di Panduan Administrator Amazon Chime SDK.

Bagian berikut menjelaskan cara mem-port nomor telepon.

Topik

Prasyarat untuk nomor porting

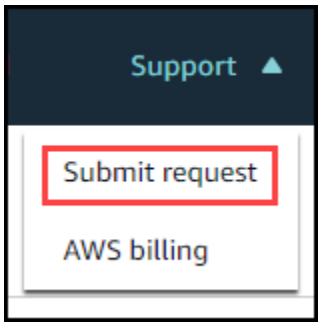
Untuk nomor port, Anda harus memiliki Letter of Agency (LOA). Anda harus memiliki LOA untuk nomor telepon domestik. Unduh formulir Letter of Agency (LOA) dan isi. Jika Anda perlu mem-port nomor telepon dari operator yang berbeda, isi LOA terpisah untuk setiap operator.

Porting nomor telepon di

Anda membuat permintaan dukungan untuk mem-port nomor telepon yang ada.

Untuk mem-port nomor telepon yang ada

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pada bilah perintah di bagian atas halaman, pilih Support, lalu pilih Kirim permintaan.



Itu membawa Anda ke konsol AWS Support.

> **Note**
>
> Anda juga bisa langsung menuju ke halaman AWS Support tengah. Jika Anda melakukannya, pilih Buat kasus, lalu ikuti langkah-langkah di bawah ini.

3. Di bawah Bagaimana kami dapat membantu, lakukan hal berikut:

   a. Pilih Akun dan penagihan.

   b. Dari daftar Layanan, pilih Chime SDK (Number Management).

   c. Dari daftar Kategori, pilih Port Nomor Telepon Masuk.

   d. Pilih Langkah selanjutnya: Informasi tambahan.

4. Di bawah Informasi tambahan, lakukan hal berikut

   a. Di bawah Subjek, masukkan**`Porting phone numbers in`**.

   b. Di bawah Deskripsi, masukkan informasi berikut:

      Untuk porting nomor AS:

      - Nomor Telepon Penagihan (BTN) dari rekening.
      - Mengotorisasi nama orang. Ini adalah orang yang bertanggung jawab atas penagihan akun dengan operator saat ini.
      - Operator saat ini, jika diketahui.
      - Nomor akun layanan, jika informasi ini hadir dengan operator saat ini.
      - PIN layanan, jika tersedia.
      - Alamat layanan dan nama pelanggan, seperti yang muncul dalam kontrak operator Anda saat ini.
      - Tanggal dan waktu yang diminta untuk port.
      - (Opsional) Jika Anda ingin mem-port Nomor Telepon Penagihan (BTN), pilih salah satu opsi berikut:
        - Saya mem-porting BTN saya dan saya ingin menggantinya dengan BTN baru yang saya sediakan. Saya dapat mengonfirmasi bahwa BTN baru ini ada di akun yang sama dengan operator saat ini.
        - Saya mem-porting BTN saya dan saya ingin menutup akun saya dengan operator saya saat ini.
        - Saya mem-porting BTN saya karena akun saya saat ini sudah diatur sehingga setiap nomor telepon adalah BTN miliknya sendiri. (Pilih opsi ini hanya jika akun Anda dengan operator saat ini diatur dengan cara ini.)
        - Setelah Anda memilih opsi, lampirkan Letter of Agency (LOA) Anda ke permintaan.

Untuk porting nomor internasional:

- Anda harus menggunakan tipe produk SIP Media Application Dial-In untuk nomor telepon non-AS.
- Jenis nomor (Lokal atau Bebas Pulsa)
- Nomor telepon yang ada untuk port in.
- Perkirakan volume penggunaan
- Negara

c. Dari daftar jenis nomor telepon, pilih Panggilan Bisnis, Panggilan Aplikasi Media SIP, atau Konektor Suara.

d. Di bawah Nomor telepon, masukkan setidaknya satu nomor telepon, bahkan jika Anda mem-porting beberapa nomor.

e. Di bawah Tanggal Porting, masukkan tanggal porting yang diinginkan.

f. Di bawah Porting Time, masukkan waktu yang diinginkan.

g. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.

5. Di bawah Selesaikan sekarang atau hubungi kami, pilih Hubungi kami.
6. Dari daftar bahasa kontak pilihan, pilih bahasa
7. Pilih Web atau Telepon. Jika Anda memilih Telepon, masukkan nomor telepon Anda. Setelah selesai, pilih Kirim.

AWS Support memberi tahu Anda apakah nomor telepon Anda dapat di-porting dari operator telepon yang ada. Jika Anda bisa, Anda harus mengirimkan dokumen yang diperlukan. Langkah-langkah di bagian selanjutnya menjelaskan cara mengirimkan dokumen-dokumen tersebut.

Mengirimkan dokumen yang diperlukan

Setelah AWS Support mengatakan Anda dapat mem-port nomor telepon, Anda harus mengirimkan dokumen yang diperlukan. Langkah-langkah berikut menjelaskan caranya.

> **Note**
>
> AWS Support menyediakan tautan Amazon S3 yang aman untuk mengunggah semua dokumen yang diminta. Jangan melanjutkan sampai Anda menerima tautan.

Untuk mengirimkan dokumen

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Masuk ke AWS akun Anda, lalu buka tautan unggahan Amazon S3 yang dibuat khusus untuk akun Anda.

   > **Note**
   >
   > Tautan kedaluwarsa setelah sepuluh hari. Ini dibuat khusus untuk akun yang membuat kasus. Tautan mengharuskan pengguna yang berwenang dari akun untuk melakukan unggahan.

3. Pilih Tambahkan File, lalu pilih dokumen identitas yang terkait dengan permintaan Anda.
4. Perluas bagian Izin, dan pilih Tentukan izin ACL individual.
5. Di akhir bagian Access control list (ACL), pilih Add granttee, lalu paste kunci yang disediakan oleh AWS Support ke dalam kotak Grantee.
6. Di bawah Objek, pilih kotak centang Baca, lalu pilih Unggah.

Setelah Anda memberikan Letter of Agency (LOA), AWS Support konfirmasikan dengan operator telepon Anda yang ada bahwa informasi pada LOA sudah benar. Jika informasi yang diberikan di LOA tidak sesuai dengan informasi yang dimiliki operator telepon Anda, AWS Support hubungi Anda untuk memperbarui informasi yang diberikan di LOA.

Melihat status permintaan

Langkah-langkah berikut menjelaskan cara menggunakan konsol Amazon Chime untuk melihat status permintaan porting Anda.

Untuk melihat status

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, pilih Manajemen nomor telepon.
3. Pilih tab Pesanan.

Kolom Status menunjukkan status permintaan Anda. AWS Support juga menghubungi Anda dengan pembaruan dan permintaan untuk informasi lebih lanjut, sesuai kebutuhan. Untuk informasi lebih lanjut, lihatDefinisi status porting nomor telepon, nanti di bagian ini.

Menetapkan nomor porting

Setelah operator telepon Anda mengonfirmasi bahwa LOA benar, mereka meninjau dan menyetujui port yang diminta. Kemudian mereka memberikan AWS Support tanggal dan waktu Firm Order Commit (FOC) agar port terjadi.

Pada tanggal FOC, nomor telepon yang di-porting diaktifkan untuk digunakan. Anda kemudian harus menetapkan nomor kepada pengguna di akun yang diinginkan.

Untuk menetapkan nomor telepon

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, pilih Manajemen nomor telepon.
3. Pada tab Inventaris, pilih kotak centang di sebelah nomor yang ingin Anda tetapkan, lalu pilih Tetapkan.

   > **Note**
   >
   > Anda hanya dapat memilih satu nomor dalam satu waktu.

4. Pada halaman Tetapkan nomor telepon +1 ke profil pengguna, pilih akun untuk nomor tersebut, lalu pilih Berikutnya.
5. Pilih pengguna yang ingin Anda tetapkan nomornya, lalu pilih Tetapkan.

Mem-porting nomor telepon keluar

Anda mem-port nomor dari Amazon Chime dengan memulai permintaan porting dengan operator pemenang Anda. Saat mengirimkan informasi ke operator pemenang Anda, sertakan ID AWS akun Anda sebagai ID akun yang terkait dengan nomor telepon yang sedang di-porting.

Ketika proses porting selesai dan operator pemenang Anda memiliki nomor, Anda harus membatalkan penetapan dan menghapus angka-angka itu dari inventaris Anda. Untuk informasi lebih lanjut, lihat Membatalkan penetapan nomor telepon Amazon Chime Business Calling dan Menghapus nomor telepon di panduan ini.

> **Important**
>
> - Kemampuan untuk mem-port nomor tergantung pada kemampuan operator yang menang untuk menerima angka-angka itu.
> - Memverifikasi keaslian permintaan port-out operator yang menang sangat penting untuk keamanan nomor telepon Anda. Jika detail akun tidak benar (misalnya, ada ketidakcocokan ID akun), permintaan port-out Anda mungkin ditolak, menyebabkan penundaan dan mengharuskan Anda untuk mengirimkan kembali permintaan Anda.

(Opsional) Cara meminta PIN untuk melindungi nomor Anda

Untuk keamanan tambahan, Anda dapat menghubungi kami untuk menerapkan PIN ke nomor Anda. Operator yang menang kemudian menggunakan PIN itu. Ikuti langkah-langkah ini:

Untuk meminta PIN

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Hubungi Kami, pilih Support.

   Itu membawa Anda ke konsol AWS Support.

   > **Note**
   >
   > Anda juga bisa langsung menuju ke halaman AWS Support tengah. Jika Anda melakukannya, pilih Buat kasus, lalu ikuti langkah-langkah di bawah ini.

3. Di bawah Bagaimana kami dapat membantu, lakukan hal berikut:
   a. Pilih Akun dan penagihan.
   b. Dari daftar Layanan, pilih Chime SDK (Number Management).
   c. Dari daftar Kategori, pilih Nomor Telepon Port Out.
   d. Pilih Langkah selanjutnya: Informasi tambahan.
4. Di bawah Informasi tambahan, lakukan hal berikut
   a. Di bawah Subjek, masukkan**`Porting phone numbers out`**.
   b. Di bawah Deskripsi, masukkan yang berikut ini.

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

> **Note**
>
> Anda harus memberikan PIN alfanumerik 4 - 10 karakter.

AWS Support mengaitkan PIN dengan nomor telepon. Saat meminta port dengan operator pemenang Anda, berikan ID AWS akun dan PIN Anda. Kami akan menggunakan informasi tersebut untuk memvalidasi setiap permintaan port yang diterima untuk nomor Anda.

Definisi status porting nomor telepon

Setelah mengirimkan permintaan untuk mem-port nomor telepon yang ada ke Amazon Chime, Anda dapat melihat status permintaan porting Anda di konsol Amazon Chime di bawah Panggilan, Manajemen nomor telepon, Tertunda.

Status dan definisi porting meliputi yang berikut:

DIBATALKAN

AWS Support membatalkan pesanan porting karena masalah dengan port, seperti permintaan pembatalan dari operator atau dari Anda. AWS Support menghubungi Anda dengan detail.

CANCEL_REQUEST

AWS Support memproses pembatalan pesanan porting karena masalah dengan port, seperti permintaan pembatalan dari operator atau dari Anda. AWS Support menghubungi Anda dengan detail.

CHANGE_REQUEST

AWS Support sedang memproses permintaan perubahan Anda, dan respons operator tertunda. Memungkinkan waktu pemrosesan tambahan.

DISELESAIKAN

Pesanan porting Anda selesai, dan nomor telepon Anda diaktifkan.

PENGECUALIAN

AWS Support menghubungi Anda untuk detail tambahan yang diperlukan untuk menyelesaikan permintaan port. Memungkinkan waktu pemrosesan tambahan.

FOC

Tanggal FOC dikonfirmasi dengan operator. AWS Support menghubungi Anda untuk mengonfirmasi tanggal.

DOKUMEN YANG TERTUNDA

AWS Support menghubungi Anda untuk dokumen tambahan yang diperlukan untuk menyelesaikan permintaan port. Memungkinkan waktu pemrosesan tambahan.

DIKIRIMKAN

Pesanan porting Anda dikirimkan, dan respons operator tertunda.

Menetapkan nomor telepon Amazon Chime Business Calling

Gunakan halaman Inventaris manajemen nomor telepon untuk menetapkan nomor telepon Panggilan Bisnis Amazon Chime kepada pengguna individu.

Untuk menetapkan nomor telepon Amazon Chime Business Calling

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pada tab Inventaris, pilih nomor telepon yang ingin Anda tetapkan.
4. PilihTetapkan.
5. Pilih akun yang dimiliki pengguna, lalu pilih Berikutnya.
6. Pilih pengguna, lalu pilih Tetapkan.

Saat Anda mengubah izin nomor telepon atau nomor telepon, sebaiknya berikan informasi baru atau izin kepada pengguna. Sebelum pengguna dapat mengakses nomor telepon atau fitur izin baru mereka, mereka harus keluar dari akun Amazon Chime mereka dan masuk lagi.

Membatalkan penetapan nomor telepon Amazon Chime Business Calling

Prosedur berikut membatalkan penetapan nomor telepon dari pengguna Amazon Chime Business Calling.

