Guida di amministrazione

Amazon Chime

Amazon Chime: Guida di amministrazione

Table of Contents

Devi essere un amministratore di sistema Amazon Chime per completare i passaggi di questa guida. Se hai bisogno di assistenza con il client desktop, l'app Web o l'app mobile Amazon Chime, consulta Ottenere assistenza nella Guida per l'utente di Amazon Chime.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.

Cos'è Amazon Chime?

Amazon Chime è un servizio di comunicazione che trasforma le riunioni online con un'applicazione sicura e completa. Amazon Chime funziona su tutti i tuoi dispositivi in modo che tu possa rimanere connesso. Puoi usare Amazon Chime per riunioni online, videoconferenze, chiamate e chat. Puoi anche condividere contenuti all'interno e all'esterno della tua organizzazione. Amazon Chime è un servizio completamente gestito che viene eseguito in modo sicuro sulAWS cloud, che libera l'IT dall'implementazione e dalla gestione di infrastrutture complesse.

Per ulteriori informazioni, consulta Amazon Chime.

Panoramica sull'amministrazione

In qualità di amministratore, usi la console Amazon Chime per eseguire attività chiave, come la creazione di account Amazon Chime e la gestione di utenti e autorizzazioni. Per accedere alla console Amazon Chime e creare un account amministratore Amazon Chime, crea prima unAWS account. Per ulteriori informazioni, consulta Prerequisiti per gli amministratori di sistema Amazon Chime.

Come iniziare

Dopo aver completato ilPrerequisiti per gli amministratori di sistema Amazon Chime, puoi creare e configurare il tuo account amministrativo Amazon Chime, quindi aggiungere utenti ad esso. Scegli le autorizzazioni Base o Pro per i tuoi utenti.

Se sei pronto a iniziare, consulta i seguenti tutorial:

- Nozioni di base

Per ulteriori informazioni sulle autorizzazioni e sull'accesso degli utenti, consulta Gestione delle autorizzazioni e degli accessi degli utenti. Per ulteriori informazioni sulle caratteristiche a cui gli utenti con le autorizzazioni Pro e Base possono accedere, consulta Piani e i prezzi.

Prezzi

Amazon Chime offre prezzi basati sull'utilizzo. Paghi solo per gli utenti con autorizzazioni Pro che ospitano riunioni e solo per i giorni in cui tali riunioni sono ospitate. Per i partecipanti alla riunione e per gli utenti della chat non sono previsti addebiti.

Non vi è alcun costo per gli utenti con le autorizzazioni di base. Gli utenti di base non sono in grado di ospitare riunioni, ma possono partecipare alle riunioni e utilizzare la chat. Per ulteriori informazioni sui prezzi e sulle caratteristiche a cui gli utenti con autorizzazioni Pro e di base possono accedere, consulta Piani e prezzi.

Risorse

Per ulteriori informazioni su Amazon Chime, consulta le risorse seguenti:

- Centro assistenza Amazon Chime
- Video di formazione Amazon Chime

Prerequisiti per gli amministratori di sistema Amazon Chime

Devi disporre di un AWS account per accedere alla console Amazon Chime e creare un account amministratore Amazon Chime.

Creazione di un account Amazon Web Services

Prima di poter creare un account amministratore per Amazon Chime, devi prima creare un AWS account. chime

Argomenti

- Registrati per un Account AWS
- Crea un utente con accesso amministrativo

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Per ulteriori informazioni sulla configurazione del tuo account amministratore Amazon Chime, consulta. Nozioni di base

Nozioni di base

Il modo più semplice per i tuoi utenti di iniziare a usare Amazon Chime è scaricare e utilizzare la versione Amazon Chime Pro gratuitamente per 30 giorni. Per ulteriori informazioni, consulta Download Amazon Chime (Scarica Amazon Chime).

Acquisto di Amazon Chime Chime

Per continuare a utilizzare la versione Amazon Chime Pro dopo il periodo di prova gratuito di 30 giorni, devi creare un account amministratore Amazon Chime e aggiungere i tuoi utenti. Per iniziare, è necessario prima completare i Prerequisiti per gli amministratori di sistema Amazon Chime, che includono la creazione di un account AWS. Quindi, puoi creare e configurare un account amministratore Amazon Chime e aggiungervi utenti completando le seguenti attività.

Processi

- Passaggio 1: creazione di un account amministratore Amazon Chime
- Fase 2 (facoltativo): configurazione delle impostazioni dell'account
- Fase 3: aggiunta di utenti all'account
- (Facoltativo) Configurazione dei numeri di telefono per l'account Amazon Chime Chime Chime

Passaggio 1: creazione di un account amministratore Amazon Chime

Una volta completati i campiPrerequisiti per gli amministratori di sistema Amazon Chime, puoi creare un account Amazon Chime Chime Amazon Chime Chime.

Per creare un account amministratore Amazon Chime

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Accounts (Account) scegliere New account (Nuovo account).
3. Per Account Name (Nome account) digitare un nome per l'account e scegli Create account (Crea account).
4. (Facoltativo) Scegli se consentire ad Amazon Chime di selezionare laAWS regione ottimale per le tue riunioni tra tutte le regioni disponibili o utilizzare solo le regioni selezionate. Per ulteriori informazioni, consulta Gestione delle impostazioni della riunione.

Fase 2 (facoltativo): configurazione delle impostazioni dell'account

Per impostazione predefinita, i nuovi account vengono creati come account di team. Se preferisci richiedere un dominio e connetterti al tuo provider di identità o Okta SSO, puoi convertirlo in un account Enterprise. Per ulteriori informazioni sugli account di team e aziendali, consulta Scelta tra un account Amazon Chime Team o un account Enterprise.

Per convertire un account Team in un account Enterprise

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per Account, scegliere il nome dell'account.
3. Per Identity (Identità), scegliere Getting Started (Nozioni di base).
4. Attenersi alla procedura indicata nella console per rivendicare il dominio.
5. (Facoltativo) Attenersi alla procedura descritta nella console per configurare il provider di identità e configurare il gruppo di directory.

Per ulteriori informazioni sulla richiesta dei domini, consulta Dichiarazione di un dominio. Per ulteriori informazioni sulla configurazione dei provider di identità, consulta Connessione ad Active Directory e Connessione al servizio SSO di Okta.

Puoi anche consentire o smettere di consentire le politiche dell'account relative a opzioni, come il controllo remoto degli schermi condivisi e la funzione chiamami di Amazon Chime.

Per configurare le policy dell'account

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Accounts (Account), selezionare il nome dell'account da configurare.
3. In Settings (Impostazioni), scegliere Meetings (Riunioni).
4. In Policies (Policy), selezionare o deselezionare le opzioni dei criteri account che si desidera consentire o interrompere l'autorizzazione.
5. Scegliere Change (Cambia).

Per ulteriori informazioni, consulta Gestione delle impostazioni della riunione.

Fase 3: aggiunta di utenti all'account

Dopo aver creato il tuo account Amazon Chime Team, invita te stesso e i tuoi utenti a partecipare. Se esegui l'upgrade dell'account a un account aziendale, non è necessario invitare gli utenti. Al contrario, effettua l'upgrade a un account aziendale e richiedi il tuo dominio. Per ulteriori informazioni, consulta Fase 2 (facoltativo): configurazione delle impostazioni dell'account.

Per aggiungere utenti all'account Amazon Chime Chime

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Accounts (Account), selezionare il nome dell'account.
3. Nella pagina Users (Utenti), scegli Invite users (Invita utenti).
4. Inserire gli indirizzi e-mail degli utenti da invitare, tra cui sé stessi, e scegliere Invite users (Invita utenti).

Gli utenti invitati ricevono inviti via e-mail per unirsi all'account Amazon Chime Team che hai creato. Quando registrano i propri account utente Amazon Chime, ricevono le autorizzazioni Pro per impostazione predefinita e il periodo di prova di 30 giorni termina. Se hanno già creato un account utente Amazon Chime con il proprio indirizzo e-mail di lavoro, possono continuare a utilizzare tale account. Possono anche scaricare l'app client Amazon Chime in qualsiasi momento scegliendo Scarica Amazon Chime e accedendo al proprio account utente.

Si paga solo per un utente con le autorizzazioni Pro quando ospitano una riunione. Non vi è alcun costo per gli utenti con le autorizzazioni di base. Gli utenti di base non sono in grado di ospitare riunioni, ma possono partecipare alle riunioni e utilizzare la chat. Per ulteriori informazioni sui prezzi e sulle funzionalità a cui possono accedere gli utenti con autorizzazioni Pro e Basic, vedi Piani e prezzi.

Per modificare le autorizzazioni utente

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Accounts (Account), selezionare il nome dell'account.
3. Nella pagina Users (Utenti), selezionare l'utente o gli utenti per cui modificare le autorizzazioni.
4. Scegliere User actions (Azioni utente), Assign user permission (Assegna autorizzazione utente).
5. Per Permissions (Autorizzazioni), selezionare Pro o Basic (Di base).
6. Scegliere Assign (Assegna).

Puoi fornire ad altri utenti le autorizzazioni di amministratore e controllare il loro accesso alla console Amazon Chime per il tuo account. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon Chime.

(Facoltativo) Configurazione dei numeri di telefono per l'account Amazon Chime Chime Chime

Le seguenti opzioni telefoniche sono disponibili per gli account amministrativi di Amazon Chime:

Call Amazon Chime Chime Chime Chime

Consente agli utenti di inviare e ricevere telefonate e messaggi di testo direttamente da Amazon Chime. Inserisci i tuoi numeri di telefono nella console o inserisci i numeri di telefono esistenti di Amazon Chime. Assegna i numeri di telefono ai tuoi utenti Amazon Chime e concedi loro le autorizzazioni per inviare e ricevere telefonate e messaggi di testo utilizzando Amazon Chime. Per ulteriori informazioni, consultare Gestione dei numeri di telefono in Amazon Chime e Trasferimento di numeri di telefono esistenti.

Connettore Amazon Chime K K K K

Fornisce un servizio di trunking SIP per un sistema telefonico esistente. Inserisci i numeri di telefono esistenti o fornisci nuovi numeri di telefono nella console Amazon Chime. Per ulteriori informazioni, consulta Managing Amazon Chime Voice Connectors nella Amazon Chime SDK Administration Guide.

Gestione degli account Amazon Chime

Puoi usare Amazon Chime come singolo utente o come gruppo senza amministratori. Ma se desideri aggiungere funzionalità di amministratore o acquistare Amazon Chime Pro, devi creare un account Amazon Chime in. AWS Management Console Per informazioni su come creare un account amministratore Amazon Chime o per ulteriori informazioni sull'acquisto di Amazon Chime Pro, consulta. Nozioni di base

Per ulteriori informazioni sui diversi tipi di account amministratore di Amazon Chime, consulta. Scelta tra un account Amazon Chime Team o un account Enterprise Per ulteriori informazioni sulla gestione di un account amministratore esistente, consulta i seguenti argomenti.

Argomenti

Scelta tra un account Amazon Chime Team o un account Enterprise

Quando crei un account amministratore Amazon Chime, scegli se creare un account Team o un account Enterprise. Per ulteriori informazioni sulla creazione di un account amministratore Amazon Chime, consulta. Nozioni di base

Account del team

Con un account Team, puoi invitare utenti e concedere loro le autorizzazioni Amazon Chime Pro senza richiedere un dominio e-mail. Per ulteriori informazioni sulle autorizzazioni Pro e Basic, consulta Piani e prezzi.

Puoi invitare utenti da qualsiasi dominio di posta elettronica che non sia stato rivendicato da un'altra organizzazione. Paghi per gli utenti solo quando ospitano delle riunioni. Gli utenti del tuo account Team possono utilizzare l'app Amazon Chime per cercare e contattare altri utenti Amazon Chime registrati sullo stesso account. Ti consigliamo anche un account Team per pagare gli utenti Pro esterni alla tua organizzazione.

Account aziendale

Con un account Enterprise, hai un maggiore controllo sugli utenti dei domini della tua organizzazione. Puoi scegliere di connetterti al tuo provider di identità o Okta SSO per autenticare e assegnare le autorizzazioni Pro o Basic. Amazon Chime supporta anche Microsoft Active Directory.

Per creare un account Enterprise, devi richiedere almeno un dominio e-mail. Ciò garantisce che tutti gli utenti che accedono ad Amazon Chime utilizzando i domini dichiarati siano inclusi nel tuo account Amazon Chime gestito centralmente. Gli account aziendali sono necessari per gestire gli utenti tramite un'integrazione di directory supportata. Per ulteriori informazioni, consulta Dichiarazione di un dominio e Connessione ad Active Directory.

Puoi anche gestire l'attivazione e la sospensione degli utenti dal tuo account Enterprise. Per ulteriori informazioni, consulta Gestione delle autorizzazioni e degli accessi degli utenti.