Untuk membatalkan penetapan nomor telepon

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pada tab Inventaris, pilih nomor telepon yang ingin Anda batalkan.
4. Pilih Unassign.
5. Pilih kotak centang, dan pilih Unassign.

Anda dapat melihat detail untuk angka-angka dalam inventaris Anda. Misalnya, Anda dapat melihat apakah panggilan telepon dan pesan teks diaktifkan.

Untuk melihat detail nomor telepon inventaris

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pilih tab Inventaris, lalu pilih nomor telepon yang ingin Anda lihat.
4. Buka daftar Tindakan dan pilih Lihat detail.

Menggunakan nama panggilan keluar

Nama panggilan keluar bertindak sebagai ID penelepon. Anda dapat menetapkan nama panggilan default untuk satu atau beberapa nomor telepon dalam inventaris Anda. Anda juga dapat mengatur nama panggilan unik untuk nomor telepon individual. Nama-nama tersebut kemudian muncul ke penerima panggilan keluar yang dilakukan menggunakan nomor telepon tersebut. Nama panggilan berlaku untuk semua jenis produk nomor telepon. Anda dapat memperbarui nama setiap tujuh hari sekali.

Misalnya, Anda dapat menetapkan nama panggilan default Departemen 5 untuk semua nomor telepon di departemen itu. Anda juga dapat menetapkan nama unik Jane Doe untuk kepala departemen.

Langkah-langkah berikut menjelaskan cara menyetel nama panggilan keluar default dan individu.

Untuk menetapkan nama panggilan

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pada tab Inventaris, lakukan salah satu dari berikut ini: pilih kotak centang di sebelah nomor telepon yang ingin Anda perbarui.
   - Untuk menetapkan nama panggilan default untuk beberapa nomor, pilih kotak centang di sebelah nomor tersebut.
   - Untuk mengatur nama panggilan individu, pilih nomor yang diinginkan.
4. Buka daftar Tindakan dan pilih Perbarui nama panggilan default.
5. Di kotak Nama panggilan default, masukkan nama hingga 15 karakter.
6. Pilih Simpan.

Biarkan 72 jam bagi sistem untuk memperbarui nama panggilan default.

Menghapus nomor telepon

> **Important**
>
> Hanya administrator sistem Amazon Chime yang dapat menyelesaikan langkah-langkah ini. Selain itu, Anda harus membatalkan penetapan nomor telepon sebelum dapat menghapusnya.

Saat Anda memberikan nomor telepon, Anda memesannya dari kumpulan nomor yang dipertahankan Amazon Chime. Menghapus nomor memindahkannya kembali ke kolam. Ketika Anda menghapus nomor, pertama kali masuk ke antrian penghapusan Anda di mana itu ditahan selama 7 hari. Selama waktu itu, Anda dapat memindahkan nomor kembali ke inventaris Anda. Setelah 7 hari, sistem secara otomatis menghapus nomor dari antrian penahanan dan memutuskannya dari

akun Anda. Itu mengembalikan nomor ke kumpulan nomor. Jika Anda perlu merebut kembali nomor setelah sistem menghapusnya dari antrian penahanan, ikuti langkah-langkahnyaMenyediakan nomor telepon, tetapi ketahuilah bahwa nomor tersebut mungkin tidak tersedia.

Untuk menghapus nomor telepon yang tidak ditetapkan

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pilih tab Inventaris, lalu pilih nomor telepon atau nomor yang ingin Anda hapus.
4. Buka daftar Tindakan dan pilih Hapus nomor telepon.
5. Pilih kotak centang, lalu pilih Hapus.

Nomor telepon yang dihapus disimpan dalam antrean Penghapusan selama 7 hari sebelum dihapus dari inventaris Anda secara permanen.

Memulihkan nomor telepon yang dihapus

Anda dapat memulihkan nomor telepon yang dihapus dari antrean Penghapusan hingga 7 hari setelah Anda menghapusnya. Memulihkan nomor telepon memindahkannya kembali ke Inventaris Anda.

Untuk mengembalikan nomor telepon yang dihapus

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Di panel navigasi, di bawah Panggilan, pilih Manajemen nomor telepon.
3. Pilih tab Antrian penghapusan, lalu pilih nomor telepon atau nomor yang ingin Anda pulihkan.
4. Pilih Pindah ke inventaris.

Mengelola pengaturan global di Amazon Chime

Anda menggunakan konsol Amazon Chime untuk mengelola pengaturan rekaman detail panggilan.

Mengkonfigurasi catatan detail panggilan

Sebelum Anda dapat mengonfigurasi pengaturan rekaman detail panggilan untuk akun administratif Amazon Chime Anda, Anda harus terlebih dahulu membuat bucket Amazon Simple Storage Service. Bucket Amazon S3 digunakan sebagai tujuan log untuk catatan detail panggilan Anda. Saat mengonfigurasi pengaturan rekaman detail panggilan, Anda memberikan akses baca dan tulis Amazon Chime ke bucket Amazon S3 untuk menyimpan dan mengelola data Anda. Untuk informasi selengkapnya tentang membuat bucket Amazon S3, lihat Memulai Amazon Simple Storage Service dalam Panduan Pengguna Amazon Simple Storage Service.

Anda dapat mengonfigurasi pengaturan rekaman detail panggilan untuk Panggilan Bisnis Amazon Chime. Untuk informasi selengkapnya tentang Amazon Chime Business Calling, lihatMengelola nomor telepon di Amazon Chime.

Untuk mengkonfigurasi pengaturan catatan detail panggilan

1. Buat bucket Amazon S3 dengan mengikuti langkah-langkah Memulai Amazon Simple Storage Service di Panduan Pengguna Amazon Simple Storage Service.
2. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
3. Untuk Pengaturan Global, pilih Catatan detail panggilan.
4. Pilih Konfigurasi Panggilan Bisnis.
5. Untuk tujuan Log, pilih bucket Amazon S3.
6. Pilih Save (Simpan).

Anda dapat menghentikan catatan detail panggilan kapan saja.

Untuk berhenti mencatat catatan detail panggilan

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Untuk Pengaturan Global, pilih Catatan detail panggilan.
3. Pilih Nonaktifkan logging untuk konfigurasi yang berlaku.

Catatan detail panggilan Amazon Chime

Saat Anda memilih untuk menerima catatan detail panggilan untuk Panggilan Bisnis Amazon Chime, catatan tersebut akan dikirim ke bucket Amazon S3 Anda. Contoh berikut menunjukkan format umum nama rekaman detail panggilan Amazon Chime Business Calling.

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

Contoh berikut menunjukkan data yang diwakili dalam panggilan nama catatan detail.

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

Contoh berikut menunjukkan format umum rekaman detail panggilan Panggilan Bisnis Amazon Chime.

```
{
    "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"
}
```

Konfigurasi ruang konferensi

Amazon Chime dapat berintegrasi dengan perangkat keras video dalam kamar Anda dari Cisco, Tandberg, Polycom, Lifesize, Vidyo, atau lainnya saat Anda menggunakan protokol SIP atau H.323.

Untuk menyambung ke Amazon Chime menggunakan perangkat VTC ruang konferensi yang mendukung SIP, masukkan salah satu opsi berikut:

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- ID rapat 10 digit diikuti oleh**`@meet.chime.in`**

`meet.chime.in`menghubungkan perangkat ruang SIP Anda ke Wilayah Amazon Chime terdekat. Untuk terhubung ke Wilayah tertentu, gunakan entri DNS khusus Wilayah untuk sistem ruang SIP. Untuk informasi selengkapnya, lihat Sistem ruang Protokol Inisiasi Sesi (SIP).

> **Note**
>
> Jika perangkat ruang SIP Anda tidak mendukung TLS dan memerlukan konektivitas TCP, hubungiAWS Support.

Jika Anda menggunakan perangkat yang hanya mendukung H.323, Anda harus menghubungi salah satu dari berikut ini:

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

Jika firewall memfilter lalu lintas antara perangkat VTC dan Amazon Chime, buka rentang untuk protokol yang digunakan. Untuk informasi selengkapnya, lihat Konfigurasi jaringan dan persyaratan bandwidth.

Pada layar selamat datang Amazon Chime, masukkan ID rapat 10 digit atau 13 digit untuk bergabung. Anda dapat menemukan 13 digit ID rapat di klien atau aplikasi web Amazon Chime, atau memilih opsi Dial-in.

Bergabung dengan pertemuan yang dimoderasi

Jika rapat dimoderasi dan Anda adalah tuan rumah atau delegasi, masukkan 13 digit ID rapat Anda untuk bergabung dengan rapat sebagai moderator. Jika Anda seorang moderator, masukkan kode sandi moderator di dialpad diikuti dengan tanda pound (#) untuk bergabung dan memulai rapat. Jika Anda bukan tuan rumah, delegasi, atau moderator, Anda terhubung ke rapat setelah moderator bergabung dan memulai rapat.

Moderator memiliki kontrol host, yang berarti mereka dapat melakukan tindakan rapat tambahan. Tindakan ini termasuk memulai dan menghentikan perekaman, mengunci dan membuka rapat, membisukan semua peserta lainnya, dan mengakhiri rapat. Untuk informasi selengkapnya, lihat Tindakan Moderator menggunakan sistem video telepon atau di dalam kamar di Panduan Pengguna Amazon Chime.

> **Note**
>
> Jika Anda menggunakan Alexa for Business untuk bergabung dengan rapat Amazon Chime, Anda dapat bergabung sebagai moderator hanya jika perangkat Anda terhubung ke sistem video dalam kamar dan Anda melakukan panggilan dengan menggunakan dialpad perangkat.

Perangkat VTC yang kompatibel

Tabel berikut adalah bagian dari daftar perangkat VTC yang kompatibel.

Perangkat	MENYESAP	H.323	Komentar
Cisco	Ya	Ya	Audio/Video/Layar: Ke dan Dari OK
Cisco	Ya	Ya	Audio/Video/Layar: Ke dan Dari OK
Ikon Lifesize	Ya	Tidak	Audio/Video/Layar: Ke dan Dari OK
Debut Polycom	Ya	Ya	Audio/Video/Layar: Ke dan Dari OK

Perangkat	MENYESAP	H.323	Komentar
RealPresence Desktop Polycom	Tidak	Ya	Audio/Video: OK, Layar: Dari perangkat OK
Trio Polycom	Ya	Ya	Audio/Video/Layar: Ke dan Dari OK
Tandberg	Ya	Ya	Audio/Video/Layar: Ke dan Dari OK

Konfigurasi jaringan dan persyaratan bandwidth

Amazon Chime memerlukan tujuan dan port yang dijelaskan dalam topik ini untuk mendukung berbagai layanan. Jika lalu lintas masuk atau keluar diblokir, penyumbatan ini dapat memengaruhi kemampuan untuk menggunakan berbagai layanan, termasuk audio, video, berbagi layar, atau obrolan.

Amazon Chime menggunakan Amazon Elastic Compute Cloud (Amazon EC2) dan layanan AWS lainnya di port TCP/443. Jika firewall Anda memblokir port TCP/443, Anda harus memasukkan `*.amazonaws.com` daftar izin, atau menempatkan rentang alamat IP AWS di layanan berikut Referensi Umum AWS:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Perluas bagian berikut untuk informasi lebih lanjut tentang tujuan, port, dan bandwidth.

Tujuan dan pelabuhan yang diperlukan

Tujuan dan port berikut diperlukan untuk menjalankan Amazon Chime.

Tujuan	Port
lonceng	TCP/443
*.chime.aws	TCP/443
.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

Rapat dan port telepon

Amazon Chime menggunakan tujuan dan port berikut untuk rapat dan Panggilan Bisnis Amazon Chime.

Tujuan	Port
99.77.128.0/18	UDP/3478

Sistem kamar H.323

Amazon Chime menggunakan tujuan dan port berikut untuk sistem video dalam kamar H.323.

Tujuan	Port
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	

Sistem ruang Protokol Inisiasi Sesi (SIP)

Tujuan dan port berikut direkomendasikan saat menjalankan Amazon Chime untuk sistem video dalam kamar SIP di lingkungan Anda.

AWS Wilayah	Tujuan	Port
Global (Wilayah terdekat)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS Wilayah	Tujuan	Port
	52.55.63.0/25	
Global	temu.chime.in 13.248.147.139 76.223.18.152	TCP/5061
AS Timur (Virginia Utara)	meet.ue1.chime.in	TCP/5061
AS Barat (Oregon)	temu.uw2.chime.in	TCP/5061
Asia Pasifik (Singapura)	meet.as1.chime.in	TCP/5061
Asia Pasifik (Sydney)	meet.as2.chime.in	TCP/5061
Asia Pasifik (Tokyo)	meet.an1.chime.in	TCP/5061
Eropa (Irlandia)	bertemu.ew1.chime.in	TCP/5061
Amerika Selatan (Sao Paulo)	meet.se1.chime.in	TCP/5061

Persyaratan bandwidth

Amazon Chime memiliki persyaratan bandwidth berikut untuk audio, video, dan berbagi layar:

- Audio
  - Panggilan 1:1:54 kbps naik dan turun
  - Panggilan besar: tidak lebih dari 32 kbps ekstra turun untuk 50 penelepon
- Video
  - Panggilan 1:1:650 kbps naik dan turun
  - Mode HD: 1400 kbps naik dan turun
  - 3—4 orang: 450 kbps naik dan (N-1) *400 kbps turun
  - 5—16 orang: 184 kbps naik dan (N-1) *134 kbps turun
  - Bandwidth naik turun beradaptasi lebih rendah berdasarkan kondisi jaringan
- Berbagi layar

- 1,2 mbps naik (saat menyajikan) dan ke bawah (saat melihat) untuk kualitas tinggi. Ini beradaptasi serendah 320 kbps berdasarkan kondisi jaringan.
- Remote control: 800 kbps tetap

Melihat laporan

Untuk membuat keputusan yang lebih tepat dan meningkatkan produktivitas organisasi, Anda dapat mengakses data penggunaan dan umpan balik langsung dari konsol. Data laporan diperbarui setiap hari, meskipun mungkin ada penundaan hingga 48 jam.

Untuk melihat laporan penggunaan dan umpan balik

1. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
2. Pilih Laporan, Dasbor.
3. Pada halaman laporan dasbor penggunaan dan umpan balik, lihat data berikut:

> **Note**
>
> Untuk informasi selengkapnya tentang data yang tersedia, lihat Dasbor Laporan Amazon Chime dan detail Aktivitas Pengguna.

- Rentang tanggal (UTC) —Rentang tanggal laporan.
- Pengguna terdaftar —Jumlah pengguna yang telah mendaftar untuk Amazon Chime.
- Pengguna aktif —Jumlah pengguna yang menghadiri rapat atau mengirim pesan dengan Amazon Chime.
- Pertemuan diadakan —Jumlah total pertemuan yang telah berakhir. Anda dapat memilih rapat tertentu untuk melihat detail, termasuk ID konferensi, waktu mulai, jenis, pengelola, durasi, dan jumlah peserta. Pilih ID Konferensi atau nilai penyelenggara Rapat tertentu untuk melihat detail tambahan, termasuk peserta, acara daftar rapat, jenis klien, dan umpan balik pertemuan.
- Memenuhi kepuasan —Persentase tanggapan positif yang diberikan pada end-of-meeting survei.
- Pesan obrolan yang dikirim —Jumlah pesan obrolan yang dikirim pengguna.

Memperluas klien desktop Amazon Chime

Anda dapat memperluas kemampuan klien desktop Amazon Chime dengan menambahkan bot obrolan, sesi telepon proxy, dan webhook. Bot obrolan memungkinkan pengguna untuk melakukan tugas-tugas seperti menanyakan sistem internal untuk informasi. Sesi telepon proxy memungkinkan pengguna untuk menelepon dan mengirim teks tanpa mengungkapkan nomor telepon mereka. Webhook dapat secara otomatis mengirim pesan ke ruang obrolan. Misalnya, webhook dapat mengirim pengingat rapat ke tim, bersama dengan tautan ke rapat.

Topik

Manajemen pengguna

Cuplikan kode berikut dapat membantu Anda mengelola pengguna Amazon Chime. Semua contoh dalam topik ini menggunakan Java.

Topik

Mengundang beberapa pengguna

Contoh berikut menunjukkan cara mengundang beberapa pengguna ke akun Amazon Chime`Team`.

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

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

Mengunduh daftar pengguna

Contoh berikut menunjukkan cara mengunduh daftar pengguna yang terkait dengan akun administratif Amazon Chime Anda dalam `.csv` format.

```
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();
```

Keluar dari beberapa pengguna

Contoh berikut menunjukkan cara keluar dari beberapa pengguna dari akun administratif Amazon Chime Anda.

```
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);
}
```

Perbarui PIN pribadi pengguna

Contoh berikut menunjukkan cara mengatur ulang PIN rapat pribadi untuk pengguna Amazon Chime yang ditentukan.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

Mengintegrasikan chatbots ke klien desktop Amazon Chime

Anda dapat menggunakanAWS Command Line Interface(AWS CLI), Amazon Chime API, atauAWSSDK untuk mengintegrasikan chatbots dengan Amazon Chime. Chatbots memungkinkan Anda menggunakan kekuatan Amazon Lex,AWS Lambda, dan lainnyaAWSlayanan untuk merampingkan tugas umum dengan antarmuka percakapan cerdas yang dapat diakses oleh pengguna di ruang obrolan Amazon Chime.

Jika Anda administrator akun Amazon Chime Enterprise, Anda dapat menggunakan chatbots untuk memungkinkan pengguna melakukan tugas-tugas seperti:

- Meminta sistem internal mereka untuk informasi.
- Mengotomatisasi tugas.
- Menerima pemberitahuan untuk masalah kritis.
- Membuat tiket dukungan.

Untuk informasi selengkapnya tentang akun Amazon Chime, lihatMengelola akun Amazon Chime Anda.

Jika Anda mengelola akun Amazon Chime Enterprise, Anda dapat membuat hingga 10 chatbots untuk integrasi dengan Amazon Chime. Chatbots hanya dapat digunakan di ruang obrolan yang dibuat oleh anggota akun Anda. Hanya administrator ruang obrolan yang dapat menambahkan chatbots ke ruang obrolan. Setelah chatbot ditambahkan ke ruang obrolan, anggota ruang obrolan dapat berinteraksi dengan bot menggunakan perintah yang disediakan oleh pembuat bot. Untuk informasi selengkapnya, lihat bagian berikutnya dalam topik ini.

Pengguna Linux dan macOS dapat membuat contoh chatbot khusus. Untuk informasi selengkapnya, lihatBuat chatbots khusus untuk Amazon Chime.

Daftar isi

Menggunakan chatbots dengan Amazon Chime

Jika Anda mengelola akun Amazon Chime Enterprise, Anda dapat membuat hingga 10 chatbots untuk integrasi dengan Amazon Chime. Chatbots hanya dapat digunakan di ruang obrolan yang dibuat oleh anggota akun Anda. Hanya administrator ruang obrolan yang dapat menambahkan chatbots ke ruang obrolan. Setelah chatbot ditambahkan ke ruang obrolan, anggota ruang obrolan dapat berinteraksi dengan bot menggunakan perintah yang disediakan oleh pembuat bot. Untuk informasi selengkapnya, lihatMenggunakan chatbotsdiPanduan Pengguna Amazon Chime.

Anda juga dapat menggunakan operasi Amazon Chime API untuk mengaktifkan atau menghentikan chatbots untuk akun Amazon Chime Anda. Untuk informasi selengkapnya, lihat Perbarui chatbots.

> **Note**
>
> Anda tidak dapat menghapus chatbots. Untuk menghentikan chatbot agar tidak digunakan di akun Anda, gunakan Amazon ChimeUpdateBotOperasi API diReferensi Amazon Chime. Saat Anda menghentikan chatbot, administrator ruang obrolan dapat menghapusnya dari ruang obrolan, tetapi mereka tidak dapat menambahkannya ke ruang obrolan. Pengguna yang @mention chatbot yang dihentikan di ruang obrolan menerima pesan kesalahan.

Prasyarat

Sebelum Anda memulai prosedur untuk mengonfigurasi chatbot dengan Amazon Chime, selesaikan prasyarat berikut:

- Buat chatbot.
- Buat titik akhir keluar untuk Amazon Chime untuk mengirim acara ke bot Anda. Pilih dariAWS LambdaFungsi ARN atau titik akhir HTTPS. Untuk informasi tentang Lambda, lihat Panduan Developer AWS Lambda.

Praktek terbaik DNS untuk titik akhir HTTPS

Kami merekomendasikan praktik terbaik berikut saat Anda mengonfigurasi DNS untuk titik akhir HTTPS Anda:

- Gunakan subdomain DNS yang didedikasikan untuk titik akhir bot.
- Gunakan hanya A-record untuk menunjuk ke titik akhir bot.
- Lindungi server DNS dan akun registrar DNS Anda untuk mencegah pembajakan domain.
- Gunakan sertifikat perantara TLS yang valid secara publik yang didedikasikan untuk titik akhir bot.
- Verifikasi tanda tangan pesan bot secara kriptografis sebelum bertindak berdasarkan pesan bot.

Setelah membuat chatbot Anda, gunakanAWS Command Line Interface(AWS CLI) atau operasi Amazon Chime API untuk menyelesaikan tugas yang dijelaskan di bagian berikut.

Tugas

- Langkah 1: Integrasikan chatbot dengan Amazon Chime
- Langkah 2: Konfigurasi titik keluar untuk chatbot Amazon Chime
- Langkah 3: Tambahkan chatbot ke ruang obrolan Amazon Chime
- Otentikasi permintaan chatbot
- Perbarui chatbots

Langkah 1: Integrasikan chatbot dengan Amazon Chime

Setelah Anda menyelesaikanprasyarat, integrasikan chatbot Anda dengan Amazon Chime menggunakanAWS CLIatau Amazon Chime API.

> **Note**
>
> Prosedur ini membuat nama dan alamat email untuk chatbot Anda. Nama Chatbot dan alamat email tidak dapat diubah setelah pembuatan.

AWS CLI

Untuk mengintegrasikan chatbot menggunakanAWS CLI

1. Untuk mengintegrasikan chatbot Anda dengan Amazon Chime, gunakancreate-botperintah diAWS CLI.

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

   a. Masukkan nama tampilan chatbot hingga 55 karakter alfanumerik atau khusus (seperti +, -, %).

   b. Masukkan nama domain terdaftar untuk akun Amazon Chime Enterprise Anda.

2. Amazon Chime mengembalikan respons yang menyertakan ID bot.

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

3. Salin dan simpan ID bot dan alamat email bot untuk digunakan dalam prosedur berikut.

Amazon Chime API

Untuk mengintegrasikan chatbot menggunakan Amazon Chime API

1. Untuk mengintegrasikan chatbot Anda dengan Amazon Chime, gunakanCreateBotOperasi API diReferensi Amazon Chime.

   a. Masukkan nama tampilan chatbot hingga 55 karakter alfanumerik atau khusus (seperti +, -, %).

   b. Masukkan nama domain terdaftar untuk akun Amazon Chime Enterprise Anda.

2. Amazon Chime mengembalikan respons yang menyertakan ID bot. Salin dan simpan ID bot dan alamat email. Alamat email bot terlihat seperti ini:*exampleBot*-chimebot@*example.com*.

AWS SDK for Java

Contoh kode berikut menunjukkan bagaimana mengintegrasikan chatbot menggunakanAWSSDK for Java

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

chime.createBot(createBotRequest);
```

Amazon Chime mengembalikan respons yang menyertakan ID bot. Salin dan simpan ID bot dan alamat email. Alamat email bot terlihat seperti ini:*exampleBot*-chimebot@*example.com*.

Langkah 2: Konfigurasi titik keluar untuk chatbot Amazon Chime

Setelah Anda membuat ID chatbot untuk akun Amazon Chime Enterprise Anda, konfigurasikan titik akhir keluar Anda untuk Amazon Chime untuk digunakan untuk mengirim pesan ke bot Anda. Titik akhir keluar bisa menjadiAWS Lambdafungsi ARN atau titik akhir HTTPS yang Anda buat sebagai bagian dariprasyarat. Untuk informasi tentang Lambda, lihat Panduan Developer AWS Lambda.

> **Note**
>
> Jika titik akhir HTTPS keluar untuk bot Anda tidak dikonfigurasi atau kosong, administrator ruang obrolan tidak dapat menambahkan bot ke ruang obrolan. Selain itu, pengguna ruang obrolan tidak dapat berinteraksi dengan bot.

AWS CLI

Untuk mengonfigurasi titik akhir keluar untuk chatbot Anda, gunakanput-events-configurationperintah diAWS CLI. Konfigurasikan ARN fungsi Lambda atau titik akhir HTTPS keluar.

Lambda ARN

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

HTTPS endpoint

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

Amazon Chime merespons dengan ID bot dan titik akhir HTTPS.

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

Amazon Chime API

Untuk mengonfigurasi titik akhir keluar untuk chatbot Anda, gunakan Amazon ChimePutEventsConfigurationOperasi API diReferensi Amazon Chime. Konfigurasikan ARN fungsi Lambda atau titik akhir HTTPS keluar.

- Jika Anda mengonfigurasi ARN fungsi Lambda— Amazon Chime memanggil Lambda untuk menambahkan izin untuk mengizinkan administrator Amazon ChimeAWSakun untuk memanggil ARN fungsi Lambda yang disediakan. Ini diikuti oleh pemanggilan kering untuk memverifikasi bahwa Amazon Chime memiliki izin untuk memanggil fungsi. Jika menambahkan izin gagal, atau jika pemanggilan dry run gagal, maka`PutEventsConfiguration`permintaan mengembalikan kesalahan HTTP 4xx.
- Jika Anda mengonfigurasi titik akhir HTTPS keluar— Amazon Chime memverifikasi titik akhir Anda dengan mengirimkan permintaan HTTP Post dengan payload Challenge JSON ke titik akhir HTTPS keluar yang Anda berikan pada langkah sebelumnya. Titik akhir HTTPS keluar Anda harus merespons dengan menggemakan kembali parameter Challenge dalam format JSON. Contoh berikut menunjukkan permintaan dan respons yang valid.

  Request

```
HTTPS POST

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

  Response

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

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

  Jika jabat tangan tantangan gagal, maka`PutEventsConfiguration`permintaan mengembalikan kesalahan HTTP 4xx.