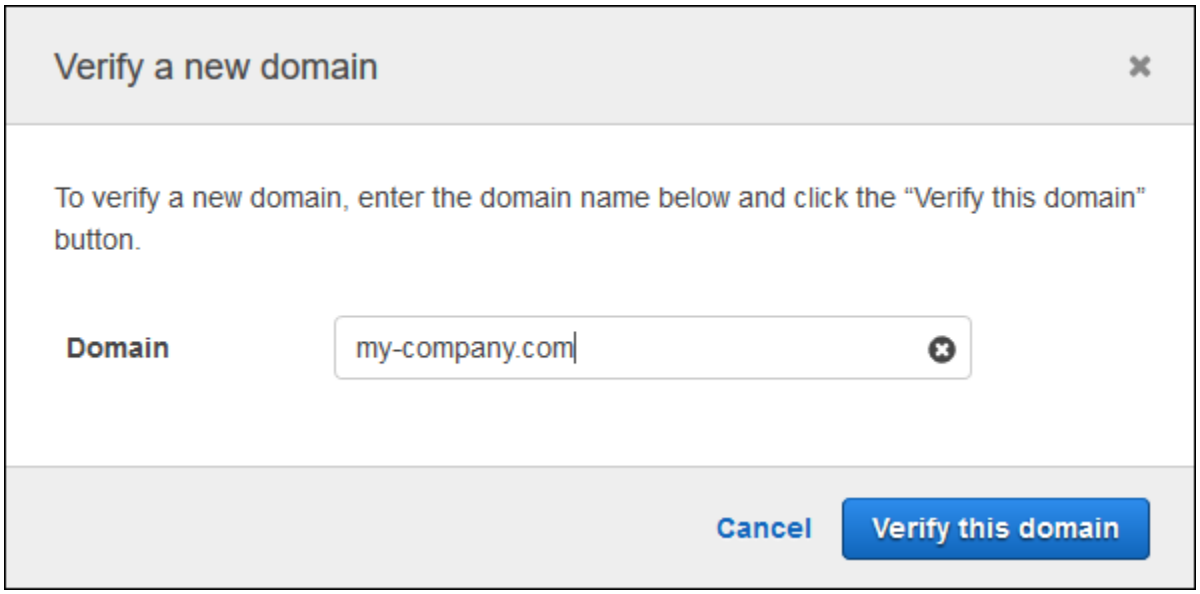
Dichiarazione di un dominio

Per creare un account aziendale e trarre vantaggio dal controllo più esteso offerto all'account e agli utenti, devi dichiarare almeno un dominio e-mail.

Per dichiarare un dominio

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Account, seleziona il nome dell'account di team.
3. Nel riquadro di navigazione, scegli Identity (Identità), Domains (Domini).
4. Nella pagina Domains (Domini), scegli Claim a new domain (Dichiara un nuovo dominio).

5. Per Domain (Dominio), digitare il dominio utilizzato dalla tua organizzazione per gli indirizzi e-mail. Scegli Verify This Domain (Verifica questo dominio).



6. Segui le istruzioni sullo schermo per aggiungere un record TXT al server DNS per il tuo dominio. In generale, il processo prevede l'accesso all'account del dominio, la ricerca dei record DNS per il dominio e l'aggiunta di un record TXT con il nome e il valore forniti da Amazon Chime. Per ulteriori informazioni su come aggiornare i record DNS relativi al tuo dominio, consulta la documentazione relativa al tuo provider DNS o registrar di nomi di dominio.

   Amazon Chime verifica l'esistenza di questo record per verificare che il dominio sia di tua proprietà. Una volta verificato il dominio, il relativo stato cambia da Pending verification (In attesa di verifica) a Verified (Verificato).

   > **Note**
   >
   > La propagazione della modifica e della verifica del DNS da parte di Amazon Chime può richiedere fino a 24 ore.

7. Se la tua organizzazione utilizza domini aggiuntivi o sottodomini per gli indirizzi e-mail, ripeti questa procedura per ogni dominio.

Per ulteriori informazioni sulla risoluzione dei problemi di attestazione di dominio, consulta Why isn't my domain claim request getting verified?.

La conversione di un account Team in un account Enterprise

Per convertire un account Team esistente in un account Enterprise, richiedi uno o più domini e-mail nella console Amazon Chime. Per ulteriori informazioni sulle differenze tra gli account Team ed Enterprise, consulta. Scelta tra un account Amazon Chime Team o un account Enterprise Per ulteriori informazioni sulla rivendicazione di un dominio, consultaDichiarazione di un dominio.

Per convertire un account Team in un account Enterprise

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per Account, scegliere il nome dell'account.
3. Per Identity (Identità), scegliere Getting Started (Nozioni di base).
4. Attenersi alla procedura indicata nella console per rivendicare il dominio.
5. (Facoltativo) Attenersi alla procedura descritta nella console per configurare il provider di identità e configurare il gruppo di directory.

Dopo che il tuo account è stato convertito in un account Enterprise, puoi decidere se connettere un'istanza di Active Directory tramite AWS Directory Service. La connessione a un'istanza di Active Directory consente agli utenti di accedere ad Amazon Chime utilizzando le proprie credenziali Active Directory. Per ulteriori informazioni, consulta Connessione ad Active Directory.

Se non ti connetti a un'istanza di Active Directory, i tuoi utenti possono continuare ad accedere ad Amazon Chime utilizzando Login with Amazon (LWA) o le credenziali del loro account Amazon.com.

Ridenominazione dell'account

I passaggi seguenti spiegano come rinominare il team di Amazon Chime e gli account aziendali che amministri. Il nome scelto viene visualizzato nelle e-mail che invitano gli utenti a iscriversi ad Amazon Chime.

Per rinominare il tuo account

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.

   La pagina Account viene visualizzata per impostazione predefinita.
2. Nella colonna Nome account, seleziona l'account che desideri rinominare.
3. Nel riquadro a sinistra, in Impostazioni, scegli Account.

Viene visualizzata la pagina di riepilogo dell'account.

4. Apri l'elenco delle azioni dell'account e scegli Rinomina account.

   Viene visualizzata la finestra di dialogo Rinomina account.

5. Inserisci il nuovo nome dell'account e scegli Salva.

Eliminazione dell'account

Se elimini il tuo AWS account in AWS Management Console, i tuoi account Amazon Chime vengono eliminati automaticamente. In alternativa, puoi utilizzare la console Amazon Chime per eliminare un account Amazon Chime Team o Enterprise.

> **Note**
>
> Gli utenti che non sono gestiti su un account Team o Enterprise possono richiedere l'eliminazione utilizzando il comando «Delete me» di Amazon Chime Assistant. Per ulteriori informazioni, consulta Uso di Amazon Chime Assistant.

Per eliminare un account di team

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Seleziona l'account nella colonna Account name (Nome account) e seleziona Account in Settings (Impostazioni).
3. Nel riquadro di navigazione, viene visualizzata la pagina Users (Utenti).
4. Seleziona gli utenti e scegli User actions (Operazioni utente), Remove user (Rimuovi utente).
5. Nel riquadro di navigazione, scegli Accounts (Account), Account actions (Operazioni account) ed Delete account (Elimina account).
6. Conferma che desideri eliminare l'account.

Amazon Chime elimina tutti i dati utente quando elimini il tuo account. Ciò include la chiusura di un AWS account, di singoli account Amazon Chime o di utenti Amazon Chime non gestiti. Sono esclusi i dati non di contenuto relativi agli account utente e all'utilizzo di Amazon Chime (attributi del servizio coperti dal Contratto con il cliente) generati da Amazon Chime.

Per eliminare un account aziendale

1. Rimozione dei domini.

   > **Note**
   >
   > Quando rimuovi un dominio, accade quanto segue:
   >
   > - Gli utenti associati al dominio vengono immediatamente disconnessi da tutti i dispositivi e perdono l'accesso a tutti i contatti, alle conversazioni in chat e alle chat room.
   > - Le riunioni pianificate dagli utenti del dominio non hanno più luogo.
   > - Gli utenti sospesi continuano ad apparire con lo stato Suspended (Sospeso) nelle pagine Users (Utenti) e User detail (Dettagli utente) e non possono accedere ai propri dati. Non possono creare nuovi account Amazon Chime con il loro indirizzo e-mail.
   > - Gli utenti registrati compaiono come Released (Rilasciati) nelle pagine Users (Utenti) e User detail (Dettagli utente) e non possono accedere ai propri dati. Possono creare un nuovo account Amazon Chime con il loro indirizzo e-mail.
   > - Se disponi di un account Active Directory e rimuovi un dominio associato all'indirizzo e-mail principale di un utente, l'utente non può accedere ad Amazon Chime e il suo profilo viene eliminato. Se rimuovi un dominio associato all'indirizzo e-mail secondario di un utente, quest'ultimo non può accedere con quell'indirizzo e-mail, ma conserva l'accesso ai propri contatti e dati Amazon Chime.
   > - Se disponi di un account Enterprise OpenID Connect (OIDC) e rimuovi un dominio associato all'indirizzo e-mail principale di un utente, l'utente non può più accedere ad Amazon Chime e il suo profilo viene eliminato.

2. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
3. Nella pagina Account, seleziona il nome dell'account di team.
4. Nel riquadro di navigazione, seleziona Settings (Impostazioni), Domains (Domini).
5. Nella pagina Domains (Domini), scegli Remove domain (Rimuovi dominio).
6. Nel riquadro di navigazione, scegli Accounts (Account), Account actions (Operazioni account) ed Delete account (Elimina account).
7. Conferma che desideri eliminare l'account.

Amazon Chime elimina tutti i dati utente quando elimini il tuo account. Ciò include la chiusura di un AWS account, di singoli account Amazon Chime o di utenti Amazon Chime non gestiti. Sono esclusi i dati non di contenuto relativi agli account utente e all'utilizzo di Amazon Chime (attributi del servizio coperti dal Contratto con il cliente) generati da Amazon Chime.

Gestione delle impostazioni della riunione

Gestisci le impostazioni delle riunioni dalla console Amazon Chime.

Impostazioni delle policy della riunione

Gestisci le politiche dell'account nella console Amazon Chime in Impostazioni, Riunioni. Sceglie tra le seguenti opzioni delle policy.

Abilita il controllo condiviso nella condivisione dello schermo

> Sceglie se gli utenti dell'organizzazione possono concedere il controllo condiviso dei computer durante le riunioni. I partecipanti che richiedono il controllo condiviso del computer del tuo utente ricevono un messaggio di errore che indica che il controllo remoto non è disponibile.

Abilita le chiamate in uscita per la partecipazione alle riunioni

> Attiva la funzione Amazon Chime call me. Offre ai partecipanti alla riunione la possibilità di partecipare alle riunioni ricevendo una telefonata da Amazon Chime.

Impostazioni applicazione riunione

Gestisci l'accesso alle applicazioni di riunione in Impostazioni, Riunioni nella console Amazon Chime. Puoi scegliere le seguenti opzioni:

Consenti agli utenti di accedere ad Amazon Chime utilizzando l'app Amazon Chime Meetings per Slack

> Questa opzione consente agli utenti della tua organizzazione di accedere ad Amazon Chime dall'app Amazon Chime Meetings per Slack. Per ulteriori informazioni, consulta Configurazione dell'app Amazon Chime Meetings per Slack.

Impostazioni regione riunione

Per migliorare la qualità delle riunioni e ridurre la latenza, Amazon Chime elabora le riunioni nella regione AWS ottimale per tutti i partecipanti. Puoi scegliere se consentire ad Amazon Chime di selezionare la regione ottimale per una riunione tra tutte le regioni disponibili o utilizzare solo le regioni selezionate.

Puoi aggiornare questa impostazione dalle impostazioni Meetings (Riunioni) dell'account in qualsiasi momento. Dalle impostazioni Riunioni, puoi anche visualizzare la percentuale di riunioni Amazon Chime che vengono elaborate in ciascuna regione.

Per aggiornare le impostazioni della regione della riunione

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Accounts (Account), seleziona il nome del tuo account.
3. Nel riquadro di navigazione, seleziona Settings (Impostazioni), Meetings (Riunioni).
4. Per Regions (Regioni), scegli una delle seguenti opzioni:
   - Utilizza tutte le regioni disponibili per garantire la qualità delle riunioni: consente ad Amazon Chime di ottimizzare l'elaborazione delle riunioni per te.
   - Usa solo le regioni che ho selezionato: ti consente di selezionare le regioni dal menu a discesa.
5. Selezionare Salva.

Gestione delle policy di conservazione della chat

Se amministri uno o più account Amazon Chime Enterprise, puoi impostare politiche di conservazione delle chat per quanto segue:

- Conversazioni in chat che includono solo i membri del tuo account Enterprise.
- Chat room create dai membri del tuo account Enterprise.

Una politica di conservazione elimina automaticamente i messaggi in base al periodo di tempo impostato. Puoi impostare periodi di tempo che vanno da un giorno a 15 anni.

> **Note**
>
> Gli account Amazon Chime Enterprise hanno un periodo di conservazione di 90 giorni. La politica si applica alle conversazioni che coinvolgono utenti che appartengono all'account e agli utenti che non appartengono all'account.
> Le policy di conservazione non si applicano ai seguenti elementi:
>
> - Conversazioni in chat che non includono membri di account Amazon Chime Enterprise
> - Chat room create da utenti che non appartengono a un account Amazon Chime Enterprise

In che modo le politiche di conservazione influiscono sugli utenti di Amazon Chime

Le politiche di conservazione impostate dagli amministratori degli account Enterprise influiscono sugli utenti di Amazon Chime in modo diverso, a seconda che gli utenti facciano parte dello stesso account Enterprise, di un account Enterprise diverso, di un account Team o che gli utenti non siano membri di alcun account.

Conversazioni in chat dei membri dell'organizzazione

Nella tabella seguente viene illustrato in che modo le policy di conservazione influiscono sulle conversazioni in chat per i membri dell'account aziendale.

Se la conversazione in chat include...	La policy di conservazione è...
Solo altri membri dell'account aziendale dell'utente	Impostata dall'amministratore dell'utente
Chiunque all'esterno dell'account aziendale dell'utente	Impostata automaticamente su 90 giorni

Chat room per membri aziendali

Nella tabella seguente viene illustrato come le policy di conservazione influiscono sulle chat room per membri dell'account aziendale.

Se la chat room viene creata da...	La policy di conservazione è...
Un membro dell'account aziendale dell'utente	Impostata dall'amministratore dell'utente
Un altro membro dell'account aziendale	Impostata dall'amministratore dell'altro account
Un membro di un account non aziendale	Non applicabile

Conversazioni in chat dei membri del team

Nella tabella seguente viene illustrato in che modo le policy di conservazione influiscono sulle conversazioni in chat per i membri dell'account di team.

Se la conversazione in chat include...	La policy di conservazione è...
Solo gli utenti che non sono membri di un account aziendale	Non applicabile
Almeno un membro di un account aziendale	Impostata automaticamente su 90 giorni

Chat room dei membri del team

Nella tabella seguente viene illustrato come le policy di conservazione influiscono sulle chat room per membri dell'account di team.