AWS SDK for Java

Kode contoh berikut menunjukkan cara mengkonfigurasi titik akhir menggunakanAWSSDK for Java

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

 chime.putEventsConfiguration(putEventsConfigurationRequest):
```

Langkah 3: Tambahkan chatbot ke ruang obrolan Amazon Chime

Hanya administrator ruang obrolan yang dapat menambahkan chatbot ke ruang obrolan. Mereka menggunakan alamat email chatbot yang dibuat diLangkah 1.

Untuk menambahkan chatbot ke ruang obrolan

1. Buka klien desktop Amazon Chime atau aplikasi web.
2. Pilih ikon roda gigi di sudut kanan atas, dan pilihKelola webhook dan bot.
3. PilihTambahkan bot.
4. UntukAlamat email, masukkan alamat email bot.
5. Pilih Tambahkan.

Nama bot muncul di daftar ruang obrolan. Jika ada tindakan tambahan yang diperlukan untuk menambahkan chatbot ke ruang obrolan, berikan tindakan kepada administrator ruang obrolan.

Setelah chatbot ditambahkan ke ruang obrolan, berikan perintah chatbot kepada pengguna ruang obrolan Anda. Salah satu cara untuk melakukannya adalah dengan memprogram chatbot Anda untuk mengirim bantuan perintah ke ruang obrolan ketika menerima undangan ruang obrolan. AWS juga merekomendasikan untuk membuat perintah bantuan untuk digunakan pengguna chatbot Anda.

Otentikasi permintaan chatbot

Anda dapat mengautentikasi permintaan yang dikirim ke chatbot Anda dari ruang obrolan Amazon Chime. Untuk melakukan ini, hitung tanda tangan berdasarkan permintaan. Kemudian, validasi

bahwa tanda tangan yang dihitung cocok dengan yang ada di header permintaan. Amazon Chime menggunakan hash HMAC SHA256 untuk menghasilkan tanda tangan.

Jika chatbot Anda dikonfigurasi untuk Amazon Chime menggunakan titik akhir HTTPS keluar, gunakan langkah autentikasi berikut.

Untuk memvalidasi permintaan yang ditandatangani dari Amazon Chime untuk chatbot dengan titik akhir HTTPS keluar yang dikonfigurasi

1. DapatkanTanda Tangan Loncengheader dari permintaan HTTP.
2. DapatkanLonceng Permintaan-TimestampHeader danbadandari permintaan. Kemudian, gunakan bilah vertikal sebagai pembatas antara dua elemen untuk membentuk string.
3. GunakanSecurityTokendari CreateBot respon sebagai kunci awalHMAC_SHA_256, dan hash string yang Anda buat di langkah 2.
4. Mengkodekan byte hash dengan encoder Base64 ke string tanda tangan.
5. Bandingkan tanda tangan yang dihitung ini dengan yang ada diTanda Tangan Loncengsundulan

Contoh kode berikut menunjukkan cara menghasilkan tanda tangan menggunakan Java.

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

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

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

Titik akhir HTTPS keluar harus menanggapi permintaan Amazon Chime dengan`200 OK`dalam waktu 2 detik. Jika tidak, permintaan gagal. Jika titik akhir HTTPS keluar tidak tersedia setelah 2 detik, mungkin karena batas waktu Koneksi atau Baca, atau jika Amazon Chime menerima kode respons 5xx, Amazon Chime akan mencoba ulang permintaan tersebut dua kali. Coba lagi pertama dikirim 200 milidetik setelah permintaan awal gagal. Percobaan kedua dikirim 400 milidetik setelah percobaan ulang sebelumnya gagal. Jika titik akhir HTTPS keluar masih tidak tersedia setelah percobaan ulang kedua, permintaan gagal.

> **Note**
>
> TheLonceng Permintaan-Timestampberubah setiap kali permintaan dicoba ulang.

Jika chatbot Anda dikonfigurasi untuk Amazon Chime menggunakan ARN fungsi Lambda, gunakan langkah autentikasi berikut.

Untuk memvalidasi permintaan yang ditandatangani dari Amazon Chime untuk chatbot dengan fungsi Lambda ARN yang dikonfigurasi

1. DapatkanTanda Tangan LoncengdanLonceng Permintaan-Timestampdari permintaan LambdaClientContext, dalam format JSON yang dikodekan Base64.

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

2. Dapatkanbadanpermintaan dari payload permintaan.
3. GunakanSecurityTokendari`CreateBot`respon sebagai kunci awalHMAC_SHA_256, dan hash string yang Anda buat.
4. Mengkodekan byte hash dengan encoder Base64 ke string tanda tangan.
5. Bandingkan tanda tangan yang dihitung ini dengan yang ada diTanda Tangan Loncengsundulan

Jika`com.amazonaws.SdkClientException`terjadi selama pemanggilan Lambda, Amazon Chime mencoba ulang permintaan dua kali.

Perbarui chatbots

Sebagai administrator akun Amazon Chime, Anda dapat menggunakan Amazon Chime API denganAWSSDK atauAWS CLIuntuk melihat detail chatbot Anda. Anda juga dapat mengaktifkan atau menghentikan chatbots Anda agar tidak digunakan di akun Anda. Anda juga dapat membuat ulang token keamanan untuk chatbot Anda.

Untuk informasi selengkapnya, lihat topik berikut diReferensi Amazon Chime:

- GetBot— Mendapatkan detail chatbot Anda, seperti alamat email bot dan jenis bot.
- UpdateBot— Mengaktifkan atau menghentikan chatbot agar tidak digunakan di akun Anda.
- RegenerateSecurityToken— Meregenerasi token keamanan untuk chatbot Anda.

Anda juga dapat mengonfigurasi`PutEventsConfiguration`untuk chatbot Anda. Misalnya, jika chatbot Anda awalnya dikonfigurasi untuk menggunakan titik akhir HTTPS keluar, Anda dapat menghapus konfigurasi peristiwa sebelumnya dan menempatkan konfigurasi peristiwa baru untuk ARN fungsi Lambda.

Untuk informasi selengkapnya, lihat topik berikut diReferensi Amazon Chime:

- DeleteEventsConfiguration
- PutEventsConfiguration

Acara Amazon Chime dikirim ke chatbots

Peristiwa berikut dikirim ke chatbot Anda dari Amazon Chime:

- Mengundang— Dikirim saat chatbot Anda ditambahkan ke ruang obrolan Amazon Chime
- Sebutkan— Dikirim ketika pengguna di ruang obrolan @mentions chatbot Anda
- Hapus— Dikirim ketika chatbot Anda dihapus dari ruang obrolan Amazon Chime

Contoh berikut menunjukkan payload JSON yang dikirim ke chatbot Anda untuk setiap peristiwa ini.

Example : Mengundang acara

```
            {
              "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 : Sebutkan acara

```
            {
                "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**
>
> The`InboundHttpsEndpoint`URL untuk acara Mention akan kedaluwarsa 2 menit setelah dikirim.

Example : Hapus acara