Se la chat room viene creata da...	La policy di conservazione è...
Un utente dell'account di team	Non applicabile
Chiunque non sia membro di un account aziendale	Non applicabile
Un membro di un account aziendale	Impostata dall'amministratore dell'account aziendale

Gli utenti di Amazon Chime che non sono membri di un account Enterprise o Team sono soggetti solo alle politiche di conservazione delle chat room nelle chat room create da un membro di un account Enterprise.

Conversazioni in chat con destinatari che non appartengono a un account aziendale o di team

La tabella seguente mostra come le politiche di conservazione influiscono sulle conversazioni in chat per gli utenti che non sono membri di un account Amazon Chime Enterprise o Team.

Se la conversazione in chat include...	La policy di conservazione è...
Solo gli utenti che non sono membri di un account aziendale	Non applicabile
Almeno un membro di un account aziendale	Impostata automaticamente su 90 giorni

Chat room create da utenti che non appartengono a un account aziendale o di team

La tabella seguente mostra come le politiche di conservazione influiscono sulle chat room per gli utenti che non sono membri di un account Amazon Chime Enterprise o Team.

Se la chat room viene creata da...	La policy di conservazione è...
Un utente che non è membro di un account aziendale o di team	Non applicabile
Un utente dell'account di team	Non applicabile
Un membro di un account aziendale	Impostata dall'amministratore dell'account aziendale

Attivazione della conservazione delle chat

Gli amministratori degli account Amazon Chime Enterprise possono utilizzare la console Amazon Chime per attivare la conservazione delle chat per le conversazioni e le chat room del proprio account. È inoltre possibile utilizzare la console per aggiornare i periodi di conservazione delle chat o disattivare la conservazione delle chat in qualsiasi momento.

Per attivare la conservazione delle chat

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Account, selezionare il nome dell'account.
3. Nel pannello di navigazione, in Impostazioni, scegli Conservazione.
4. Nella pagina Conservazione, in Conservazione delle conversazioni in chat, sposta il cursore su Attivato.
5. In Periodo di conservazione, inserisci un numero nella prima casella, quindi apri l'elenco accanto alla casella e scegli Giorni, Settimane o Anni.
6. In Conservazione della chat room, ripeti i passaggi 4-5. Al termine, scegli Save (Salva).

Entro un giorno dall'impostazione del periodo di conservazione, gli utenti del tuo account perdono l'accesso ai messaggi inviati al di fuori del periodo di conservazione.

Ripristino dei messaggi di chat

> **Note**
>
> Devi essere un amministratore dell'account Amazon Chime Enterprise per completare questi passaggi.

Puoi ripristinare i messaggi di chat entro 30 giorni dall'impostazione di un periodo di conservazione della chat. Quando ripristini i messaggi di chat, ripristini tutti i messaggi inviati da tutti gli utenti del tuo account Amazon Chime.

Entro tale periodo di 30 giorni, puoi effettuare una delle seguenti operazioni per ripristinare i messaggi:

- Usa la console Amazon Chime per disattivare la conservazione dei dati.

  - OPPURE -

- Allunga il periodo di conservazione.

Dopo il periodo di prova di 30 giorni, tutti i messaggi di chat che rientrano nel periodo di conservazione vengono eliminati definitivamente. I nuovi messaggi di chat vengono eliminati definitivamente non appena superano il periodo di conservazione.

Per informazioni sull'impostazione o la modifica di un periodo di conservazioneAttivazione della conservazione delle chat, consulta la sezione precedente di questa sezione.

I messaggi di chat vengono inoltre eliminati definitivamente da Amazon Chime quando tu o un membro dell'account eseguite una delle seguenti azioni:

- Elimina una chat room di Amazon Chime. Per ulteriori informazioni sull'eliminazione delle chat room, consulta Eliminazione delle chat room, nella Guida per l'utente di Amazon Chime.
- Termina una riunione Amazon Chime in cui sono presenti messaggi di chat.

> **Note**
>
> Se necessario, puoi copiare e salvare manualmente i messaggi di chat da una riunione, ma devi farlo prima della fine della riunione. Per ulteriori informazioni, consulta Usare la chat durante le riunioni, nella Guida per l'utente di Amazon Chime.

Eliminazione dei messaggi di chat

Per rispettare le politiche di conservazione dei dati, Amazon Chime conserva tutti i messaggi di chat e impedisce agli utenti finali di eliminare i messaggi inviati. Tuttavia, gli amministratori di sistema di Amazon Chime possono utilizzare un paio di API per eliminare singoli messaggi dalle conversazioni e dalle chat room. I messaggi devono risiedere nell'account Amazon Chime dell'amministratore.

Gli utenti possono richiedere l'eliminazione dei messaggi inviandoti un ID del messaggio e l'ID della conversazione o della chat room corrispondente. L'argomento Uso delle funzionalità di chat, nella Guida per l'utente di Amazon Chime, spiega come.

Quando ricevi una richiesta di eliminazione, puoi scrivere codice o utilizzare la AWS CLI per richiamare le seguenti API.

Per rimuovere un messaggio

- Esegui una di queste operazioni:
  - Per i messaggi di conversazione: utilizza l'API. RedactConversationMessage

Nella CLI, esegui il seguente comando:

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

- Per i messaggi nelle chat room: utilizza l'RedactRoomMessageAPI.

  Nella CLI, esegui il seguente comando:

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

Connessione ad Active Directory

Quando colleghi il tuo account amministrativo Amazon Chime a un Active Directory, puoi beneficiare delle seguenti funzionalità:

- I tuoi utenti Amazon Chime possono accedere con le proprie credenziali Active Directory.
- In qualità di amministratore di Amazon Chime, puoi scegliere quali funzionalità di sicurezza delle credenziali aggiungere, tra cui rotazione delle password, regole di complessità delle password e autenticazione a più fattori.
- Quando rimuovi gli account utente da Active Directory, vengono rimossi anche i relativi account Amazon Chime.
- Puoi specificare quali gruppi Active Directory ricevono le autorizzazioni Amazon Chime Pro.
  - È possibile configurare più gruppi per la ricezione delle autorizzazioni Base o Pro.
  - Gli utenti devono appartenere a uno dei due gruppi per accedere ad Amazon Chime.
  - Gli utenti di entrambi i gruppi ricevono una licenza Pro.

Per ulteriori informazioni sulla gestione delle autorizzazioni degli utenti, consulta. Gestione delle autorizzazioni e degli accessi degli utenti

Prerequisiti

Prima di poterti connettere ad Active Directory in Amazon Chime, devi completare i seguenti prerequisiti:

- Assicurati di disporre delle AWS Identity and Access Management autorizzazioni corrette per configurare domini, active directory e gruppi di directory. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi per Amazon Chime.
- Crea una directory configurata nella regione Stati Uniti orientali (Virginia settentrionale). AWS Directory Service Per ulteriori informazioni, consulta la Guida di amministrazione di AWS Directory Service. Amazon Chime può connettersi tramite AD Connector, Microsoft AD o Simple AD.
- Richiedi un dominio per creare un account Amazon Chime Enterprise o convertire il tuo account Team esistente in un account Enterprise. Se i tuoi utenti hanno indirizzi e-mail di lavoro provenienti da più di un dominio, assicurati di rivendicare tutti quei domini. Per ulteriori informazioni, consulta Dichiarazione di un dominio e La conversione di un account Team in un account Enterprise.

Connessione ad Active Directory in Amazon Chime

Dopo aver collegato Active Directory ad Amazon Chime, agli utenti viene richiesto di accedere con le proprie credenziali di directory quando utilizzano un indirizzo e-mail di uno dei domini che hai dichiarato nel tuo account Amazon Chime Enterprise.

Per connetterti al tuo Active Directory in Amazon Chime

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel riquadro di navigazione, per Identity, scegli Active directory.
3. Per Cloud directory ID, seleziona la AWS Directory Service directory da utilizzare per Amazon Chime, quindi scegli Connect.

   > **Note**
   >
   > Puoi individuare il tuo ID directory tramite la console AWS Directory Service.

4. Dopo la connessione della directory, scegli Aggiungi un nuovo gruppo.
5. Per Gruppo, inserisci il nome del gruppo. Il nome deve corrispondere esattamente un gruppo di Active Directory nella directory di destinazione. Le Active Directory Organization Unit (OU) non sono supportate.
6. Per Autorizzazioni, scegli Basic o Pro.
7. Scegliere Add Group (Aggiungi gruppo).
8. (Facoltativo) Ripetete questa procedura per creare gruppi di directory aggiuntivi.

Configurazione di più indirizzi e-mail

Dopo la connessione ad Active Directory in Amazon Chime, gli utenti possono accedere ad Amazon Chime utilizzando le proprie credenziali Active Directory. Ai tuoi utenti possono essere assegnati più indirizzi e-mail in Active Directory. Per consentire ai tuoi utenti di accedere ad Amazon Chime utilizzando le loro credenziali Active Directory, devi richiedere ogni dominio e-mail applicabile nel tuo account amministrativo Amazon Chime. Per ulteriori informazioni, consulta Dichiarazione di un dominio.

> **Note**
>
> Se i tuoi utenti tentano di accedere utilizzando un indirizzo e-mail di un dominio non registrato, viene richiesto loro di accedere utilizzando Accedi con Amazon. Non sono in grado di accedere al tuo account amministrativo quando utilizzano un indirizzo e-mail proveniente da un dominio non registrato.

Quando visualizza i dettagli dell'utente nella console Amazon Chime, Amazon Chime utilizza il singolo indirizzo e-mail nell'`EmailAddress`attributo di Active Directory come indirizzo e-mail principale di ogni utente. Questo è l'unico indirizzo e-mail che puoi visualizzare per l'utente nella console Amazon Chime. Tuttavia, gli utenti possono accedere con qualsiasi indirizzo aggiuntivo elencato nell'`ProxyAddress`attributo, purché rivendichi tali domini nel tuo account Amazon Chime.

Esempio di configurazione errata

Un utente con il nome utente shirley.rodriguez è membro di un account Amazon Chime che ha rivendicato due domini: example.com ed example.org. In Active Directory, questo utente ha i seguenti tre indirizzi e-mail:

- Indirizzo e-mail principale: shirley.rodriguez@esempio.com
- Indirizzo e-mail proxy 1: shirley.rodriguez@esempio2.com
- Indirizzo e-mail proxy 2: srodriguez@example.org

Questo utente può accedere ad Amazon Chime utilizzando shirley.rodriguez@example.com o srodriguez@example.org e shirley.rodriguez. Se tentano di accedere utilizzando shirley.rodriguez@example2.com, gli viene chiesto di accedere con Amazon e non fanno parte del tuo account gestito. Ecco perché è importante rivendicare tutti i domini e-mail dei tuoi utenti.

Altri utenti di Amazon Chime possono aggiungere questo utente come contatto, invitarlo alle riunioni o aggiungerlo come delegato utilizzando l'indirizzo e-mail shirley.rodriguez@example.com o srodriguez@example.org.

Esempio di configurazione corretta

Un utente con il nome utente shirley.rodriguez è membro di un account Amazon Chime che ha rivendicato tre domini: example.com, example2.com ed example.org. In Active Directory, questo utente ha i seguenti tre indirizzi e-mail:

- Indirizzo e-mail principale: shirley.rodriguez@esempio.com
- Indirizzo e-mail proxy 1: shirley.rodriguez@esempio2.com
- Indirizzo e-mail proxy 2: srodriguez@example.org

Questo utente può accedere ad Amazon Chime utilizzando uno qualsiasi dei propri indirizzi e-mail di lavoro. Altri utenti possono anche aggiungerlo come contatto, invitarlo alle riunioni o aggiungerlo come delegato utilizzando uno dei loro indirizzi e-mail di lavoro.

Connessione al servizio SSO di Okta

Se disponi di un account aziendale, puoi connetterti al servizio SSO di Okta per autenticare e assegnare le autorizzazioni utente.

> **Note**
>
> Se devi creare un account aziendale, che consente di gestire tutti gli utenti all'interno di un determinato set di domini di indirizzi e-mail, consulta Dichiarazione di un dominio.

La connessione di Amazon Chime a Okta richiede la configurazione di due applicazioni nella Console di amministrazione Okta. La prima applicazione è configurata manualmente e utilizza OpenID Connect per autenticare gli utenti al servizio Amazon Chime. La seconda applicazione è disponibile come Amazon Chime SCIM Provisioning nell'Okta Integration Network (OIN). È configurato per inviare aggiornamenti ad Amazon Chime sulle modifiche a utenti e gruppi.

Per connettersi al servizio SSO di Okta

1. Crea l'applicazione Amazon Chime (OpenID Connect) nella console di amministrazione Okta:

1. Accedi a Okta Administration Dashboard (Pannello di controllo di amministrazione Okta), quindi scegli Add Application (Aggiungi applicazione). Nella finestra di dialogo Create New Application (Crea nuova applicazione), scegli Web, Next (Avanti).
2. Configura le Application Settings (Impostazioni applicazione):
   a. Denomina l'applicazione **`Amazon Chime`**.
   b. Per Login Redirect URI (URI di reindirizzamento di accesso), inserisci il seguente valore: **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
   c. Nella sezione Allowed Grant Types (Tipi di concessione consentiti), seleziona tutte le opzioni per abilitarle.
   d. Nel menu a discesa Login initiated by (Accesso avviato da), scegli Either (Okta or App) (Una delle due opzioni(Okta o app)) e seleziona tutte le opzioni correlate.
   e. Per Initiate Login URI (Avvia URI di accesso), inserisci il seguente valore: **`https://signin.id.ue1.app.chime.aws/auth/okta`**
   f. Selezionare Salva.
   g. Mantieni aperta questa pagina perché, per la fase 2, sarà necessario disporre delle informazioni relative a Client ID (ID client), Client secret (Segreto client) e Issuer URI (URI approvatore).

2. Nella console Amazon Chime, segui questi passaggi:
   1. Nella parte superiore della pagina Okta single-sign on configuration (Configurazione Single Sign-On Okta), scegli Set up incoming keys (Imposta chiavi in entrata).
   2. Nella finestra di dialogo Setup Setup incoming Okta keys (Imposta chiavi Okta in entrata):
      a. Incolla le informazioni relative a Client ID (ID client) e Client secret (Segreto client) dalla pagina Okta Application Settings (Impostazioni applicazione Okta).
      b. Incolla le informazioni relative a Issuer URI (URI approvatore) dalla pagina Okta API (API Okta). L'URI dell'emittente deve essere un dominio Okta, ad esempio `https://example.okta.com`.
3. Configura l'applicazione Amazon Chime SCIM Provisioning nella console di amministrazione Okta per lo scambio di determinate informazioni sull'identità e sull'appartenenza a gruppi con Amazon Chime:
   1. Nella console di amministrazione Okta, scegli Applicazioni, Aggiungi applicazione, cerca Amazon Chime SCIM Provisioning e aggiungi l'applicazione.

> **Important**
>
> Durante la configurazione iniziale, scegli sia Do not display application to users (Non mostrare l'applicazione agli utenti) sia Do not display application icon in the Okta Mobile App (Non mostrare l'icona dell'applicazione nell'app per dispositivi mobili Okta), quindi scegli Done (Fatto).

2. Nella scheda Provisioning, scegli Configure API Integration (Configura integrazione API), quindi seleziona Enable API Integration (Abilita integrazione API). Mantieni aperta questa pagina perché, per la fase successiva, dovrai copiare una chiave di accesso API in tale pagina.
3. Nella console Amazon Chime, scegli Crea chiave di accesso per creare una chiave di accesso API. Copia tale chiave nel campo Okta API Token (Token API Okta) nella finestra di dialogo Configure API Integration (Configura integrazione API), scegli Test the Integration (Verifica l'integrazione), quindi Save (Salva).
4. Configura le azioni e gli attributi che Okta utilizzerà per aggiornare Amazon Chime. Nella scheda Provisioning, sotto la sezione To App (All'app), seleziona Edit (Modifica), scegli tra Enable Users (Abilita utenti), Update User Attributes (Aggiorna attributi utente) e Deactivate Users (Disattiva utenti), quindi seleziona Save (Salva).
5. Nella scheda Assignments (Assegnazioni), concedi agli utenti le autorizzazioni per la nuova app SCIM.

> **Important**
>
> Ti consigliamo di concedere le autorizzazioni tramite un gruppo che contiene tutti gli utenti che devono avere accesso ad Amazon Chime, indipendentemente dalla licenza. Il gruppo deve essere lo stesso utilizzato per assegnare l'applicazione OIDC rivolta agli utenti nella fase 1 riportata in precedenza. In caso contrario, gli utenti finali non saranno in grado di accedere.

6. Nella scheda Push Groups, configura quali gruppi e iscrizioni vengono sincronizzati con Amazon Chime. Questi gruppi sono utilizzati per distinguere tra utenti Base e Pro.

4. Configura i gruppi di directory in Amazon Chime:

1. Nella console Amazon Chime, vai alla pagina di configurazione Single Sign-On di Okta.
2. In Directory groups (Gruppi di directory), scegli Add new groups (Aggiungi nuovi gruppi).

3. Inserisci il nome di un gruppo di directory da aggiungere ad Amazon Chime. Il nome deve essere una corrispondenza esatta di uno dei gruppi in Push Groups (Esegui push dei gruppi) configurati in precedenza nella fase 3-f.
4. Scegli se gli utenti di questo gruppo devono ricevere funzionalità Basic (Base) o Pro, quindi seleziona Save (Salva). Ripeti questa procedura per configurare gruppi aggiuntivi.

> **Note**
>
> Se ricevi un messaggio di errore che indica che il gruppo non è stato trovato, è possibile che i due sistemi non abbiano completato la sincronizzazione. Attendi alcuni minuti, quindi scegli di nuovo Add new groups (Aggiungi nuovi gruppi).

La scelta delle funzionalità Basic o Pro per gli utenti del tuo gruppo di directory influisce sulla licenza, sulle funzionalità e sul costo di tali utenti nel tuo account Amazon Chime Enterprise. Per ulteriori informazioni, consulta la sezione Prezzi di .

Distribuzione del componente aggiuntivo Amazon Chime per Outlook

Amazon Chime offre due componenti aggiuntivi per Microsoft Outlook: il componente aggiuntivo Amazon Chime per Outlook su Windows e il componente aggiuntivo Amazon Chime per Outlook. Questi componenti aggiuntivi offrono le stesse caratteristiche di programmazione, ma supportano tipi di utenti diversi. Gli abbonati a Microsoft Office 365 e le organizzazioni che utilizzano Microsoft Exchange 2013 o versioni successive locali possono utilizzare il componente aggiuntivo Amazon Chime per Outlook. Gli utenti Windows con un server Exchange locale che esegue Exchange Server 2010 o versioni precedenti e gli utenti di Outlook 2010 devono utilizzare il componente aggiuntivo Amazon Chime per Outlook su Windows.

Gli utenti Windows che non dispongono delle autorizzazioni per installare il componente aggiuntivo Amazon Chime per Outlook devono optare per il componente aggiuntivo Amazon Chime per Outlook su Windows.

Per ulteriori informazioni sul componente aggiuntivo adatto per l'utente e l'organizzazione, consulta Choosing the Right Outlook Add-In.

Se scegli il componente aggiuntivo Amazon Chime per Outlook per la tua organizzazione, puoi distribuirlo ai tuoi utenti con una distribuzione centralizzata. Per ulteriori informazioni, consulta la Guida all'installazione del componente aggiuntivo Amazon Chime per Outlook per amministratori.

Configurazione dell'app Amazon Chime Meetings per Slack

Se utilizzi Slack Enterprise Grid Organizations e possiedi o amministri un'organizzazione Slack, puoi configurare l'app Amazon Chime Meetings per Slack per le tue organizzazioni. Se sei un amministratore dell'area di lavoro Slack, puoi configurare l'app Amazon Chime Meetings per Slack per le tue aree di lavoro.

I passaggi nelle sezioni seguenti spiegano come eseguire entrambi i tipi di configurazioni e come completare attività aggiuntive come la migrazione di uno spazio di lavoro in un'organizzazione.

Argomenti

Installazione dell'app Amazon Chime Meetings per Slack in un'organizzazione

L'installazione dell'app Amazon Chime Meetings per Slack su un'organizzazione Slack consente agli utenti di avviare riunioni e chiamate istantanee con altri utenti nei vari spazi di lavoro dell'organizzazione. Consente inoltre agli amministratori dell'area di lavoro di installare automaticamente l'applicazione per riunioni Amazon Chime Meetings App per Slack su qualsiasi nuova area di lavoro. I passaggi seguenti spiegano come.

> **Note**
>
> I passaggi seguenti presuppongono che tu sia il proprietario o l'amministratore dell'organizzazione e che tu possa accedere alla console di gestione di Slack.

Per configurare l'app Amazon Chime Meetings per Slack in un'organizzazione

1. Nel riquadro a sinistra della console di gestione Slack, scegli App.

   Viene visualizzata la pagina App che elenca le app installate dall'organizzazione, se presenti.
2. Scegli Gestisci app, che si trova nell'angolo in alto a destra della pagina, quindi scegli Installa un'app.

   Viene visualizzata la finestra di dialogo Trova un'app da installare.
3. Continua la ricerca**`Amazon Chime Meetings`**, quindi selezionala nei risultati della ricerca.

   Viene visualizzata la finestra di dialogo Aggiungi Amazon Chime Meetings agli spazi di lavoro in cui sono elencate le aree di lavoro dell'organizzazione.
4. Scegli l'area o le aree di lavoro su cui installare l'app Amazon Chime Meetings per Slack.
5. Facoltativamente, scegli Predefinito per le aree di lavoro future se desideri installare automaticamente l'app Amazon Chime Meetings per Slack in tutte le nuove aree di lavoro, quindi scegli Avanti.

   Viene visualizzata la finestra di dialogo Rivedi le autorizzazioni richieste di questa app che mostra le autorizzazioni e le azioni per l'app Amazon Chime Meetings per Slack.
6. Seleziona Successivo.
7. Se hai scelto di installare l'app Amazon Chime Meetings per Slack su nuove aree di lavoro per impostazione predefinita, scegli Sono pronto a impostare questa app come predefinita per le aree di lavoro future, quindi scegli Salva. Altrimenti, scegli Salva.

> **Note**
>
> Puoi anche usare OAuth per installare app nelle tue organizzazioni. Per maggiori informazioni, consulta Installazione con OAuth nella guida di Slack.

Installazione dell'app Amazon Chime Meetings per Slack negli spazi di lavoro

L'installazione dell'app Amazon Chime Meetings per Slack su un'area di lavoro consente agli utenti di avviare riunioni e chiamate istantanee con altri utenti in quell'area di lavoro. Gli utenti non hanno bisogno di un profilo utente Amazon Chime per utilizzare l'app Amazon Chime Meetings per Slack.

Possono accedere con i propri profili utente Slack e avviare chiamate o riunioni in qualsiasi momento. Se gli utenti devono tenere riunioni con più di un'altra persona, devi configurare un account Amazon Chime Team e concedere a tali utenti aggiuntivi le autorizzazioni Pro. Per ulteriori informazioni sull'avvio di chiamate e riunioni Amazon Chime, consulta Uso dell'app Amazon Chime Meetings per Slack nella Guida per l'utente di Amazon Chime. Per ulteriori informazioni sulla configurazione di un account Amazon Chime Team, consulta questa Associazione delle aree di lavoro agli account del team Amazon Chime guida.

Per installare l'app Amazon Chime Meetings per Slack per aree di lavoro Slack

1. Vai alla Slack App Directory e individua l'app Amazon Chime Meetings.
2. Scegli Aggiungi a Slack per installare l'app Amazon Chime Meetings per Slack dalla directory delle app di Slack.
3. Configura l'impostazione Chiamate dell'area di lavoro Slack su Abilita le chiamate in Slack, utilizzando Amazon Chime.

Migrazione degli spazi di lavoro verso le organizzazioni

Se possiedi un'organizzazione Slack, puoi migrare gli spazi di lavoro in quell'organizzazione. Per ulteriori informazioni sulla migrazione delle aree di lavoro, consulta Migrare le aree di lavoro a Enterprise Grid nella guida di Slack.

Associazione delle aree di lavoro agli account del team Amazon Chime

Associa il tuo spazio di lavoro a un account Amazon Chime Team per gestire le autorizzazioni degli utenti. Puoi aggiornare gli organizzatori delle riunioni ad Amazon Chime Pro in modo che possano avviare riunioni con un massimo di 250 partecipanti e 25 riquadri video e includere numeri di telefono a cui chiamare per l'audio. Assegna agli utenti le autorizzazioni Amazon Chime Basic in modo che possano one-on-one avviare riunioni o partecipare a riunioni Amazon Chime. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon Chime.

> **Note**
>
> Se associ un account Amazon Chime Team al tuo spazio di lavoro Slack, gli utenti possono accedere ad Amazon Chime dall'app Amazon Chime Meetings per Slack. Puoi modificare questa impostazione in qualsiasi momento. Per ulteriori informazioni, consulta Gestione delle impostazioni della riunione.

Prima di poter associare il tuo spazio di lavoro Slack a un account Amazon Chime Team, devi creare un account. AWS Per ulteriori informazioni su come creare un AWS account, consulta. Prerequisiti per gli amministratori di sistema Amazon Chime

Per associare il tuo spazio di lavoro Slack a un account Amazon Chime Team durante l'installazione dell'app Amazon Chime Meetings per Slack

1. Subito dopo aver installato l'app Amazon Chime Meetings per Slack nella tua area di lavoro Slack, scegli Aggiorna ora.
2. Segui le istruzioni per accedere alla console Amazon Chime utilizzando AWS le credenziali del tuo account.
3. Segui le istruzioni per creare un nuovo account Team in Amazon Chime o scegline uno esistente.
   - Crea un nuovo account: crea un nuovo account Amazon Chime a cui invitare i tuoi utenti Slack. Inserisci un nome account, scegli se invitare gli utenti Slack, quindi scegli Create (Crea).
   - Scegli un account esistente: seleziona un account Amazon Chime esistente a cui invitare i tuoi utenti Slack. Seleziona l'account, quindi scegli Invite (Invita).

Quando inviti i tuoi utenti Slack a iscriversi ad Amazon Chime, ricevono un invito via e-mail. Quando accettano l'invito, vengono automaticamente aggiornati ad Amazon Chime Pro.

Se non hai associato il tuo spazio di lavoro Slack a un account Amazon Chime Team quando hai installato l'app Amazon Chime Meetings per Slack, puoi farlo dopo l'installazione utilizzando i passaggi seguenti.

Per associare il tuo spazio di lavoro Slack a un account Amazon Chime Team dopo aver installato l'app Amazon Chime Meetings per Slack

1. Accedi al tuo account. AWS
2. Accedi all'area di lavoro Slack come amministratore.
3. Vai a https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Segui le istruzioni per creare un nuovo account Team in Amazon Chime o scegli un account esistente.
   - Crea un nuovo account: crea un nuovo account Amazon Chime a cui invitare i tuoi utenti Slack. Inserisci un nome account, scegli se invitare gli utenti Slack, quindi scegli Create (Crea).

- Scegli un account esistente: seleziona un account Amazon Chime esistente a cui invitare i tuoi utenti Slack. Seleziona l'account, quindi scegli Invite (Invita).

Gestione degli utenti

> **Note**
>
> I passaggi di questa sezione presuppongono che tu disponga di un set di indirizzi e-mail utente o che tu abbia collegato il tuo account amministratore ad Active Directory. Per ulteriori informazioni, consultaConnessione ad Active Directory, in questa guida.