```
{
    "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"
}
```

Membuat webhook untuk Amazon Chime

Webhook memungkinkan aplikasi web untuk berkomunikasi satu sama lain secara real time. Biasanya, webhook mengirim notifikasi saat tindakan terjadi. Misalnya, katakanlah Anda menjalankan situs belanja online. Webhook dapat memberi tahu Anda ketika pelanggan menambahkan item ke keranjang belanja, membayar pesanan, atau mengirim komentar. Webhook tidak membutuhkan pemrograman sebanyak aplikasi tradisional, dan mereka tidak menggunakan banyak kekuatan pemrosesan. Tanpa webhook, sebuah program harus sering melakukan polling untuk data agar bisa mendapatkannya secara real time. Dengan webhook, aplikasi pengirim memposting data segera.

Webhook masuk yang Anda buat dapat mengirim pesan secara terprogram ke ruang obrolan Amazon Chime. Misalnya, webhook dapat memberi tahu tim layanan pelanggan tentang pembuatan tiket prioritas tinggi baru, dan menambahkan tautan ke tiket di ruang obrolan.

Pesan webhook dapat diformat dengan penurunan harga dan dapat menyertakan emoji. Tautan HTTP dan alamat email dirender sebagai tautan aktif. Pesan juga dapat menyertakan anotasi @All

dan @Present untuk memberi tahu semua anggota dan anggota ruang obrolan yang ada. Untuk langsung @mention peserta chat room, gunakan alias atau alamat email lengkap mereka. Misalnya, `@aliasatau @alias@domain.com`.

Webhook hanya dapat menjadi bagian dari ruang obrolan dan tidak dapat dibagikan. Administrator ruang obrolan Amazon Chime dapat menambahkan hingga 10 webhook untuk setiap ruang obrolan.

Setelah membuat webhook, Anda dapat mengintegrasikannya dengan ruang obrolan Amazon Chime, seperti yang ditunjukkan dalam prosedur berikut.

Untuk mengintegrasikan webhook dengan ruang obrolan

1. Dapatkan URL webhook dari administrator ruang obrolan. Untuk informasi lebih lanjut, lihatMenambahkan webhook ke ruang obrolandi dalamPanduan Pengguna Amazon Chime.
2. Gunakan URL webhook di skrip atau aplikasi yang Anda buat untuk mengirim pesan ke ruang obrolan:

   a. URL menerima permintaan HTTP POST.

   b. Webhook Amazon Chime menerima payload JSON dengan satu kunciKonten. Berikut ini adalah contoh perintah curl dengan payload sampel:

   ```
   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"}'
   ```

   Berikut ini adalah contohPowerShellperintah untuk pengguna Windows:

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

Setelah program eksternal mengirimkan HTTP POST ke URL webhook, server memvalidasi bahwa webhook valid dan memiliki ruang obrolan yang ditetapkan. Webhook muncul di daftar ruang obrolan dengan ikon webhook di samping namanya. Pesan ruang obrolan yang dikirim oleh webhook muncul di ruang obrolan dengan nama webhook diikuti oleh(Webhook).

> **Note**
>
> CORS saat ini tidak diaktifkan untuk webhooks.

Memecahkan masalah kesalahan webhook

Berikut ini adalah daftar kesalahan terkait webhook:

- Batas tingkat webhook yang masuk untuk setiap webhook adalah 1 TPS per chat room. Throttling menghasilkan kesalahan HTTP 429.
- Pesan yang diposting oleh webhook harus berukuran 4 KB atau kurang. Payload pesan yang lebih besar menghasilkan galat HTTP 413.
- Pesan yang diposting oleh webhook dengan anotasi @All dan @Present hanya berfungsi untuk ruang obrolan dengan 50 anggota atau lebih sedikit. Lebih dari 50 anggota menghasilkan kesalahan HTTP 400.
- Jika URL webhook diregenerasi, menggunakan URL lama menghasilkan kesalahan HTTP 404.
- Jika webhook di ruangan dihapus, menggunakan URL lama menghasilkan kesalahan HTTP 404.
- URL webhook tidak valid menghasilkan kesalahan HTTP 403.
- Jika layanan tidak tersedia, pengguna menerima kesalahan HTTP 503 dalam respons.

Dukungan administratif untuk Amazon Chime

> **Note**
>
> Untuk bantuan dengan akun belanja Amazon Anda, buka Layanan Pelanggan di amazon.com.

Jika Anda perlu menghubungi dukungan untuk Amazon Chime, pilih salah satu opsi berikut:

- Jika Anda memiliki akun AWS Support, buka Support Center dan kirimkan tiket.
- Jika tidak, buka AWS Management Consoledan pilih Amazon Chime, Support, Submit request.

Berikan sebanyak mungkin informasi berikut:

- Penjelasan rinci tentang masalah ini.
- Waktu terjadinya masalah, termasuk zona waktu Anda.
- Versi Amazon Chime Anda. Untuk menemukan nomor versi Anda:
  - Di Windows, pilih Bantuan, Tentang Amazon Chime.
  - Di macOS, pilih Amazon Chime, Tentang Amazon Chime.
  - Di iOS dan Android, pilih Pengaturan, Tentang.
- ID referensi log. Untuk menemukan ID ini:
  - Di Windows dan macOS, pilih Bantuan, Kirim Log Diagnostik.
  - Di iOS dan Android, pilih Pengaturan, Kirim Log Diagnostik.
- Jika masalah Anda terkait dengan rapat, ID rapat.

Keamanan di Amazon Chime

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Chime, lihat AWS Services in Scope by Compliance Program AWS Program.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon Chime. Topik berikut menunjukkan cara mengonfigurasi Amazon Chime untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya Amazon Chime Anda.

Topik

- Menggunakan peran tertaut layanan untuk Amazon Chime
- Pencatatan dan pemantauan di Amazon Chime
- Validasi kepatuhan untuk Amazon Chime
- Ketahanan di Amazon Chime
- Keamanan infrastruktur di Amazon Chime
- Memahami pembaruan otomatis Amazon Chime

Manajemen identitas dan akses untuk Amazon Chime

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon Chime. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon Chime.

Pengguna layanan — Jika Anda menggunakan layanan Amazon Chime untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon Chime untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon Chime, lihat. Memecahkan masalah identitas dan akses Amazon Chime

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon Chime di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon Chime. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Chime mana yang harus diakses pengguna layanan

Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon Chime, lihat. Bagaimana Amazon Chime bekerja dengan IAM

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon Chime. Untuk melihat contoh kebijakan berbasis identitas Amazon Chime yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas Amazon Chime

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

AWS pengguna root akun

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran

dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat

kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

AWS kebijakan terkelola untuk Amazon Chime

Menambahkan izin ke para pengguna, grup, dan peran lebih mudah dilakukan dengan menggunakan kebijakan terkelola AWS dibandingkan dengan menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan terkelola pelanggan IAM yang hanya menyediakan izin sesuai kebutuhan tim Anda. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan-kebijakan ini mencakup kasus penggunaan umum dan tersedia di akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan AWS terkelola ReadOnlyAccess menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Daftar Kontrol Akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon Chime bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon Chime, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan dengan Amazon Chime. Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon Chime dan layanan AWS lainnya dengan IAM, AWS lihat layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Topik

Kebijakan berbasis identitas Amazon Chime

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Amazon Chime mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Kunci syarat

Amazon Chime tidak menyediakan kunci kondisi khusus layanan apa pun. Untuk melihat semua kunci syarat global AWS , lihat Kunci Konteks Syarat Global AWS dalam Panduan Pengguna IAM.

Sumber daya

Amazon Chime tidak mendukung menentukan ARN sumber daya dalam kebijakan.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Amazon Chime, lihat. Contoh kebijakan berbasis identitas Amazon Chime

Pencegahan confused deputy lintas layanan

Masalah Deputi yang membingungkan adalah masalah keamanan informasi yang terjadi ketika entitas tanpa izin untuk melakukan tindakan memanggil entitas yang lebih istimewa untuk melakukan tindakan. Ini dapat memungkinkan aktor jahat untuk menjalankan perintah atau memodifikasi sumber daya yang jika tidak, mereka tidak akan memiliki izin untuk menjalankan atau mengakses. Untuk informasi selengkapnya, lihat Masalah deputi yang membingungkan di Panduan AWS Identity and Access Management Pengguna.

Pada tahun AWS, peniruan lintas layanan dapat menyebabkan skenario wakil yang membingungkan. Peniruan identitas lintas layanan terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Aktor jahat dapat menggunakan layanan panggilan untuk mengubah sumber daya di layanan lain dengan menggunakan izin yang biasanya tidak mereka miliki.

AWS menyediakan prinsip layanan dengan akses terkelola ke sumber daya di akun Anda untuk membantu Anda melindungi keamanan sumber daya Anda. Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount` global dalam kebijakan sumber daya Anda. Kunci ini membatasi izin yang diberikan Amazon Chime layanan lain ke sumber daya tersebut.

Contoh berikut menunjukkan kebijakan bucket S3 yang menggunakan kunci konteks kondisi `aws:SourceAccount` global dalam bucket `CallDetailRecords` S3 yang dikonfigurasi untuk membantu mencegah masalah deputi yang membingungkan.

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

Kebijakan berbasis sumber daya Amazon Chime

Amazon Chime tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag Amazon Chime

Amazon Chime tidak mendukung sumber daya penandaan atau mengontrol akses berdasarkan tag.

Peran Amazon Chime IAM

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensil sementara dengan Amazon Chime

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau GetFederation Token.

Amazon Chime mendukung penggunaan kredensil sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain yang menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda, dan layanan memiliki peran tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Amazon Chime mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola peran terkait layanan Amazon Chime, lihat. Menggunakan peran tertaut layanan untuk Amazon Chime

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Amazon Chime tidak mendukung peran layanan.

Contoh kebijakan berbasis identitas Amazon Chime

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Chime. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan di tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Amazon Chime
- Izinkan pengguna akses penuh ke Amazon Chime
- Mengizinkan pengguna melihat izin mereka sendiri
- Memungkinkan pengguna untuk mengakses tindakan manajemen pengguna
- AWS kebijakan terkelola: AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- Amazon Chime memperbarui kebijakan terkelola AWS

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon Chime di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan.

Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Amazon Chime

Untuk mengakses konsol Amazon Chime, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon Chime di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan konsol Amazon Chime, lampirkan juga AmazonChimeReadOnlykebijakan AWS terkelola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

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

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan pengguna akses penuh ke Amazon Chime

AmazonChimeFullAccessKebijakan AWS terkelola berikut memberi pengguna IAM akses penuh ke sumber daya Amazon Chime. Kebijakan ini memberi pengguna akses ke semua operasi Amazon Chime, serta operasi lain yang perlu dilakukan Amazon Chime atas nama Anda.

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

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memungkinkan pengguna untuk mengakses tindakan manajemen pengguna

Gunakan AmazonChimeUserManagementkebijakan AWS terkelola untuk memberi pengguna akses ke tindakan pengelolaan pengguna di konsol Amazon Chime.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
                "chime:GetUser",
                "chime:GetUserByEmail",
                "chime:InviteUsers",
                "chime:InviteUsersFromProvider",
                "chime:SuspendUsers",
                "chime:ActivateUsers",
```

```
                "chime:UpdateUserLicenses",
                "chime:ResetPersonalPIN",
                "chime:LogoutUser",
                "chime:ListDomains",
                "chime:GetDomain",
                "chime:ListDirectories",
                "chime:ListGroups",
                "chime:SubmitSupportRequest",
                "chime:ListDelegates",
                "chime:ListAccountUsageReportData",
                "chime:GetMeetingDetail",
                "chime:ListMeetingEvents",
                "chime:ListMeetingsReportData",
                "chime:GetUserActivityReportData",
                "chime:UpdateUser",
                "chime:BatchUpdateUser",
                "chime:BatchSuspendUser",
                "chime:BatchUnsuspendUser",
                "chime:AssociatePhoneNumberWithUser",
                "chime:DisassociatePhoneNumberFromUser",
                "chime:GetPhoneNumber",
                "chime:ListPhoneNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime:AssociateSigninDelegateGroupsWithAccount",
                "chime:DisassociateSigninDelegateGroupsFromAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`Ini memungkinkan Konektor Suara Amazon Chime untuk mengalirkan media ke Amazon Kinesis Video Streams, memberikan pemberitahuan streaming, dan mensintesis ucapan menggunakan Amazon Polly. Kebijakan ini memberikan izin layanan Amazon Chime Voice Connector untuk mengakses Amazon Kinesis Video Streams pelanggan, mengirim peristiwa notifikasi ke Layanan Pemberitahuan Sederhana

Amazon dan Layanan Antrian Sederhana Amazon, dan menggunakan Amazon Polly untuk mensintesis ucapan saat menggunakan Aplikasi dan tindakan Suara Amazon Chime SDK. `Speak` `SpeakAndGetDigits` Untuk informasi selengkapnya, lihat contoh kebijakan berbasis identitas Amazon Chime SDK di Panduan Administrator Amazon Chime SDK.

Amazon Chime memperbarui kebijakan terkelola AWS

Tabel berikut mencantumkan dan menjelaskan pembaruan yang dilakukan pada kebijakan Amazon Chime IAM.

Perubahan	Deskripsi	Tanggal
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` — Permbaruan ke kebijakan yang sudah ada	Konektor Suara Amazon Chime menambahkan izin baru untuk memungkinkan Anda menggunakan Amazon Polly untuk mensintesis pidato. Izin ini diperlukan untuk menggunakan dan tindakan di Aplikasi Suara Amazon Chime SDK. `Speak` `SpeakAndGetDigits`	15 Maret 2022
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Pembaruan ke kebijakan yang ada	Amazon Chime Voice Connector menambahkan izin baru untuk memungkinkan akses ke Amazon Kinesis Video Streams dan mengirim acara notifikasi ke SNS dan SQS. Izin ini diperlukan untuk Konektor Suara Amazon Chime untuk mengalirkan media ke Amazon Kinesis Video Streams dan memberikan pemberitahuan streaming.	Desember 20, 2021

Perubahan	Deskripsi	Tanggal
Ubah kebijakan yang ada. Membuat pengguna atau peran IAM dengan kebijakan Chime SDK.	Amazon Chime menambahkan tindakan baru yang ditambahkan untuk mendukung validasi yang diperluas. Sejumlah tindakan ditambahkan untuk memungkinkan daftar dan penandaan peserta dan sumber daya rapat, dan untuk memulai dan menghentikan transkripsi rapat.	September 23, 2021
Amazon Chime mulai melacak perubahan	Amazon Chime mulai melacak perubahan untuk kebijakan yang AWS dikelola.	September 23, 2021

Memecahkan masalah identitas dan akses Amazon Chime

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon Chime dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Amazon Chime
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Amazon Chime saya

Saya tidak berwenang untuk melakukan tindakan di Amazon Chime

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `chime:`*`GetWidget`* rekaan.

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `chime:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon Chime.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Amazon Chime. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Amazon Chime saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Amazon Chime mendukung fitur-fitur ini, lihat. Bagaimana Amazon Chime bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Menggunakan peran tertaut layanan untuk Amazon Chime

Amazon Chime menggunakan peran terkait layananAWS Identity and Access Management (IAM). Peran tertaut layanan adalah jenis IAM role unik yang tertaut langsung ke Amazon Chime. Peran tertaut layanan ditentukan sebelumnya oleh Amazon Chime dan mencakup semua izin yang diperlukan layanan untuk memanggilAWS layanan lainnya atas nama Anda.

Peran tertaut layanan membuat pengaturan Amazon Chime lebih efisien karena Anda tidak diharuskan untuk menambahkan izin yang diperlukan secara manual karena Anda tidak perlu menambahkan izin yang diperlukan secara manual karena Anda tidak perlu menambahkan izin yang diperlukan secara manual karena Anda tidak perlu menambahkan izin yang diperlukan secara manual Amazon Chime menentukan izin peran tertaut layanan, dan kecuali ditentukan lain, hanya

Amazon Chime yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Tindakan ini akan melindungi sumber daya Amazon Chime karena Anda tidak dapat secara tidak sengaja menghapus izin untuk menghapus izin untuk menghapus izin untuk mengakses izin untuk mengakses izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bekerja dengan IAM. Cari layanan yang memiliki Yes di kolom Service-Linked Role. Pilih Yes (Ya) bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Topik

- Menggunakan peran dengan perangkat Alexa for Business yang dibagikan
- Menggunakan peran dengan transkripsi langsung
- Menggunakan peran dengan pipeline media Amazon Chime SDK

Menggunakan peran dengan perangkat Alexa for Business yang dibagikan

Informasi di bagian berikut menjelaskan cara menggunakan peran terkait layanan dan memberikan akses Amazon Chime ke sumber daya Alexa for Business diAWS akun Anda.

Topik

- Izin peran tertaut layanan untuk Amazon Chime
- Membuat Peran Terkait Layanan untuk Amazon Chime
- Mengedit Peran Terkait Layanan untuk Amazon Chime
- Menghapus Peran Terkait Layanan untuk Amazon Chime
- Wilayah yang Didukung untuk Peran Terkait Layanan Amazon Chime

Izin peran tertaut layanan untuk Amazon Chime

Amazon Chime menggunakan peran tertaut layanan yang bernama AWSServiceRoleForAmazonChime— Memungkinkan untuk mengakses keAWS layanan dan sumber daya yang digunakan atau dikelola oleh Amazon Chime, seperti perangkat bersama Alexa for Business.

Peran AWSServiceRoleForAmazonChime tertaut layanan memercayakan layanan berikut untuk mengambil peran:

- `chime.amazonaws.com`

Kebijakan izin peran memungkinkan Amazon Chime untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

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

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat Peran Terkait Layanan untuk Amazon Chime

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda mengaktifkan Alexa for Business perangkat bersama di Amazon Chime diAWS Management ConsoleAWS APIAWS CLI, atau, Amazon Chime membuat peran tertaut layanan untuk Anda.

Anda juga dapat menggunakan konsol IAM untuk membuat peran tertaut layanan dengan kasus penggunaan Amazon Chime. Di AWS CLI atau API AWS, buat peran yang terhubung dengan layanan dengan nama layanan `chime.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat peran terkait layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit Peran Terkait Layanan untuk Amazon Chime

Amazon Chime tidak mengizinkan Anda untuk mengedit peran AWSServiceRoleForAmazonChime tertaut layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus Peran Terkait Layanan untuk Amazon Chime

Jika Anda tidak lagi memerlukan fitur atau layanan yang memerlukan peran tertaut layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang

tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran tertaut-layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut.

> **Note**
>
> Jika Amazon Chime menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Amazon Chime yang digunakan oleh AWSServiceRoleForAmazonChime (konsol)

- Matikan Alexa for Business untuk semua perangkat bersama di akun Amazon Chime Anda.
  a. Buka konsol Amazon Chime di https://chime.aws.amazon.com/.
  b. Pilih Pengguna, Perangkat bersama.
  c. Pilih perangkat.
  d. Pilih Tindakan.