Utilizzi la console Amazon Chime per aggiungere e gestire utenti. Aggiungi utenti invitandoli. Quando accettano i tuoi inviti, vengono visualizzati nella sezione Utenti, che elenca tutti gli utenti del tuo account e i relativi dettagli utente. Per ulteriori informazioni, consulta Visualizzazione dei dettagli dell'utente.

Gli amministratori di account che utilizzano Login with Amazon (LWA) vedono anche le opzioni per gestire i livelli di autorizzazione e rimuovere utenti da un account. Queste azioni sono gestite tramite Active Directory o Okta, a seconda di quale di queste si configura un account da utilizzare. Per ulteriori informazioni, consulta Gestione delle autorizzazioni e degli accessi degli utenti.

Indice

Aggiunta di utenti

Aggiungi utenti a un account Amazon Chime invitandoli a iscriversi all'account. Invii inviti a potenziali utenti dalla console Amazon Chime e questi passaggi spiegano come.

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.

Viene visualizzato un elenco degli account che amministri.

2. Scegli l'account a cui desideri aggiungere membri, quindi scegli Invita utenti.

   Viene visualizzata la finestra di dialogo Invita nuovi utenti.

3. Inserisci gli indirizzi e-mail degli utenti che desideri invitare. Separa ogni indirizzo con un punto e virgola (;).
4. Scegliere Invite users (Invita utenti).

I nuovi utenti vengono visualizzati nell'elenco. Quando inviti gli utenti a utilizzare un account Team, i loro dettagli non verranno visualizzati finché non accettano il tuo invito.

Visualizzazione dei dettagli dell'utente

Nella console Amazon Chime, in Utenti, puoi visualizzare un elenco di tutti gli utenti del tuo account e vedere i relativi dettagli utente. Cerca un utente specifico in base al suo indirizzo e-mail e scegli il suo nome per visualizzarne i dettagli. In Dettagli utente, puoi visualizzare informazioni dettagliate sull'utente e apportare aggiornamenti al suo account utente.

La tabella seguente elenca i dettagli dell'utente visualizzati nella console.

> **Note**
>
> I dettagli utente completi vengono visualizzati per gli utenti dell'account Team solo dopo aver accettato gli inviti.

Campo	Descrizione	Esempio
Display name (Nome visualizzato)	Il nome dell'utente visualizzato in Amazon Chime. Per gli utenti di Login with Amazon (LWA), questo è il nome completo. Per gli utenti di Active Directory, viene utilizzato DISPLAY_NAME_ATTRIBUTE.	Rossi, Maria

Campo	Descrizione	Esempio
Indirizzo e-mail	Per gli utenti LWA, l'indirizzo e-mail utilizzato per la registrazione. Per gli utenti di Active Directory, viene visualizzato l'indirizzo e-mail primario di Active Directory.	maria.rossi@esempio.com
Registration (Registrazione)	Lo stato di registrazione corrente dell'utente. I valori possibili sono diversi tra gli account aziendali, dove gli inviti non vengono inviati, e gli account di team, dove gli inviti vengono inviati.	Registrato, Non registrato per un account di team, oppure Sospeso per un account aziendale
Permission tier (Livello di autorizzazione)	Impostato su Pro per impostazione predefinita, per consentire agli utenti di ospitare riunioni. Può essere modificato in Basic (Base).	Pro, Basic (Base)
Invited (Invitato)	Per gli account di team, la data in cui l'utente è stato invitato nell'account.	01/05/2020
Joined (Collegato)	La data in cui l'utente ha effettuato per la prima volta l'accesso ad Amazon Chime. Per gli utenti della versione di prova Pro, questa è anche la data di inizio della versione di prova Pro.	01/10/2020
Personal PIN (PIN personale)	IL PIN riunioni personale che l'utente può utilizzare per pianificare riunioni.	0123456789

Campo	Descrizione	Esempio
Privacy setting (Impostazione privacy)	Le impostazioni di presenza selezionate dall'utente.	Public (Pubblica) o Private (Privata)
Meetings attended (Riunioni a cui si è partecipato)	Il numero di riunioni a cui un utente ha partecipato.	87
Meetings organized (Riunioni organizzate)	Il numero di riunioni che un utente ha organizzato.	12
Meeting satisfaction (Valutazi one soddisfazione riunione)	La percentuale di risposte positive fornite al end-of-me eting sondaggio.	92%
Last active date (Data ultima attività)	Data dell'ultima attività eseguita dall'utente.	12/06/2020
Chat messages sent (Messaggi chat inviati)	Il numero di messaggi di chat inviati dall'utente.	1025
Numero di telefono	Il numero di telefono assegnato a un utente, se presente.	+12065550100

Gestione delle autorizzazioni e degli accessi degli utenti

Gestisci le funzionalità a cui possono accedere gli utenti di Amazon Chime assegnando loro autorizzazioni Pro o Basic. Gli utenti con autorizzazioni di base non possono ospitare riunioni, ma possono partecipare alle riunioni e utilizzare la chat. Per ulteriori informazioni sulle funzionalità a cui possono accedere gli utenti con autorizzazioni Pro e Basic, consulta Piani e prezzi.

Gestisci chi può accedere al tuo account amministrativo Amazon Chime invitando o sospendendo gli utenti. Solo gli amministratori di account Enterprise possono sospendere gli utenti. Gli amministratori degli account del team possono rimuovere gli utenti dai propri account in modo che non debbano più pagare per le autorizzazioni dell'utente. Tuttavia, non possono sospendere l'utente per impedirgli di accedere. Per ulteriori informazioni sulle differenze tra gli account Enterprise e Team, consultaGestione degli account Amazon Chime.

Gestione delle autorizzazioni utente

In qualità di amministratore di Amazon Chime, puoi gestire le autorizzazioni Pro e Basic per gli utenti del tuo account Amazon Chime.

Se Active Directory o Okta sono configurati per il tuo account Amazon Chime, gestisci le autorizzazioni degli utenti tramite l'appartenenza al gruppo di directory. Se non hai configurato Active Directory o Okta, gestisci le autorizzazioni utente dalla console Amazon Chime.

Login with Amazon per account aziendali e di team

Se amministri un account Amazon Chime Team o un account Enterprise LWA, in cui gli utenti accedono con i propri account Login with Amazon (LWA), puoi gestire le autorizzazioni Pro e Basic nella console Amazon Chime.

Per gestire le autorizzazioni utente per gli account Team ed Enterprise LWA

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per gli account, scegli il nome dell'account Amazon Chime.
3. Scegliere Users (Utenti).
4. Seleziona gli utenti e scegli Azioni, Assegna autorizzazioni.
5. Scegli una delle seguenti autorizzazioni:
   - Pro
   - Base
6. Scegliere Assign (Assegna).

Account Enterprise Active Directory o Enterprise OpenID Connect (Okta)

Se i tuoi utenti accedono con credenziali Active Directory o Okta, gestisci le loro autorizzazioni rendendoli membri di un gruppo di directory a cui sono assegnate le autorizzazioni Pro o Basic.

Per assegnare le autorizzazioni Pro a un utente, rendilo membro di un gruppo Active Directory o Okta a cui hai assegnato le autorizzazioni Pro. Per assegnare autorizzazioni Basic a un utente, rendilo membro di un gruppo a cui hai assegnato le autorizzazioni Basic. Gli utenti che non dispongono delle autorizzazioni Pro o Basic non possono accedere ad Amazon Chime.

Gestione dell'accesso degli utenti

Se amministri un account Amazon Chime, puoi invitare gli utenti a consentire loro di accedere al tuo account. Gli amministratori degli account aziendali possono sospendere l'accesso degli utenti per impedire loro di accedere all'account.

Invitare e rimuovere gli utenti dell'account Team

Se amministri un account Team, usa la console Amazon Chime per invitare utenti da qualsiasi dominio di posta elettronica.

> **Note**
>
> La prova gratuita di 30 giorni di Pro di un utente termina quando l'utente accetta il tuo invito.

Per invitare gli utenti a un account di team

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per gli account, scegli il nome dell'account Team.
3. Scegli Utenti, Invita utenti.
4. Inserisci gli indirizzi e-mail degli utenti da invitare, separando gli indirizzi e-mail con un punto e virgola (). **;**
5. Scegliere Invite users (Invita utenti).

La procedura seguente dissocia gli utenti dal tuo account Team rimuovendo tutte le autorizzazioni Pro o Basic a loro assegnate. Gli utenti rimossi possono ancora accedere ad Amazon Chime, ma non sono più membri a pagamento del tuo account Amazon Chime.

Per rimuovere gli utenti da un account di team

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per gli account, scegli il nome dell'account Team.
3. Scegliere Users (Utenti).
4. Seleziona gli utenti da rimuovere e scegli Azioni, Rimuovi utente.

Tutte le autorizzazioni Pro o Basic assegnate agli utenti vengono rimosse. Gli utenti non possono più utilizzare il completamento automatico per trovare nuovi utenti del Team nei loro Contatti.

Invito e sospensione degli utenti dell'account Enterprise

Se amministri un account Enterprise, tutti gli utenti che si registrano ad Amazon Chime con un indirizzo e-mail dei domini rivendicati vengono aggiunti automaticamente al tuo account. Se hai configurato Active Directory o Okta, gli utenti devono anche essere membri del gruppo di directory che hai configurato per Amazon Chime.

Per invitare gli utenti in un account aziendale

- Invia un'e-mail di invito agli utenti della tua organizzazione e chiedi loro di seguire la procedura descritta nella sezione Creazione di un account Amazon Chime nella Amazon Chime User Guide.

Gli utenti accedono con un indirizzo e-mail proveniente da uno dei domini che hai richiesto per il tuo account. Dopo aver completato i passaggi per creare i propri account utente Amazon Chime, questi vengono visualizzati automaticamente nella sezione Utenti del tuo account Enterprise nella console Amazon Chime.

La procedura seguente sospende gli utenti da un account Enterprise su cui non sono configurati Active Directory o Okta. Ciò impedisce agli utenti di accedere ad Amazon Chime.

Per sospendere gli utenti da un account aziendale

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per gli account, scegli il nome dell'account Enterprise.
3. Scegliere Users (Utenti).
4. Seleziona gli utenti da sospendere e scegli Azioni, Sospendi utente.
5. Seleziona la casella di controllo e scegli Sospendi.

Se hai configurato Active Directory o Okta per il tuo account Enterprise, usa la seguente procedura per sospendere gli utenti.

Per sospendere gli utenti da un account aziendale Active Directory o OpenID Connect (Okta)

- Esegui una di queste operazioni:

- Dalla dashboard di amministrazione di Active Directory o Okta, sospendi l'utente o contrassegnalo come inattivo.
- Rimuovi l'utente da qualsiasi gruppo di Active Directory a cui sono state assegnate le autorizzazioni Basic o Pro.

Modifica dei PIN riunioni personale

Un PIN riunioni personale è un ID statico generato quando l'utente si registra. Il PIN consente a un utente di Amazon Chime di pianificare facilmente riunioni con altri utenti Amazon Chime. L'utilizzo di un PIN riunioni personale fa sì che gli organizzatori delle riunioni non debbano ricordare i dettagli della riunione per ogni nuova riunione che pianificano.

Se un utente ritiene che il PIN riunioni personale sia stato compromesso, puoi reimpostarlo e generare un nuovo ID. Dopo l'aggiornamento di un PIN riunioni personale, l'utente deve aggiornare tutte le riunioni che sono state programmate utilizzando il vecchio PIN.

Per modificare un PIN riunioni personale.

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Account, seleziona il nome dell'account Amazon Chime.
3. Nel pannello di navigazione, seleziona Utenti.
4. Cerca l'utente che richiede la modifica del PIN.
5. Per aprire la pagina User detail (Dettagli utente), scegli il nome dell'utente.
6. Scegli User actions (Operazioni utente), Reset personal PIN (Reimposta PIN personale), Confirm (Conferma).

Gestione delle versioni di prova di Pro

Quando un utente accetta un invito al team Amazon Chime o viene aggiunto a un account Enterprise, la prova gratuita termina e dispone delle autorizzazioni Pro. Ciò consente agli utenti di continuare a ospitare le riunioni pianificate. La modifica del livello delle autorizzazioni di un utente in Basic (Base) impedisce di ospitare riunioni.

Con i prezzi basati sull'utilizzo di Amazon Chime, paghi solo per gli utenti che organizzano riunioni nei giorni in cui le ospitano. Per i partecipanti alla riunione e per gli utenti della chat non sono previsti addebiti.

Gli utenti sono considerati Active Pro se hanno ospitato una riunione che è terminata in un giorno di calendario e si è verificata almeno una delle seguenti condizioni:

- La riunione era pianificata.
- La riunione includeva più di due partecipanti.
- La riunione ha avuto almeno un evento di registrazione.
- La riunione includeva un partecipante che ha chiamato.
- La riunione includeva un partecipante che si è collegato con H.323 o SIP.

Per ulteriori informazioni, consulta Piani e prezzi.

Richiesta degli allegati degli utenti

Se gestisci un account Enterprise e disponi delle autorizzazioni appropriate, puoi richiedere e ricevere gli allegati che i tuoi utenti caricano in Amazon Chime. Puoi ottenere allegati che gli utenti caricano in conversazioni individuali e di gruppo o nelle chat room da loro create.

> **Note**
>
> Se gestisci un account Amazon Chime Team, puoi passare a un account Enterprise rivendicando uno o più domini. In alternativa, puoi rimuovere utenti dall'account Team, il che consente agli utenti non gestiti di ottenere i propri allegati utilizzando Amazon Chime Assistant.

Per richiedere gli allegati degli utenti

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella pagina Account, seleziona il nome dell'account Amazon Chime.
3. In Settings (Impostazioni), scegli Account (Account), Account actions (Operazioni account), Request attachments (Richiedi allegati).
4. Entro circa 24 ore, la pagina di riepilogo dell'account fornisce un collegamento a un file contenente un elenco di URL predefiniti che utilizzi per accedere a ciascun allegato.

5. Scarica il file .

> **Note**
>
> Assicurati di mantenere un livello appropriato di controllo degli accessi al file. Qualunque utente che ottenga il file può utilizzare l'elenco di URL per scaricare gli allegati associati. Gli URL prefirmati scadono dopo 6 giorni. La richiesta può essere inviata una volta ogni 7 giorni.

Per utilizzare le policy AWS Identity and Access Management (IAM) per gestire l'accesso alla console di amministrazione di Amazon Chime e all'azione Richiedi allegati, utilizza una delle politiche gestite di Amazon Chime (FullAccess, o). UserManagement ReadOnly In alternativa, puoi aggiornare le policy personalizzate per includere le operazioni `StartDataExport` e `RetrieveDataExport`. Per ulteriori informazioni su queste azioni, consulta Actions defined by Amazon Chime nella IAM User Guide.

In che modo Amazon Chime gestisce gli aggiornamenti automatici

Amazon Chime offre diversi modi per aggiornare i propri client. Il metodo varia a seconda che tu esegua Amazon Chime in un browser, sul desktop o su un dispositivo mobile.

L'applicazione web Amazon Chime, https://app.chime.aws, viene sempre caricata con le funzionalità e le correzioni di sicurezza più recenti.

Il client desktop Amazon Chime verifica la presenza di aggiornamenti ogni volta che scegli Esci o Esci. Questo vale per le macchine Windows e macOS. Durante l'esecuzione, il client verifica la presenza di aggiornamenti ogni tre ore. Puoi anche verificare la presenza di aggiornamenti scegliendo Controlla aggiornamenti nel menu Aiuto di Windows o nel menu Amazon Chime di macOS.

Quando il client desktop rileva un aggiornamento, Amazon Chime richiede all'utente di installarlo a meno che non sia coinvolto in una riunione in corso. Partecipano a una riunione continua quando:

- Partecipano a una riunione.
- Sono stati invitati a una riunione che è ancora in corso.

Amazon Chime richiede loro di installare la versione più recente e fornisce un conto alla rovescia di 15 secondi in modo che possano posticipare l'installazione. Gli utenti scelgono Riprova più tardi per posticipare l'aggiornamento.

Se gli utenti posticipano un aggiornamento e non partecipano a una riunione in corso, il client verifica la presenza dell'aggiornamento dopo tre ore e chiede loro nuovamente di installarlo. L'installazione inizia al termine del conto alla rovescia.

> **Note**
>
> Su un computer macOS, gli utenti devono scegliere Riavvia ora per iniziare l'aggiornamento.

Su dispositivi mobili: le applicazioni mobili di Amazon Chime utilizzano le opzioni di aggiornamento fornite da App Store e Google Play per fornire la versione più recente del client Amazon Chime. Puoi anche utilizzare il sistema di gestione dei dispositivi mobili per distribuire gli aggiornamenti.

Migrazione degli utenti verso un altro account Team

Esegui la migrazione degli utenti ad altri account Team creando e configurando un account di destinazione, se non ne esiste già uno. Quindi aggiungi gli utenti all'account di destinazione. I passaggi seguenti forniscono informazioni sul completamento di ogni parte di una migrazione.

Per migrare gli utenti

1. Se non disponi di un account Team di destinazione, creane uno. Per ulteriori informazioni, consulta Passaggio 1: creazione di un account amministratore Amazon Chime.
2. Se necessario, configura l'account. Per ulteriori informazioni, consulta Fase 2 (facoltativo): configurazione delle impostazioni dell'account.
3. Aggiungi utenti all'account. Per ulteriori informazioni, consulta Fase 3: aggiunta di utenti all'account.

Gestione dei numeri di telefono in Amazon Chime

Usa la console Amazon Chime per fornire numeri di telefono. Quando esegui il provisioning dei numeri, li richiedi da un pool di numeri gestito da Amazon Chime. Quando annulli l'assegnazione e poi elimini i numeri, questi ritornano nel pool. Quando trasferisci i numeri, li trasferisci da e verso Amazon Chime.

> **Note**
>
> Quando usi la console Amazon Chime, puoi fornire solo i numeri di chiamata Amazon Chime Business. Se hai bisogno di numeri internazionali, utilizza i connettori vocali Amazon Chime e le applicazioni multimediali SIP. Per farlo, devi prima creare un account amministrativo Amazon Chime SDK. Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'amministratore di Amazon Chime SDK:
>
> - Prerequisiti
> - Gestione dell'inventario dei numeri di telefono
> - Gestione dei connettori vocali
> - Gestione delle applicazioni multimediali SIP

Gli argomenti nelle sezioni seguenti spiegano come fornire e gestire i numeri di telefono di Amazon Chime.

Indice

Provisioning di numeri di telefono

Usa la console Amazon Chime per fornire i numeri di telefono per il tuo account Amazon Chime. I numeri provengono da un pool gestito da Amazon Chime. Scegli Amazon Chime Business Calling per fornire e assegnare numeri di telefono ai tuoi utenti Amazon Chime esistenti.

Una volta completato il provisioning, i numeri di telefono vengono visualizzati nel tuo inventario. Li assegni quindi a singoli utenti.

Per effettuare il provisioning di numeri di telefono

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Scegliere Orders (Ordini), Provision phone numbers (Effettua il provisioning di numeri di telefono).
4. Seleziona Business Calling, quindi scegli Avanti.
5. Cerca i numeri di telefono disponibili. Selezionare i numeri di telefono desiderati, quindi scegliere Provision (Effettua il provisioning).

I numeri di telefono vengono visualizzati negli elenchi Ordini e In sospeso durante l'approvvigionamento.

Trasferimento di numeri di telefono esistenti

Oltre a fornire numeri di telefono, puoi anche trasferire i numeri del tuo operatore telefonico nel tuo inventario. Sono inclusi i numeri verdi.

> **Note**
>
> Se devi trasferire numeri internazionali, usare Amazon Chime Voice Connector o usare applicazioni multimediali SIP, devi creare un account amministratore Amazon Chime SDK e utilizzare la console Amazon Chime SDK. Per ulteriori informazioni su questa operazione, consulta Prerequisiti, nella Amazon Chime SDK Administrator Guide.

Le seguenti sezioni spiegano come trasferire i numeri di telefono.

Argomenti

Prerequisiti per la portabilità dei numeri

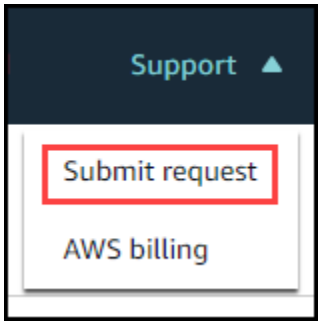
Per i numeri di porta, è necessario disporre di una lettera di agenzia (LOA). È necessario disporre di un LOA per i numeri di telefono nazionali. Scarica il modulo Letter of Agency (LOA) e compilalo. Se devi trasferire numeri di telefono di diversi operatori, compila un LOA separato per ciascun operatore.

Trasferimento dei numeri di telefono in

Si crea una richiesta di supporto per trasferire i numeri di telefono esistenti.

Per trasferire numeri di telefono esistenti

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nella barra dei comandi nella parte superiore della pagina, scegli Support, quindi scegli Invia richiesta.



   Verrai reindirizzato alla console AWS Support.

> **Note**
>
> Puoi anche andare direttamente alla pagina del AWS Support Centro. In tal caso, scegli Crea custodia, quindi segui i passaggi seguenti.

3. Nella sezione Come possiamo aiutarti, procedi come segue:
   a. Scegli Account e fatturazione.
   b. Dall'elenco dei servizi, scegli Chime SDK (Number Management).
   c. Dall'elenco delle categorie, scegli Phone Number Port In.
   d. Scegli Fase successiva: informazioni aggiuntive.
4. In Informazioni aggiuntive, procedi come segue
   a. In Oggetto, inserisci**`Porting phone numbers in`**.
   b. In Descrizione, inserisci le seguenti informazioni:

      Per la portabilità di numeri statunitensi:

      - Numero di telefono di fatturazione (BTN) dell'account.
      - Nome della persona autorizzante. Si tratta della persona responsabile della fatturazione dell'account con l'operatore corrente.
      - Operatore corrente, se noto.
      - Numero dell'account del servizio, se queste informazioni sono presenti all'operatore corrente.
      - PIN del servizio, se disponibile.
      - Indirizzo del servizio e nome del cliente, come indicato nel contratto di telefonia corrente.
      - Data e ora richieste per la porta.
      - (Facoltativo) Se desideri trasferire il tuo numero di telefono di fatturazione (BTN), seleziona una delle seguenti opzioni:
        - Sto trasferendo il mio BTN e voglio sostituirlo con un nuovo BTN che sto fornendo. Posso confermare che questo nuovo BTN è sullo stesso conto del gestore attuale.
        - Sto trasferendo il mio BTN e voglio chiudere il mio account con il mio attuale carrier.

- Sto trasferendo il mio BTN perché il mio account è attualmente configurato in modo che ogni numero di telefono sia il proprio BTN. (Seleziona questa opzione solo quando il tuo account con il carrier corrente è impostato in questo modo.)
- Dopo aver scelto un'opzione, allega la tua lettera di agenzia (LOA) alla richiesta.

Per la portabilità di numeri internazionali:

- È necessario utilizzare il tipo di prodotto SIP Media Application Dial-In per numeri di telefono non statunitensi.
- Tipo di numero (locale o gratuito)
- Numeri di telefono esistenti da trasferire.
- Stima del volume di utilizzo
- Paese

c. Dall'elenco dei tipi di numero di telefono, selezionare Business Calling, SIP Media Application Dial-In o Voice Connector.

d. In Numero di telefono, inserisci almeno un numero di telefono, anche se stai trasferendo più numeri.

e. In Data di portabilità, inserisci la data di portabilità desiderata.

f. In Porting Time, inserisci l'ora desiderata.

g. Scegli Passaggio successivo: risolvi ora o contattaci.

5. In Risolvi ora o contattaci, scegli Contattaci.
6. Dall'elenco Lingua di contatto preferita, scegli una lingua
7. Scegli Web o Telefono. Se scegli Telefono, inserisci il tuo numero di telefono. Al termine, scegli Invia.

AWS Support ti consente di sapere se i tuoi numeri di telefono possono essere trasferiti dal tuo operatore telefonico esistente. Se puoi, devi inviare tutti i documenti richiesti. I passaggi indicati nella sezione successiva spiegano come inviare tali documenti.

Invio dei documenti richiesti

Dopo che AWS Support ti ha detto che puoi trasferire i numeri di telefono, devi inviare tutti i documenti richiesti. I passaggi seguenti spiegano come.

> **Note**
>
> AWS Support fornisce un collegamento Amazon S3 sicuro per il caricamento di tutti i documenti richiesti. Non procedere finché non ricevi il link.

Per inviare documenti

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Accedi al tuo AWS account, quindi apri il link di caricamento di Amazon S3 generato appositamente per il tuo account.

   > **Note**
   >
   > Il link scade dopo dieci giorni. Viene generato specificamente per l'account che ha creato il caso. Il collegamento richiede che un utente autorizzato dell'account esegua il caricamento.

3. Scegli Aggiungi file, quindi seleziona i documenti di identità relativi alla tua richiesta.
4. Espandi la sezione Autorizzazioni e scegli Specificare autorizzazioni ACL individuali.
5. Alla fine della sezione Access control list (ACL), scegli Aggiungi beneficiario, quindi incolla la chiave fornita da AWS Support nella casella Assegnatario.
6. In Oggetti, seleziona la casella di controllo Leggi, quindi scegli Carica.

Dopo aver fornito la lettera di agenzia (LOA), AWS Support conferma con il tuo operatore telefonico esistente che le informazioni sulla LOA sono corrette. Se le informazioni fornite sulla LOA non corrispondono a quelle che il gestore telefonico ha in archivio, AWS Support ti contatta per aggiornare le informazioni fornite sulla LOA.

Visualizzazione dello stato della richiesta

I passaggi seguenti spiegano come utilizzare la console Amazon Chime per visualizzare lo stato delle richieste di porting.

Per visualizzare lo stato

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.

2. Nel pannello di navigazione, scegli Gestione dei numeri di telefono.
3. Scegli la scheda Ordini.

La colonna Stato mostra lo stato della richiesta. AWS Support ti contatta anche per aggiornamenti e richieste di ulteriori informazioni, se necessario. Per ulteriori informazioni, consulta Definizioni dello stato di conversione del numero di telefono, in seguito in questa sezione.

Assegnazione di numeri di porta

Dopo che l'operatore telefonico ha confermato che il LOA è corretto, esaminerà e approverà la porta richiesta. Quindi forniscono AWS Support una data e un'ora del Firm Order Commit (FOC) in cui si verificherà la porta.

Alla data FOC, i numeri di telefono trasferiti vengono attivati per l'uso. È quindi necessario assegnare i numeri agli utenti dell'account desiderato.

Per assegnare numeri di telefono

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, scegli Gestione dei numeri di telefono.
3. Nella scheda Inventario, seleziona la casella di controllo accanto al numero che desideri assegnare, quindi scegli Assegna.

> **Note**
>
> Puoi scegliere un solo numero alla volta.

4. Nella pagina Assegna +1 numero di telefono a un profilo utente, seleziona l'account per il numero, quindi scegli Avanti.
5. Seleziona l'utente a cui vuoi assegnare il numero, quindi scegli Assegna.

Trasferimento dei numeri di telefono

Puoi trasferire i numeri da Amazon Chime avviando una richiesta di portabilità con il tuo operatore vincente. Quando invii le informazioni al tuo operatore vincente, includi l'ID del tuo AWS account come ID dell'account associato al numero di telefono da trasferire.

Quando il processo di trasferimento è terminato e l'operatore vincente avrà i numeri, dovrai annullare l'assegnazione ed eliminare tali numeri dal tuo inventario. Per ulteriori informazioni, consulta Annullamento dell'assegnazione dei numeri di telefono di Amazon Chime Business Calling e Eliminazione di numeri di telefono in questa guida.