  e. Pilih Nonaktifkan Alexa for Business.

Menghapus peran tertaut layanan secara manual

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForAmazonChime Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Terkait Layanan Amazon Chime

Amazon Chime mendukung penggunaan peran tertaut layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Endpoint dan kuota Amazon Chime.

Menggunakan peran dengan transkripsi langsung

Informasi di bagian berikut menjelaskan cara membuat dan mengelola peran terkait layanan untuk transkripsi langsung Amazon Chime. Untuk informasi selengkapnya tentang layanan transkripsi langsung, lihat Menggunakan transkripsi langsung Amazon Chime SDK.

Topik

Izin Peran Tertaut layanan untuk Amazon Chime

Amazon Chime Live Transcription menggunakan peran terkait layanan bernama AWSServiceRoleForAmazonChimeTranscription— Memungkinkan Amazon Chime mengakses Amazon Transcribe dan Amazon Transcribe Medical atas nama Anda.

Peran AWSServiceRoleForAmazonChimeTranscription Tertaut layanan memercayakan layanan berikut

- `transcription.chime.amazonaws.com`

Kebijakan Amazon Chime Peran an

- Tindakan: `transcribe:StartStreamTranscription` pada `all AWS resources`
- Tindakan: `transcribe:StartMedicalStreamTranscription` pada `all AWS resources`

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat Peran Tertaut layanan untuk Amazon Chime

Anda menggunakan konsol IAM untuk membuat peran yang terhubung dengan layanan menggunakan kasus penggunaan Transkripsi Chime.

> **Note**
>
> Anda harus memiliki izin administratif IAM Jika tidak, hubungi administrator sistem.

Untuk membuat peran

1. Login ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Buat Peran.
3. Pilih jenis peran Layanan AWS, lalu pilih Chime, lalu pilih Transkripsi Chime.
4. Pilih Selanjutnya.
5. Pilih Selanjutnya.
6. Edit deskripsi sesuai kebutuhan, lalu pilih Buat peran.

Anda juga dapat menggunakanAWS CLI atauAWS API untuk membuat peran tertaut layanan dengan transcription.chime.amazonaws.com.

Di CLI, jalankan perintah ini:`aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit Peran Tertaut layanan untuk Amazon Chime

Amazon Chime tidak mengizinkan Anda untuk mengedit peran AWSServiceRoleForAmazonChimeTranscription tertaut layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menggunakan IAM untuk mengedit deskripsi peran. Untuk informasi lebih lanjut, lihat Mengedit Peran Tertaut Layanan di Panduan Pengguna IAM.

Menghapus Peran Tertaut layanan untuk Amazon Chime

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForAmazonChimeTranscription. Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Tertaut layanan

Amazon Chime mendukung penggunaan Peran Tertaut layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon Chime, dan Menggunakan Wilayah media Amazon Chime SDK.

Menggunakan peran dengan pipeline media Amazon Chime SDK

Informasi di bagian berikut menjelaskan cara membuat dan mengelola peran terkait layanan untuk Amazon Chime SDK Media Pipelines.

Topik

- Izin peran tertaut layanan untuk saluran media Amazon Chime SDK
- Membuat Peran Terkait Layanan untuk Peran Media Amazon Chime SDK
- Mengedit Peran Terkait Layanan untuk Peran Media Amazon Chime SDK
- Menghapus Peran Terkait Layanan untuk Peran Media Amazon Chime SDK
- Wilayah yang Didukung untuk Peran Terkait Layanan Amazon Chime SDK

Izin peran tertaut layanan untuk saluran media Amazon Chime SDK

Amazon Chime menggunakan peran tertaut layanan yang bernama AWSServiceRoleForAmazonChimeSDKMediaPipelines— Memungkinkan saluran media Amazon Chime SDK untuk mengakses rapat Amazon Chime SDK atas nama Anda.

Peran AWSServiceRoleForAmazonChimeSDKMediaPipelines tertaut layanan memercayakan layanan berikut untuk mengambil peran:

- `mediapipelines.chime.amazonaws.com`

Peran ini memungkinkan Amazon Chime untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `chime:CreateAttendee` pada `all AWS resources`
- Tindakan: `chime:DeleteAttendee` pada `all AWS resources`
- Tindakan: `chime:GetMeeting` pada `all AWS resources`

Anda harus mengonfigurasikan izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran terhubung dengan layanan. Untuk informasi lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat Peran Terkait Layanan untuk Peran Media Amazon Chime SDK

Anda menggunakan konsol IAM untuk membuat peran tertaut layanan dengan kasus penggunaan Amazon Chime SDK Media Pipelines*.

> **Note**
>
> Anda harus memiliki izin administrasi IAM untuk menyelesaikan langkah-langkah ini. Jika tidak, hubungi administrator sistem.

Untuk membuat peran

1. Login ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, lalu pilih Buat peran.
3. Pilih jenis peran AWSLayanan, lalu pilih Chime, lalu pilih Chime SDK Media Pipelines.
4. Pilih Selanjutnya.
5. Pilih Selanjutnya.
6. Edit deskripsi sesuai kebutuhan, lalu pilih Buat peran.

Anda juga dapat menggunakanAWS APIAWS CLI atau untuk membuat peran tertaut layanan dengan nama mediapipelines.chime.amazonaws.com.

DalamAWS CLI, jalankan perintah ini:`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit Peran Terkait Layanan untuk Peran Media Amazon Chime SDK

Amazon Chime tidak mengizinkan Anda untuk mengedit peran AWSServiceRoleForAmazonChimeSDKMediaPipelines tertaut layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit Peran Tertaut Layanan di Panduan Pengguna IAM.

Menghapus Peran Terkait Layanan untuk Peran Media Amazon Chime SDK

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForAmazonChimeSDKMediaPipelines. Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Terkait Layanan Amazon Chime SDK

Amazon Chime SDK mendukung penggunaan peran tertaut layanan di semuaAWS Wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Endpoint dan kuota Amazon Chime.

Pencatatan dan pemantauan di Amazon Chime

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja Amazon Chime danAWS solusi Anda lainnya. AWSmenyediakan alat berikut untuk memantau Amazon Chime, melaporkan masalah, dan mengambil tindakan otomatis jika diperlukan:

- Amazon CloudWatch memantau secara waktu nyataAWS sumber daya Anda dan aplikasi yang Anda jalankan padaAWS. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat membuat CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis

meluncurkan instans baru ketika diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

- Amazon EventBridge memberikan aliran kejadian sistem secara hampir waktu-nyata yang menjelaskan perubahan dalamAWS sumber daya. EventBridge memungkinkan komputasi otomatis Dengan demikian Anda dapat menulis aturan yang mengawasi kejadian tertentu, dan memicu tindakan otomatis dalamAWS layanan lainnya saat tindakan ini terjadi. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log dari instans Amazon EC2, CloudTrail, dan sumber lainnya. CloudWatch Pencatatan dapat memantau informasi dalam berkas log dan memberi tahu Anda ketika ambang tertentu terpenuhi. Anda juga dapat mengarsipkan data log Anda dalam penyimpanan yang sangat tahan lama. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmerekam panggilan API dan peristiwa terkait yang dilakukan oleh atau atas namaAWS akun Anda. Kemudian, mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil AWS, alamat IP sumber yang melakukan panggilan, dan kapan panggilan tersebut terjadi. Untuk mengetahui informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

Memantau Amazon Chime dengan Amazon CloudWatch

Anda dapat memantau Amazon Chime menggunakan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca dan hampir waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi riwayat dan mendapatkan perspektif yang lebih baik tentang bagaimana kinerja aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

CloudWatch metrik untuk Amazon Chime

Amazon Chime mengirimkan metrik berikut ke CloudWatch.

`AWS/ChimeVoiceConnector`Namespace menyertakan metrik berikut untuk nomor telepon yang ditetapkan keAWS akun Anda dan ke Amazon Chime Voice Connectors.

Metrik	Deskripsi
`InboundCallAttempts`	Jumlah panggilan masuk yang dilakukan. Unit: Count (Jumlah)
`InboundCallFailures`	Jumlah kegagalan panggilan masuk. Unit: Count (Jumlah)
`InboundCallsAnswered`	Jumlah panggilan masuk yang dijawab. Unit: Count (Jumlah)
`InboundCallsActive`	Jumlah panggilan masuk yang saat ini aktif. Unit: Count (Jumlah)
`OutboundCallAttempts`	Jumlah panggilan keluar yang dilakukan. Unit: Count (Jumlah)
`OutboundCallFailures`	Jumlah kegagalan panggilan keluar. Unit: Count (Jumlah)
`OutboundCallsAnswered`	Jumlah panggilan keluar yang dijawab. Unit: Count (Jumlah)
`OutboundCallsActive`	Jumlah panggilan keluar yang saat ini aktif. Unit: Count (Jumlah)
`Throttles`	Berapa kali akun Anda dibatasi saat mencoba melakukan panggilan. Unit: Count (Jumlah)

Metrik	Deskripsi
`Sip1xxCodes`	Jumlah pesan SIP dengan kode status 1xx-level. Unit: Count (Jumlah)
`Sip2xxCodes`	Jumlah pesan SIP dengan kode status 2xx-level. Unit: Count (Jumlah)
`Sip3xxCodes`	Jumlah pesan SIP dengan kode status 3xx-level. Unit: Count (Jumlah)
`Sip4xxCodes`	Jumlah pesan SIP dengan kode status 4xx-level. Unit: Count (Jumlah)
`Sip5xxCodes`	Jumlah pesan SIP dengan kode status 5xx-level. Unit: Count (Jumlah)
`Sip6xxCodes`	Jumlah pesan SIP dengan kode status 6xx-level. Unit: Count (Jumlah)
`CustomerToVcRtpPackets`	Jumlah paket RTP yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)

Metrik	Deskripsi
CustomerToVcRtpBytes	Jumlah byte yang dikirim dari pelanggan ke Amazon Chime Voice Connector dalam paket RTP. Unit: Count (Jumlah)
CustomerToVcRtcpPackets	Jumlah paket RTCP yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)
CustomerToVcRtcpBytes	Jumlah byte yang dikirim dari pelanggan ke Amazon Chime Voice Connector dalam paket RTCP. Unit: Count (Jumlah)
CustomerToVcPacketsLost	Jumlah paket yang hilang saat transit dari pelanggan ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)
CustomerToVcJitter	Jitter rata-rata untuk paket yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector. Unit
VcToCustomerRtpPackets	Jumlah paket RTP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke pelanggan. Unit: Count (Jumlah)

Metrik	Deskripsi
VcToCustomerRtpBytes	Jumlah byte yang dikirim dari Amazon Chime Voice Connector ke pelanggan dalam paket RTP. Unit: Count (Jumlah)
VcToCustomerRtcpPackets	Jumlah paket RTCP yang dikirim dari infrastruktur Amazon Chime Voice Connector ke pelanggan. Unit: Count (Jumlah)
VcToCustomerRtcpBytes	Jumlah byte yang dikirim dari Amazon Chime Voice Connector ke pelanggan dalam paket RTCP. Unit: Count (Jumlah)
VcToCustomerPacketsLost	Jumlah paket yang hilang saat transit dari infrastruktur Amazon Chime Voice Connector ke pelanggan. Unit: Count (Jumlah)
VcToCustomerJitter	Jitter rata-rata untuk paket yang dikirim dari infrastruktur Amazon Chime Voice Connector ke pelanggan. Unit
RTTBetweenVcAndCustomer	Rata-rata waktu pulang-pergi antara pelanggan dan infrastruktur Amazon Chime Voice Connector. Unit

Metrik	Deskripsi
`MOSBetweenVcAndCustomer`	Perkiraan Mean opinion score (MOS) yang terkait dengan aliran suara antara pelanggan dan infrastruktur Amazon Chime Voice Connector. Unit: Skor antara 1,0-4,4. Skor yang lebih tinggi menunjukkan kualitas audio yang dirasakan lebih baik.
`RemoteToVcRtpPackets`	Jumlah paket RTP yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)
`RemoteToVcRtpBytes`	Jumlah byte yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector dalam paket RTP. Unit: Count (Jumlah)
`RemoteToVcRtcpPackets`	Jumlah paket RTCP yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)
`RemoteToVcRtcpBytes`	Jumlah byte yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector dalam paket RTCP. Unit: Count (Jumlah)
`RemoteToVcPacketsLost`	Jumlah paket yang hilang saat transit dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector. Unit: Count (Jumlah)

Metrik	Deskripsi
RemoteToVcJitter	Jitter rata-rata untuk paket yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector. Unit
VcToRemoteRtpPackets	Jumlah paket RTP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke ujung jarak jauh. Unit: Count (Jumlah)
VcToRemoteRtpBytes	Jumlah byte yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh dalam paket RTP. Unit: Count (Jumlah)
VcToRemoteRtcpPackets	Jumlah paket RTCP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke ujung jarak jauh. Unit: Count (Jumlah)
VcToRemoteRtcpBytes	Jumlah byte yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh dalam paket RTCP. Unit: Count (Jumlah)
VcToRemotePacketsLost	Jumlah paket yang hilang saat transit dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh. Unit: Count (Jumlah)

Metrik	Deskripsi
`VcToRemoteJitter`	Jitter rata-rata untuk paket yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh. Unit
`RTTBetweenVcAndRemote`	Rata-rata waktu pulang-pergi antara remote end dan infrastruktur Amazon Chime Voice Connector. Unit
`MOSBetweenVcAndRemote`	Perkiraan Mean opinion score (MOS) yang terkait dengan aliran suara antara remote end dan infrastruktur Amazon Chime Voice Connector. Unit: Unit: Skor antara 1,0-4,4. Skor yang lebih tinggi menunjukkan kualitas audio yang dirasakan lebih baik.

CloudWatch dimensi untuk Amazon Chime

CloudWatch Dimensi yang dapat Anda gunakan dengan Amazon Chime tercantum sebagai berikut.

Dimensi	Deskripsi
`VoiceConnectorId`	Pengenal Amazon Chime Voice Connector untuk menampilkan metrik.
`Region`	AWSWilayah yang terkait dengan kejadian.

CloudWatch log untuk Amazon Chime

Anda dapat mengirim metrik Konektor Suara Amazon Chime ke CloudWatch Log. Untuk informasi selengkapnya, lihat Mengedit pengaturan Konektor Suara Amazon Chime di Panduan Administrasi Amazon Chime SDK.

Log metrik kualitas media

Anda dapat memilih untuk menerima log metrik kualitas media untuk Konektor Suara Amazon Chime Anda. Saat Anda melakukannya, Amazon Chime mengirimkan metrik terperinci per menit untuk semua panggilan Konektor Suara Amazon Chime Anda ke grup CloudWatch log Log yang dibuat untuk Anda. Nama grup`/aws/ChimeVoiceConnectorLogs/${`*`VoiceConnectorID`*`}` Bidang berikut disertakan dalam log, dalam format JSON.

Bidang	Deskripsi
voice_connector_id	Amazon Chime Voice Connector ID membawa panggilan.
event_timestamp	Waktu saat metrik dipancarkan, dalam detik sejak jangka waktunya sejak jangka waktunya (tengah malam pada 1 Januari 1970) di UTC.
call_id	Sesuai dengan ID Transaksi.
dari_sip_user	Pengguna yang memulai panggilan.
dari_negara	Negara penggagas untuk panggilan.
sip_user	Pengguna penerima untuk panggilan.
to_country	Negara penerima untuk panggilan.
endpoint_id	Pengenal buram yang menunjukkan titik akhir panggilan lainnya. Gunakan dengan Wawasan CloudWatch Log. Untuk informasi selengkap nya, lihat Menganalisis data CloudWatch log dengan Wawasan Log di Panduan Pengguna Amazon CloudWatch Logs.

Bidang	Deskripsi
aws_region	AWSWilayah untuk panggilan.
cust2vc_rtp_packets	Jumlah paket RTP yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector.
cust2vc_rtp_bytes	Jumlah byte yang dikirim dari pelanggan ke Amazon Chime Voice Connector dalam paket RTP.
cust2vc_rtcp_packets	Jumlah paket RTCP yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector.
cust2vc_rtcp_bytes	Jumlah byte yang dikirim dari pelanggan ke Amazon Chime Voice Connector dalam paket RTCP.
cust2vc_packets_lost	Jumlah paket yang hilang saat transit dari pelanggan ke infrastruktur Amazon Chime Voice Connector.
cust2vc_jitter	Jitter rata-rata untuk paket yang dikirim dari pelanggan ke infrastruktur Amazon Chime Voice Connector.
vc2cust_rtp_packets	Jumlah paket RTP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke pelanggan.
vc2cust_rtp_bytes	Jumlah byte yang dikirim dari Amazon Chime Voice Connector ke pelanggan dalam paket RTP.
vc2cust_rtcp_packets	Jumlah paket RTCP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke pelanggan.

Bidang	Deskripsi
vc2cust_rtcp_bytes	Jumlah byte yang dikirim dari Amazon Chime Voice Connector ke pelanggan dalam paket RTCP.
vc2cust_packets_lost	Jumlah paket yang hilang saat transit dari infrastruktur Amazon Chime Voice Connector ke pelanggan.
vc2cust_jitter	Jitter rata-rata untuk paket yang dikirim dari infrastruktur Amazon Chime Voice Connector ke pelanggan.
rtt_btwn_vc_and_cust	Rata-rata waktu pulang-pergi antara pelanggan dan infrastruktur Amazon Chime Voice Connector.
mos_btwn_vc_and_cust	Perkiraan Mean opinion score (MOS) yang terkait dengan aliran suara antara pelanggan dan infrastruktur Amazon Chime Voice Connector.
rem2vc_rtp_packets	Jumlah paket RTP yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector.
rem2vc_rtp_byte	Jumlah byte yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector dalam paket RTP.
rem2vc_rtcp_packets	Jumlah paket RTCP yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector.
rem2vc_rtcp_byte	Jumlah byte yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector dalam paket RTCP.

Bidang	Deskripsi
rem2vc_packets_lost	Jumlah paket yang hilang saat transit dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector.
rem2vc_jitter	Jitter rata-rata untuk paket yang dikirim dari ujung jarak jauh ke infrastruktur Amazon Chime Voice Connector.
vc2rem_rtp_packets	Jumlah paket RTP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke ujung jarak jauh.
vc2rem_rtp_bytes	Jumlah byte yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh dalam paket RTP.
vc2rem_rtcp_packets	Jumlah paket RTCP yang dikirim dari infrastru ktur Amazon Chime Voice Connector ke ujung jarak jauh.
vc2rem_rtcp_bytes	Jumlah byte yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh dalam paket RTCP.
vc2rem_packets_lost	Jumlah paket yang hilang saat transit dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh.
vc2rem_jitter	Jitter rata-rata untuk paket yang dikirim dari infrastruktur Amazon Chime Voice Connector ke ujung jarak jauh.
rtt_btwn_vc_and_rem	Rata-rata waktu pulang-pergi antara remote end dan infrastruktur Amazon Chime Voice Connector.

Bidang	Deskripsi
mos_btwn_vc_and_rem	Perkiraan Mean opinion score (MOS) yang terkait dengan aliran suara antara remote end dan infrastruktur Amazon Chime Voice Connector.

log

Anda dapat memilih untuk menerima log pesan SIP untuk Konektor Suara Amazon Chime Anda. Ketika Anda melakukannya, Amazon Chime menangkap pesan SIP masuk dan keluar dan mengirimkannya ke grup CloudWatch log Log yang dibuat untuk Anda. Nama grup`/aws/ChimeVoiceConnectorSipMessages/${`*`VoiceConnectorID`*`}` Bidang berikut disertakan dalam log, dalam format JSON.

Bidang	Deskripsi
voice_connector_id	ID Amazon Chime Voice Connector.
aws_region	AWSWilayah yang terkait dengan kejadian.
event_timestamp	Waktu saat pesan diambil, dalam jumlah milidetik sejak jangka waktunya (tengah malam pada 1 Januari 1970) di UTC.
call_id	ID panggilan Amazon Chime Voice Connector.
sip_message	Pesan SIP lengkap yang ditangkap.

Mengotomatisasi Amazon Chime dengan EventBridge

Amazon EventBridge memungkinkan Anda mengotomatiskanAWS layanan Anda dan merespons peristiwa sistem secara otomatis seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Untuk informasi selengkapnya tentang acara rapat, lihat Acara pertemuan di Panduan Pengembang Amazon Chime.

Ketika Amazon Chime membuat peristiwa, ia mengirim mereka ke EventBridge pengiriman dengan upaya terbaik, yang berarti Amazon Chime mencoba untuk mengirim semua peristiwa EventBridge, tetapi dalam kasus yang jarang terjadi, peristiwa mungkin tidak terkirim. Untuk informasi selengkapnya, lihat Acara dariAWS layanan di Panduan EventBridge Pengguna Amazon.

> **Note**
>
> Jika Anda perlu mengenkripsi data, Anda harus menggunakan Amazon S3-Managed Keys. Kami tidak mendukung enkripsi sisi server menggunakan Kunci Master Pelanggan yang disimpan dalam Layanan ManajemenAWS Kunci.

Mengotomatisasi Amazon Chime Voice Connector EventBridge

Tindakan yang dapat dipicu secara otomatis untuk Amazon Chime Voice Connector mencakup hal berikut:

- Memanggil fungsi AWS Lambda
- Meluncurkan tugas Amazon Elastic
- Mengirimkan kejadian ke Amazon Kinesis Video Streams
- Mengaktifkan mesin keadaan AWS Step Functions
- Memberi tahu topik Amazon SNS atau antrean Amazon SQS

Beberapa contoh penggunaan EventBridge dengan Amazon Chime Voice Connectors meliputi:

- Mengaktifkan fungsi Lambda untuk mengunduh audio untuk panggilan setelah panggilan berakhir.
- Meluncurkan tugas Amazon ECS untuk mengaktifkan transkripsi waktu nyata setelah panggilan dimulai.

Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Peristiwa Amazon Chime Voice Connector

Konektor Suara Amazon Chime mendukung pengiriman peristiwa EventBridge saat peristiwa yang dibahas di bagian ini terjadi.

Streaming Amazon Chime Voice Connector

Konektor Suara Amazon Chime mengirim acara ini saat streaming media ke Kinesis Video Streams dimulai.

Example Data Peristiwa

Berikut adalah contoh data untuk peristiwa ini.


```
{
    "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"
    }
}
```

Streaming Amazon Chime Voice Connector

Konektor Suara Amazon Chime mengirim acara ini saat streaming media ke Kinesis Video Streams berakhir.

Example Data Peristiwa

Berikut adalah contoh data untuk peristiwa ini.

```
{
    "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"
    }
}
```

Pembaruan streaming Amazon Chime Voice Connector

Konektor Suara Amazon Chime mengirim acara ini saat streaming media ke Kinesis Video Streams diperbarui.

Example Data Peristiwa

Berikut adalah contoh data untuk peristiwa ini.

```
{
    "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"
    }
}
```

Streaming Amazon Chime Voice Connector

Konektor Suara Amazon Chime mengirim acara ini saat streaming media ke Kinesis Video Streams gagal.

Example Data Peristiwa

Berikut adalah contoh data untuk peristiwa ini.

```
{
  "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"
  }
}
```

Mencatat panggilan API Amazon ChimeAWS CloudTrail

Amazon Chime terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWS layanan di Amazon Chime. CloudTrail menangkap semua panggilan API untuk Amazon Chime sebagai peristiwa, termasuk panggilan dari konsol Amazon Chime dan panggilan kode ke API Amazon Chime. Jika membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk Amazon Chime. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam CloudTrail konsol di Riwayat peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon Chime, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

Informasi Amazon Chime di CloudTrail

CloudTrail diaktifkan diAWS akun Anda saat Anda membuat akun. Ketika panggilan API dibuat dari konsol administrasi Amazon Chime, aktivitas tersebut dicatat di CloudTrail peristiwa bersama peristiwaAWS layanan lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail peristiwa.

Untuk catatan peristiwa yang sedang berlangsung diAWS akun Anda, termasuk peristiwa untuk Amazon Chime, buatlah jejak. Jejak memungkinkan CloudTrail untuk mengirimkan berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah . Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasiAWS layanan lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan: Data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat :

- Gambaran
- CloudTrail Layanan yang didukung dan integrasi
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan Amazon Chime dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Amazon Chime. Misalnya, panggilan ke`CreateAccount`,`InviteUsers` dan`ResetPersonalPIN` bagian menghasilkan entri dalam file CloudTrail log. Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Jika permintaan tersebut dibuat dengan kredensial pengguna root atau IAM.
- Jika permintaan tersebut dibuat dengan kredensi keamanan sementara untuk peran, atau pengguna gabungan.
- Bahwa permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log Amazon Chime

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau beberapa entri log Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail berkas log bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Entri untuk Amazon Chime diidentifikasi oleh sumber peristiwa chime.amazonaws.com.

Jika Anda telah mengonfigurasi Active Directory untuk akun Amazon Chime Anda, lihat Menggunakan Log panggilan API AWS Directory Service CloudTrail. Ini menjelaskan cara memantau masalah yang mungkin memengaruhi kemampuan pengguna Amazon Chime Anda untuk masuk.

Contoh berikut menunjukkan entri CloudTrail log untuk Amazon Chime:


```
{"eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":" AAAAAABBBBBBBBEXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice ",
            "accountId":"0123456789012",
            "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
            "sessionContext":{
               "attributes":{
                  "mfaAuthenticated":"false",
```