Important

- La capacità di trasferire i numeri dipende dalla capacità del vettore vincente di accettare tali numeri.
- La verifica dell'autenticità della richiesta di porting del nuovo operatore è fondamentale per la sicurezza del tuo numero di telefono. Se i dettagli dell'account non sono corretti (ad esempio, l'ID dell'account non corrisponde), la richiesta di portout potrebbe essere rifiutata, causando ritardi e richiedendo di inviare nuovamente la richiesta.

(Facoltativo) Come richiedere un PIN per proteggere il tuo numero

Per una maggiore sicurezza, puoi contattarci per applicare un PIN al tuo numero. L'operatore che si aggiudica il premio utilizza quindi quel PIN. Completare la procedura riportata di seguito.

Per richiedere un PIN

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel riquadro di navigazione, in Contattaci, scegli Support.

   Verrai reindirizzato alla console AWS Support.

   Note

   Puoi anche andare direttamente alla pagina del AWS Support Centro. In tal caso, scegli Crea custodia, quindi segui i passaggi seguenti.
3. Nella sezione Come possiamo aiutarti, procedi come segue:

   a. Scegli Account e fatturazione.
   b. Dall'elenco dei servizi, scegli Chime SDK (Number Management).
   c. Dall'elenco delle categorie, scegli Phone Number Port Out.
   d. Scegli Fase successiva: informazioni aggiuntive.

4. In Informazioni aggiuntive, procedi come segue

   a. In Oggetto, inserisci**`Porting phone numbers out`**.

   b. In Descrizione, inserire quanto segue.

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

   > **Note**
   >
   > È necessario fornire un PIN alfanumerico di 4-10 caratteri.

AWS Support associa un PIN al numero di telefono. Quando richiedi il porto al corriere vincente, fornisci l'ID AWS dell'account e il PIN. Utilizzeremo tali informazioni per convalidare tutte le richieste portuali ricevute per il tuo numero.

Definizioni dello stato di conversione del numero di telefono

Dopo aver inviato una richiesta di trasferimento dei numeri di telefono esistenti in Amazon Chime, puoi visualizzare lo stato della richiesta di portabilità nella console Amazon Chime in Chiamate, Gestione dei numeri di telefono, In sospeso.

Gli stati e le definizioni della portabilità includono quanto segue:

CANCELLED

AWS Support ha annullato l'ordine di portabilità a causa di un problema relativo al porto, ad esempio una richiesta di annullamento da parte del corriere o da parte tua. AWS Support ti contatta con i dettagli.

CANCEL_REQUESTED

AWS Support sta elaborando un annullamento dell'ordine di portabilità a causa di un problema con il porto, ad esempio una richiesta di cancellazione da parte del corriere o da parte tua. AWS Support ti contatta con i dettagli.

CHANGE_REQUESTED

AWS Support sta elaborando la tua richiesta di modifica e la risposta del corriere è in sospeso. Consentire ulteriore tempo di elaborazione.

COMPLETED

L'ordine di portabilità è stato completato e i numeri di telefono sono attivati.

EXCEPTION

AWS Support ti contatta per ulteriori dettagli necessari per completare la richiesta di porto. Consentire ulteriore tempo di elaborazione.

FOC

La data FOC è confermata con il corriere. AWS Support ti contatta per confermare la data.

PENDING DOCUMENTS

AWS Support ti contatta per i documenti aggiuntivi necessari per completare la richiesta del porto. Consentire ulteriore tempo di elaborazione.

SUBMITTED (INVIATO)

L'ordine di portabilità è stato inviato e la risposta del corriere è in sospeso.

Assegnazione dei numeri di telefono di Amazon Chime Business Calling

Utilizza la pagina Inventario per la gestione dei numeri di telefono per assegnare i numeri di telefono di Amazon Chime Business Calling ai singoli utenti.

Per assegnare i numeri di telefono di Amazon Chime Business Calling

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Nella scheda Inventario, seleziona il numero di telefono che desideri assegnare.
4. Scegliere Assign (Assegna).
5. Seleziona l'account a cui appartiene l'utente, quindi scegli Avanti.
6. Seleziona l'utente, quindi scegli Assegna.

Quando modifichi un numero di telefono o le autorizzazioni di un numero di telefono, ti consigliamo di fornire all'utente le informazioni nuove o sulle autorizzazioni. Prima che gli utenti possano accedere

al nuovo numero di telefono o alle nuove funzionalità di autorizzazione, devono uscire dal proprio account Amazon Chime e accedere nuovamente.

Annullamento dell'assegnazione dei numeri di telefono di Amazon Chime Business Calling

La procedura seguente annulla l'assegnazione dei numeri di telefono agli utenti di Amazon Chime Business Calling.

Per annullare l'assegnazione dei numeri di telefono

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Nella scheda Inventario, seleziona il numero di telefono che desideri annullare l'assegnazione.
4. Scegliere Unassign (Annulla assegnazione).
5. Selezionare la casella di controllo e scegliere Unassign (Annulla assegnazione).

Puoi visualizzare i dettagli dei numeri nel tuo inventario. Ad esempio, puoi vedere se le telefonate e gli SMS sono abilitati.

Per visualizzare i dettagli del numero di telefono di inventario

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Scegli la scheda Inventario, quindi seleziona il numero di telefono che desideri visualizzare.
4. Apri l'elenco Azioni e scegli Visualizza dettagli.

Utilizzo dei nomi per le chiamate in uscita

I nomi delle chiamate in uscita fungono da ID chiamante. Puoi impostare un nome di chiamata predefinito per uno o più numeri di telefono nel tuo inventario. Puoi anche impostare nomi di chiamata univoci per singoli numeri di telefono. I nomi vengono quindi visualizzati ai destinatari delle chiamate in uscita effettuate utilizzando tali numeri di telefono. I nomi di chiamata si applicano a tutti i tipi di prodotti con numeri di telefono. Puoi aggiornare i nomi una volta ogni sette giorni.

Ad esempio, puoi impostare il nome di chiamata predefinito Dipartimento 5 per tutti i numeri di telefono di quel reparto. Puoi anche impostare un nome univoco di Jane Doe per il capo dipartimento.

I passaggi seguenti spiegano come impostare i nomi di chiamata in uscita predefiniti e individuali.

Per impostare un nome di chiamata

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Nella scheda Inventario, esegui una delle seguenti operazioni: seleziona le caselle di controllo accanto ai numeri di telefono che desideri aggiornare.
   - Per impostare un nome di chiamata predefinito per più numeri, seleziona le caselle di controllo accanto a tali numeri.
   - Per impostare un nome di chiamata individuale, seleziona il numero desiderato.
4. Apri l'elenco Azioni e scegli Aggiorna il nome di chiamata predefinito.
5. Nella casella Nome di chiamata predefinito, inserisci un nome composto da un massimo di 15 caratteri.
6. Selezionare Salva.

Attendi 72 ore affinché il sistema aggiorni il nome di chiamata predefinito.

Eliminazione di numeri di telefono

> **Important**
>
> Solo gli amministratori di sistema Amazon Chime possono completare questi passaggi. Inoltre, devi annullare l'assegnazione dei numeri di telefono prima di poterli eliminare.

Quando fornisci un numero di telefono, lo ordini da un pool di numeri gestito da Amazon Chime. L'eliminazione di un numero lo riporta nel pool. Quando elimini un numero, questo viene prima inserito nella coda di eliminazione, dove viene conservato per 7 giorni. Durante questo periodo, puoi riportare il numero nel tuo inventario. Dopo 7 giorni, il sistema elimina automaticamente il numero dalla coda di attesa e lo dissocia dal tuo account. In questo modo il numero viene riportato nel pool di numeri. Se hai bisogno di recuperare un numero dopo che il sistema lo ha eliminato dalla coda di

attesa, segui i passaggi indicatiProvisioning di numeri di telefono, ma tieni presente che il numero potrebbe non essere disponibile.

Per eliminare i numeri di telefono non assegnati

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Scegli la scheda Inventario, quindi seleziona il numero o i numeri di telefono che desideri eliminare.
4. Apri l'elenco Azioni e scegli Elimina numeri di telefono.
5. Seleziona la casella di controllo, quindi scegli Elimina.

I numeri di telefono eliminati vengono conservati nella coda di eliminazione per 7 giorni prima di essere eliminati definitivamente dall'inventario.

Ripristino di numeri di telefono eliminati

Puoi ripristinare i numeri di telefono eliminati dalla coda di eliminazione per un massimo di 7 giorni dopo averli eliminati. Il ripristino di un numero di telefono lo sposta nuovamente in Inventory (Inventario).

Per ripristinare numeri di telefono eliminati

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Nel pannello di navigazione, sotto Chiamata, scegli Gestione dei numeri di telefono.
3. Scegli la scheda Coda di eliminazione, quindi seleziona il numero o i numeri di telefono che desideri ripristinare.
4. Scegliere Move to inventory (Sposta in inventario).

Gestione delle impostazioni globali in Amazon Chime

Utilizzi la console Amazon Chime per gestire le impostazioni dei record dei dettagli delle chiamate.

Configurazione dei record di dettaglio delle chiamate

Prima di poter configurare le impostazioni dei record di dettaglio delle chiamate per il tuo account amministrativo Amazon Chime, devi prima creare un bucket Amazon Simple Storage Service. Il bucket Amazon S3 viene utilizzato come destinazione per i registri delle chiamate. Quando configuri le impostazioni del record dei dettagli delle chiamate, concedi ad Amazon Chime l'accesso in lettura e scrittura al bucket Amazon S3 per salvare e gestire i tuoi dati. Per ulteriori informazioni sulla creazione di un bucket Amazon S3, consulta Nozioni di base su Amazon Simple Storage Service nella Guida per l'utente di Amazon Simple Storage Service.

Puoi configurare le impostazioni dei record dei dettagli delle chiamate per Amazon Chime Business Calling. Per ulteriori informazioni su Amazon Chime Business Calling, vedereGestione dei numeri di telefono in Amazon Chime.

Per configurare le impostazioni del record di dettaglio delle chiamate

1. Crea un bucket Amazon S3 seguendo le operazioni di base di Amazon Simple Storage Service nella Guida per l'utente di Amazon Simple Storage Service.
2. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
3. Per Global Settings (Impostazioni globali), scegliere Call detail records (Record di dettaglio delle chiamate).
4. Scegli Business Calling Configuration.
5. Per Destinazione Log, seleziona il bucket Amazon S3.
6. Seleziona Salva.

È possibile interrompere la registrazione dei dettagli delle chiamate in qualsiasi momento.

Per interrompere la registrazione dei record dei dettagli delle chiamate

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Per Global Settings (Impostazioni globali), scegliere Call detail records (Record di dettaglio delle chiamate).

3. Scegliere Disabilita registrazione per la configurazione applicabile.

Record delle chiamate Amazon Chime Business Calling

Quando scegli di ricevere i record dei dettagli delle chiamate per Amazon Chime Business Calling, questi vengono inviati al tuo bucket Amazon S3. L'esempio seguente mostra il formato generale del nome del record di dettaglio di una chiamata 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
```

Nell'esempio seguente vengono illustrati i dati rappresentati nel nome del record di dettaglio della chiamata.

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

L'esempio seguente mostra il formato generale di un record di dettaglio di una chiamata Amazon Chime Business Calling.

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

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

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

    "ConferenceStartTimeEpochSeconds": "1556009595",
    "ConferenceEndTimeEpochSeconds": "1556009623",
```

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

Configurazione della sala riunioni

Amazon Chime può integrarsi con l'hardware video in camera di Cisco, Tandberg, Polycom, Lifesize, Vidyo o altri quando usi il protocollo SIP o H.323.

Per connetterti ad Amazon Chime utilizzando un dispositivo VTC per sala conferenze che supporti SIP, inserisci una delle seguenti opzioni:

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- ID riunione di 10 cifre seguito da **`@meet.chime.in`**

`meet.chime.in`collega il dispositivo della sala SIP alla regione Amazon Chime più vicina. Per connetterti a una regione specifica, utilizza le voci DNS specifiche della regione per i sistemi sala SIP. Per ulteriori informazioni, consulta Sistemi di videoconferenza SIP (Session Initiation Protocol).

> **Note**
>
> Se il dispositivo sala SIP non supporta TLS e richiede connettività TCP, contatta AWS Support.

Se utilizzi un dispositivo che supporta solo H.323, è necessario comporre uno dei seguenti elementi:

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

Se un firewall filtra il traffico tra il dispositivo VTC e Amazon Chime, apri gli intervalli per i protocolli utilizzati. Per ulteriori informazioni, consulta Requisiti di larghezza di banda e di configurazione di rete.

Nella schermata di benvenuto di Amazon Chime, inserisci l'ID della riunione a 10 o 13 cifre per partecipare. Puoi trovare l'ID riunione a 13 cifre nel client Amazon Chime o nell'app web oppure scegliere l'opzione Dial-in.

Partecipazione a una riunione moderata

Se la riunione è moderata e sei l'organizzatore o il delegato, immetti l'ID riunione di 13 cifre per accedere alla riunione come moderatore. Se sei un moderatore, immetti il codice di accesso del moderatore nel tastierino seguito da cancelletto (#) per accedere e iniziare la riunione. Se non sei un organizzatore, un delegato o un moderatore, vieni connesso alla riunione dopo l'accesso del moderatore e l'avvio della riunione.

I moderatori dispongono di controlli da organizzatore, ovvero possono eseguire operazioni aggiuntive durante la riunione. Queste operazioni includono l'avvio e l'arresto della registrazione, la disattivazione dell'audio di tutti gli altri partecipanti, il blocco, lo sblocco e la terminazione della riunione. Per ulteriori informazioni, consulta Azioni dei moderatori utilizzando il telefono o i sistemi video in camera nella Guida per l'utente di Amazon Chime.

> **Note**
>
> Se utilizzi Alexa for Business per partecipare alle riunioni Amazon Chime, puoi partecipare come moderatore solo se il tuo dispositivo è collegato a un sistema video in camera e accedi utilizzando la tastiera del dispositivo.