```
                "creationDate":"2017-07-24T17:57:43Z"
             },
             "sessionIssuer":{
                "type":"Role",
                "principalId":"AAAAAABBBBBBBBEXAMPLE",
                "arn":"arn:aws:iam::123456789012:role/Joe",
                "accountId":"123456789012",
                "userName":"Joe"
             }
          }
       } ,
       "eventTime":"2017-07-24T17:58:21Z",
       "eventSource":"chime.amazonaws.com",
       "eventName":"AddDomain",
       "awsRegion":"us-east-1",
       "sourceIPAddress":"72.21.198.64",
       "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
       "errorCode":"ConflictException",
       "errorMessage":"Request could not be completed due to a conflict",
       "requestParameters":{
          "domainName":"example.com",
          "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
       },
       "responseElements":null,
       "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
       "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
       "eventType":"AwsApiCall",
       "recipientAccountId":"123456789012"
    }
```


Validasi kepatuhan untuk Amazon Chime

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS layanan sebagai bagian dari beberapa program AWS kepatuhan, seperti SOC, PCI, FedRAMP, dan HIPAA.

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Amazon Chime

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Amazon Chime menawarkan berbagai fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda. Untuk informasi selengkapnya, lihat Mengelola grup Amazon Chime Voice Connector dan Streaming media Amazon Chime Voice Connector ke Kinesis di Panduan Administrasi SDK Amazon Chime.

Keamanan infrastruktur di Amazon Chime

Sebagai layanan terkelola, Amazon Chime dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Memahami pembaruan otomatis Amazon Chime

Amazon Chime menyediakan berbagai cara untuk memperbarui kliennya. Metode ini bervariasi, tergantung pada apakah pengguna Anda menjalankan Amazon Chime di browser, di desktop, atau di perangkat seluler.

Aplikasi web Amazon Chime - https://app.chime.aws - selalu memuat dengan fitur terbaru dan perbaikan keamanan.

Klien desktop Amazon Chime memeriksa pembaruan setiap kali pengguna memilih Keluar atau Keluar. Ini berlaku untuk mesin Windows dan macOS. Saat pengguna menjalankan klien, ia memeriksa pembaruan setiap tiga jam. Pengguna juga dapat memeriksa pembaruan dengan memilih Periksa Pembaruan di menu Bantuan Windows atau di menu MacOS Amazon Chime.

Saat klien desktop mendeteksi pembaruan, Amazon Chime meminta pengguna untuk menginstalnya kecuali mereka sedang dalam rapat yang sedang berlangsung. Pengguna sedang dalam rapat yang sedang berlangsung ketika:

- Mereka menghadiri pertemuan.
- Mereka diundang ke pertemuan yang masih berlangsung.

Amazon Chime meminta mereka untuk menginstal versi terbaru, dan itu memberi mereka hitungan mundur 15 detik sehingga mereka dapat menunda instalasi. Pilih Coba Nanti untuk menunda pembaruan.

Ketika pengguna menunda pembaruan, dan mereka tidak dalam rapat yang sedang berlangsung, klien memeriksa pembaruan setelah tiga jam dan meminta mereka lagi untuk menginstal. Instalasi dimulai ketika hitungan mundur berakhir.

> **Note**
>
> Pada mesin macOS, pengguna harus memilih Restart Now untuk memulai pembaruan.

Di perangkat seluler - Aplikasi seluler Amazon Chime menggunakan opsi pembaruan yang disediakan oleh App Store dan Google Play untuk menghadirkan versi terbaru klien Amazon Chime. Anda juga dapat mendistribusikan pembaruan melalui sistem manajemen perangkat seluler Anda. Topik ini mengasumsikan bahwa Anda tahu caranya.

Riwayat dokumen untuk Amazon Chime

Tabel berikut menjelaskan perubahan penting pada Panduan Administrator Amazon Chime, dimulai pada Maret 2018. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Panduan Administrasi Amazon Chime SDK diterbitkan	Topik Amazon Chime SDK sekarang diterbitkan di Panduan Administrasi SDK Amazon Chime. Untuk selengkapnya, lihat Panduan Administrasi SDK Amazon Chime.	24 Maret 2022
Pembaruan kebijakan IAM	Perubahan pada kebijakan IAM yang dikelola oleh sekarang AWS dilacak dalam panduan administrator ini. Lihat contoh kebijakan berbasis identitas Amazon Chime.	September 23, 2021
Peran terkait layanan	Administrator sekarang dapat membuat peran terkait layanan untuk Transkripsi Amazon Live, dan melihat pesan peristiwa saat operasi transkripsi langsung Amazon Chime dimulai dan berakhir. Untuk informasi selengkap nya, lihat Menggunakan peran dengan transkripsi langsung dan Mengotoma	Agustus 12, 2021

	tiskan Amazon CloudWatch Chime dengan peristiwa.	
Aplikasi dan aturan media SIP	Administrator dapat membuat aplikasi dan aturan media SIP untuk digunakan dengan Konektor AWS Lambda dan fungsi Amazon Chime Voice. Untuk informasi selengkap nya, lihat Mengelola aplikasi dan aturan SIP, di Panduan Administrator Amazon Chime.	18 November 2020
Nomor perutean panggilan darurat Amazon Chime Voice Connector	Administrator Amazon Chime dapat mengatur nomor perutean panggilan darurat untuk Konektor Suara Amazon Chime. Untuk informasi selengkapnya, lihat Menyiapka n nomor perutean panggilan darurat untuk Konektor Suara Amazon Chime, di Panduan Administrator Amazon Chime.	1 Juli 2020
Amazon Chime di Dolby Voice Huddle	Amazon Chime menawarka n pengalaman pertemuan asli atau pihak pertama pada perangkat keras konferensi audio dan video Dolby Voice Huddle. Untuk informasi selengkapnya, lihat Menyiapka n Amazon Chime di Perangkat Keras Dolby, di Panduan Administrator Amazon Chime.	3 Juni 2020

Menyetel kebijakan retensi obrolan	Administrator Amazon Chime dapat menyetel kebijakan retensi obrolan untuk akun Enterprise mereka. Untuk informasi selengkapnya, lihat Mengelola kebijakan penyimpanan obrolan, di Panduan Administrator Amazon Chime.	21 Mei 2020
Menghapus pesan obrolan	Jika Anda memiliki kemampuan untuk memprogram, Anda dapat menggunakan sepasang Amazon Chime API untuk menghapus pesan dari ruang obrolan dan percakapan di akun Anda. Untuk informasi selengkapnya, lihat Menghapus pesan individual, di Panduan Administrator Amazon Chime.	18 Mei 2020
CloudWatch metrik kualitas media untuk Konektor Suara Amazon Chime	Amazon Chime mendukung pengiriman metrik kualitas media untuk Konektor Suara Amazon Chime Anda. CloudWatch Untuk informasi selengkapnya, lihat Memantau Lonceng Amazon dengan CloudWatch, di Panduan Administrator Amazon Chime.	23 Januari 2020

Aplikasi Amazon Chime Meetings untuk Slack	Amazon Chime mendukung Aplikasi Amazon Chime Meetings untuk Slack. Untuk informasi selengkapnya, lihat Menyiapkan Aplikasi Rapat Amazon Chime untuk Slack, di Panduan Administrator Amazon Chime.	4 Desember 2019
Pengaturan Wilayah Rapat	Amazon Chime mendukung pemrosesan rapat di AWS Wilayah optimal untuk semua peserta. Untuk informasi selengkapnya, lihat Pengaturan Wilayah Rapat, di Panduan Administrator Amazon Chime.	3 Desember 2019
Kompatibilitas perekaman media berbasis SIP (SIPREC)	Konektor Suara Amazon Chime mendukung media streaming dari infrastruktur suara yang kompatibel dengan Siprec ke Kinesis Video Streams. Untuk informasi selengkapnya, lihat Kompatibilitas perekaman media berbasis SIP (SIPREC), di Panduan Administrator Amazon Chime.	25 November 2019

Amazon Chime di Ruang Suara Dolby	Jika Anda ingin pengguna bergabung dengan rapat dengan nyaman, Amazon Chime menawarkan pengalaman pertemuan asli atau pihak pertama pada perangkat keras konferens i audio dan video Dolby Voice Room. Untuk informasi selengkapnya, lihat Menyiapka n Amazon Chime di Ruang Suara Dolby, di Panduan Administrator Amazon Chime.	Oktober 29, 2019
Memperbarui nama panggilan keluar	Tetapkan nama panggilan default yang muncul ke penerima panggilan keluar yang dilakukan menggunak an nomor telepon di inventari s Amazon Chime Anda. Untuk informasi selengkapnya, lihat Memperbarui nama panggilan keluar, di Panduan Administr ator Amazon Chime.	24 Oktober 2019

Media streaming ke Amazon Kinesis	Streaming audio panggilan telepon dari Amazon Chime Voice Connectors ke Kinesis Video Streams untuk analitik, pembelajaran mesin, dan pemrosesan lainnya. Untuk informasi selengkapnya, lihat Streaming media Konektor Suara Amazon Chime ke Kinesis dan Menggunakan peran terkait layanan Konektor Suara Amazon Chime, di Panduan Administrator Amazon Chime.	24 Oktober 2019
Memantau Amazon Chime dengan Amazon CloudWatch	Pantau penggunaan Amazon Chime CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Untuk informasi selengkapnya, lihat Memantau Lonceng Amazon dengan CloudWatch, di Panduan Administrator Amazon Chime.	24 Oktober 2019

Grup Konektor Suara Amazon Chime	Buat grup Konektor Suara Amazon Chime yang menyertakan Konektor Suara Amazon Chime yang dibuat di berbagai Wilayah. AWS Hal ini memungkinkan panggilan masuk gagal di seluruh Wilayah, yang menciptakan mekanisme toleran kesalahan untuk fallback jika terjadi peristiwa ketersediaan. Untuk informasi selengkapnya, lihat Bekerja dengan grup Amazon Chime Voice Connector, di Panduan Administrator Amazon Chime.	24 Oktober 2019
Pembaruan konfigurasi jaringan	Amazon Chime menyederh anakan persyaratan firewall-nya. Untuk informasi selengkapnya, lihat Konfigurasi jaringan dan persyaratan bandwidth, di Panduan Administrator Amazon Chime.	6 September 2019
Pertemuan yang dimoderasi	Amazon Chime mendukung rapat yang dimoderasi. Untuk informasi selengkapnya, lihat Bergabung dengan rapat yang dimoderasi, di Panduan Administrator Amazon Chime.	25 Juli 2019

Validasi kepatuhan untuk Amazon Chime	Amazon Chime adalah Layanan yang Memenuhi Syarat HIPAA. Untuk informasi selengkapnya, lihat Validasi kepatuhan untuk Amazon Chime di Panduan Administrator Amazon Chime.	11 Juni 2019
Porting nomor telepon bebas pulsa	Amazon Chime mendukung porting nomor telepon Amerika Serikat bebas pulsa untuk digunakan dengan Konektor Suara Amazon Chime. Untuk informasi selengkapnya, lihat Mem-porting nomor telepon yang ada, di Panduan Administrator Amazon Chime.	28 Mei 2019
Mengelola nomor telepon di Amazon Chime	Gunakan Panggilan Bisnis Amazon Chime untuk menyediakan dan menetapkan nomor telepon ke pengguna Amazon Chime. Integrasikan Konektor Suara Amazon Chime dengan sistem telepon yang ada. Untuk informasi selengkapnya, lihat Mengelola nomor telepon di Amazon Chime di Panduan Administrator Amazon Chime.	18 Maret 2019

Amazon Chime Add-In untuk Outlook	Amazon Chime menyediakan dua add-in untuk Microsoft Outlook: Amazon Chime Add-In untuk Outlook di Windows dan Amazon Chime Add-In untuk Outlook. Add-in ini menawarkan fitur penjadwalan yang sama, tetapi mendukung berbagai jenis pengguna. Untuk informasi selengkapnya, lihat Menerapkan Add-In untuk Outlook, di Panduan Administrator Amazon Chime.	12 Maret 2019
Berbagai pembaruan	Berbagai pembaruan untuk tata letak topik dan organisasi.	11 Februari 2019
Fitur Amazon Chime panggil saya	Administrator dapat mengaktifkan fitur Amazon Chime call me di bawah pengaturan Rapat mereka. Untuk informasi selengkapnya, lihat Mengelola setelan rapat, di Panduan Administrator Amazon Chime.	22 Agustus 2018
Connect ke Okta SSO	Jika Anda memiliki akun perusahaan, Anda dapat terhubung ke Okta SSO untuk mengautentikasi dan menetapkan izin pengguna. Untuk informasi selengkapnya, lihat Connect to Okta SSO, di Panduan Administrator Amazon Chime.	1 Agustus 2018

Minta lampiran pengguna	Terima lampiran yang diunggah ke Amazon Chime oleh pengguna. Untuk informasi selengkapnya, lihat Meminta lampiran pengguna, di Panduan Administrator Amazon Chime.	23 April 2018
Lihat data laporan tambahan	Lihat data laporan tambahan. Untuk informasi selengkapnya, lihat Melihat laporan, di Panduan Administrator Amazon Chime.	Maret 30, 2018
Tetapkan pengguna Izin Pro atau Dasar	Tetapkan pengguna Izin Pro atau Dasar. Untuk informasi selengkapnya, lihat Mengelola akses dan izin pengguna, di Panduan Administrator Amazon Chime.	29 Maret 2018