Dispositivi VTC compatibili

La tabella seguente è un sottoinsieme dell'elenco dei dispositivi compatibili con VTC.

Dispositivo	SIP	H.323	Commento
Cisco SX20	Sì	Sì	Audio/Video/ Schermo: OK in ingresso e in uscita
Cisco DX80	Sì	Sì	Audio/Video/ Schermo: OK in ingresso e in uscita
Lifesize Icon	Sì	No	Audio/Video/ Schermo: OK in ingresso e in uscita

Dispositivo	SIP	H.323	Commento
Polycom Debut	Sì	Sì	Audio/Video/Schermo: OK in ingresso e in uscita
RealPresence Desktop Polycom	No	Sì	Audio/Video: OK, Schermo: dispositivo in ingresso OK
Polycom Trio	Sì	Sì	Audio/Video/Schermo: OK in ingresso e in uscita
Tandberg C40	Sì	Sì	Audio/Video/Schermo: OK in ingresso e in uscita

Requisiti di larghezza di banda e di configurazione di rete

Amazon Chime richiede le destinazioni e le porte descritte in questo argomento per supportare vari servizi. Se il traffico in entrata o in uscita è bloccato, questo potrebbe pregiudicare la possibilità di utilizzare diversi servizi, tra cui audio, video, condivisione dello schermo o chat.

Amazon Chime utilizza Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute EC2) e altri servizi AWS sulla porta TCP/443. Se il firewall blocca la porta TCP/443, è necessario inserire `*.amazonaws.com` in un elenco di indirizzi consentiti o inserire gli intervalli di indirizzi IP AWS in Riferimenti generali di AWS per i seguenti servizi:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Espandi le seguenti sezioni per ulteriori informazioni su destinazioni, porte e larghezza di banda.

Destinazioni e porte richieste

Le seguenti destinazioni e porte sono necessarie per eseguire Amazon Chime.

Destinazione	Porte
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

Porta per riunioni e telefonia

Amazon Chime utilizza la destinazione e la porta seguenti per le riunioni e Amazon Chime Business Calling.

Destinazione	Porta
99.77.128.0/18	UDP/3478

Sistemi di videoconferenza H.323

Amazon Chime utilizza le seguenti destinazioni e porte per i sistemi video in sala H.323.

Destinazione	Porte
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	

Sistemi di videoconferenza SIP (Session Initiation Protocol)

Le seguenti destinazioni e porte sono consigliate quando si eseguono sistemi video in sala Amazon Chime for SIP nel proprio ambiente.

AWS Regione	Destinazione	Porte
Globale (regione più vicina)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS Regione	Destinazione	Porte
	52.55.63.0/25	
Globale	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
Stati Uniti orientali (Virginia settentrionale)	meet.ue1.chime.in	TCP/5061
US West (Oregon)	meet.uw2.chime.in	TCP/5061
Asia Pacifico (Singapore)	meet.as1.chime.in	TCP/5061
Asia Pacifico (Sydney)	meet.as2.chime.in	TCP/5061
Asia Pacifico (Tokyo)	meet.an1.chime.in	TCP/5061
Europa (Irlanda)	meet.ew1.chime.in	TCP/5061
Sud America (San Paolo)	meet.se1.chime.in	TCP/5061

Requisiti di larghezza di banda

Amazon Chime ha i seguenti requisiti di larghezza di banda per la condivisione di audio, video e schermo:

- Audio
  - Chiamata 1:1: 54 kbps in upload e in download
  - Chiamata con più utenti: non più di 32 kbps extra in download per 50 chiamanti
- Video
  - Chiamata 1:1: 650 kbps in upload e in download
  - Modalità HD: 1400 kbps in upload e in download
  - 3-4 utenti: 450 kbps in upload e (N-1)*400 kbps in download
  - 5-16 utenti: 184 kbps in upload e (N-1)*134 kbps in download

  - La larghezza di banda in upload e download si adatta al valore più basso in base alle condizioni di rete
- Condivisione dello schermo
  - 1,2 mbps in upload (durante la presentazione) e in download (durante la visualizzazione) per alta qualità. Si adatta a diminuire a 320 kbps in base alle condizioni di rete.
  - Telecomando: 800 kbps fissi

Visualizzazione dei report

Per prendere decisioni più informate e aumentare la produttività dell'organizzazione, è possibile accedere ai dati di utilizzo e di feedback direttamente dalla console. I dati dei report vengono aggiornati quotidianamente, anche se potrebbe verificarsi un ritardo di 48 ore.

Per visualizzare i report di utilizzo e di feedback

1. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
2. Scegli Reports (Report), Dashboard (Pannello di controllo).
3. Nella pagina Usage and feedback dashboard report (Report pannello di controllo utilizzo e feedback), visualizza i seguenti dati:

> **Note**
>
> Per ulteriori informazioni sui dati a disposizione, consulta Pannello di controllo dei rapporti Amazon Chime e dettagli sull'attività degli utenti.

- Intervallo di date (UTC): l'intervallo di date del rapporto.
- Utenti registrati: il numero di utenti che si sono registrati ad Amazon Chime.
- Utenti attivi: il numero di utenti che hanno partecipato a una riunione o inviato un messaggio con Amazon Chime.
- Riunioni tenute: il numero totale di riunioni terminate. È possibile selezionare una riunione specifica per visualizzarne i dettagli, tra cui l'ID conferenza, l'ora di inizio, il tipo, l'organizzatore, la durata e il numero di partecipanti. Scegliere un determinato valore, Conference ID (ID conferenza) o Meeting organizer (Organizzatore riunione) per visualizzare ulteriori dettagli, tra cui i partecipanti, gli eventi del registro della riunione, il tipo di client e il feedback della riunione.
- Soddisfazione nell'incontro: la percentuale di risposte positive fornite al end-of-meeting sondaggio.
- Messaggi di chat inviati: il numero di messaggi di chat inviati dagli utenti.

Estensione del client desktop Amazon Chime

Puoi estendere le funzionalità del client desktop Amazon Chime aggiungendo bot di chat, sessioni telefoniche proxy e webhook. I chat bot consentono agli utenti di eseguire attività come l'interrogazione di informazioni sui sistemi interni. Le sessioni telefoniche proxy consentono agli utenti di chiamare e inviare messaggi senza rivelare i propri numeri di telefono. I webhook possono inviare automaticamente messaggi alle chat room. Ad esempio, un webhook può inviare promemoria delle riunioni a un team, insieme a un link alla riunione.

Argomenti

Gestione degli utenti

I seguenti frammenti di codice possono aiutarti a gestire gli utenti di Amazon Chime. Tutti gli esempi in questo argomento utilizzano Java.

Argomenti

Invita più utenti

L'esempio seguente mostra come invitare più utenti a un account 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);
```

Scaricamento di elenchi utenti

L'esempio seguente mostra come scaricare un elenco di utenti associati al tuo account amministrativo Amazon Chime in `.csv` formato.

```
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();
```

Esci da più utenti

L'esempio seguente mostra come disconnettere più utenti dal tuo account amministrativo Amazon Chime.

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

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

    chime.logoutUser(logoutUserRequest);
}
```

Aggiorna i PIN personali degli utenti

L'esempio seguente mostra come reimpostare il PIN della riunione personale per un utente Amazon Chime specificato.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

Integrazione dei chatbot nel client desktop Amazon Chime

Puoi utilizzare il pluginAWS Command Line Interface(AWS CLI), API Amazon Chime oAWSSDK per integrare i chatbot con Amazon Chime. I chatbot ti consentono di sfruttare la potenza di Amazon Lex,AWS Lambda, e altroAWSservizi per semplificare le attività comuni con interfacce conversazionali intelligenti accessibili agli utenti nelle chat room di Amazon Chime.

Se sei un amministratore di account Amazon Chime Enterprise, puoi utilizzare i chatbot per consentire agli utenti di eseguire attività come:

- Interrogazione di informazioni sui loro sistemi interni.
- Automatizzazione di attività.
- Ricezione di notifiche per problemi critici.
- Creazione di ticket di supporto.

Per ulteriori informazioni sugli account Amazon Chime Enterprise, consultareGestione degli account Amazon Chime.

Se amministri un account Amazon Chime Enterprise, puoi creare fino a 10 chatbot per l'integrazione con Amazon Chime. I chatbot possono essere utilizzati solo nelle chat room create dai membri del tuo account. Solo gli amministratori delle chat room possono aggiungere chatbot a una chat room. Dopo aver aggiunto un chatbot a una chat room, i membri della chat room possono interagire con il bot utilizzando i comandi forniti dal creatore del bot. Per ulteriori informazioni, consultare la sezione successiva di questo argomento.

Gli utenti Linux e macOS possono creare un chatbot personalizzato di esempio. Per ulteriori informazioni, consulta la paginaCrea chatbot personalizzati per Amazon Chime.

Contenuti

Usare i chatbot con Amazon Chime

Se amministri un account Amazon Chime Enterprise, puoi creare fino a 10 chatbot per l'integrazione con Amazon Chime. I chatbot possono essere utilizzati solo nelle chat room create dai membri del tuo account. Solo gli amministratori delle chat room possono aggiungere chatbot a una chat room. Dopo aver aggiunto un chatbot a una chat room, i membri della chat room possono interagire con il bot utilizzando i comandi forniti dal creatore del bot. Per ulteriori informazioni, consulta la paginaUtilizzo dei chatbotnelGuida per l'utente di Amazon Chime.

Puoi anche utilizzare l'operazione dell'API Amazon Chime per abilitare o interrompere i chatbot per il tuo account Amazon Chime. Per ulteriori informazioni, consulta Aggiorna i chatbot.

> **Note**
>
> Non puoi eliminare i chatbot. Per impedire l'utilizzo di un chatbot nel tuo account, usa Amazon ChimeUpdateBotFunzionamento API inRiferimento API Amazon Chime. Quando interrompi un chatbot, gli amministratori della chat room possono rimuoverlo da una chat room, ma non possono aggiungerlo a una chat room. Gli utenti che utilizzano @mention su un chatbot interrotto in una chat room ricevono un messaggio di errore.

Prerequisiti

Prima di iniziare la procedura DLQ, completare i seguenti prerequisiti:

- Crea un chatbot.
- Crea l'endpoint in uscita per Amazon Chime per inviare eventi al tuo bot. Scegli tra un ARN di funzione AWS Lambda o un endpoint HTTPS. Per ulteriori informazioni su Lambda, consulta la Guida per gli sviluppatori di AWS Lambda.

Best practice DNS per gli endpoint HTTPS

Consigliamo le seguenti best practice durante l'assegnazione di DNS all'endpoint HTTPS:

- Usare un sottodominio DNS dedicato all'endpoint del bot.
- Utilizzare solo record A per puntare all'endpoint del bot.
- Proteggere il server DNS e l'account di registro DNS per evitare attacchi al dominio.
- Utilizzare certificati intermedi TLS validi pubblicamente dedicati all'endpoint del bot.
- Verifica crittograficamente la firma del messaggio del bot prima di agire su un messaggio bot.

Dopo aver creato il tuo chatbot, usa ilAWS Command Line Interface(AWS CLI) o l'operazione dell'API Amazon Chime per completare le attività descritte nelle sezioni seguenti.

Processi

- Passaggio 1: integra un chatbot con Amazon Chime
- Fase 2: configurare l'endpoint DLQ per un chatbot Amazon Chime
- Passaggio 3: aggiungi il chatbot a una chat room di Amazon Chime
- Autentica le richieste DLQ
- Aggiorna i chatbot

Passaggio 1: integra un chatbot con Amazon Chime

Dopo aver completato ilprerequisiti, integra il tuo chatbot con Amazon Chime utilizzando ilAWS CLIo l'API Amazon Chime.

> **Note**
>
> Queste procedure creano un nome e un indirizzo e-mail per il tuo chatbot. I nomi e gli indirizzi e-mail dei Chatbot non possono essere modificati dopo la creazione.

AWS CLI

Per integrare un chatbot utilizzando ilAWS CLI

1. Per integrare il tuo chatbot con Amazon Chime, usa ilcreate-botcomando inAWS CLI.

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

   a. Inserisci un nome visualizzato dal chatbot composto da un massimo di 55 caratteri alfanumerici o speciali (ad esempio +, -,%).

   b. Inserisci il nome di dominio registrato per il tuo account Amazon Chime Enterprise.

2. Amazon Chime restituisce una risposta che include l'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. Copia e salva l'ID del bot e l'indirizzo e-mail del bot da utilizzare nelle seguenti procedure.

API Amazon Chime

Per integrare un chatbot utilizzando l'API Amazon Chime

1. Per integrare il tuo chatbot con Amazon Chime, usa ilCreateBotFunzionamento API inRiferimento API Amazon Chime.

   a. Inserisci un nome visualizzato dal chatbot composto da un massimo di 55 caratteri alfanumerici o speciali (ad esempio +, -,%).

   b. Inserisci il nome di dominio registrato per il tuo account Amazon Chime Enterprise.

2. Amazon Chime restituisce una risposta che include l'ID bot. Copia e salva l'ID del bot e l'indirizzo e-mail. L'indirizzo email del bot ha il seguente aspetto:*exampleBot*-chimebot@*example.com*.

SDK AWS per Java

Il codice di esempio seguente mostra come integrare un chatbot utilizzando ilAWSSDK per Java.

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

chime.createBot(createBotRequest);
```

Amazon Chime restituisce una risposta che include l'ID bot. Copia e salva l'ID del bot e l'indirizzo e-mail. L'indirizzo email del bot ha il seguente aspetto:*exampleBot*-chimebot@*example.com*.

Fase 2: configurare l'endpoint DLQ per un chatbot Amazon Chime

Dopo aver creato un ID chatbot per il tuo account Amazon Chime Enterprise, configura l'endpoint in uscita per Amazon Chime da utilizzare per inviare messaggi al bot. L'endpoint in uscita può essere unAWS Lambdafunzione ARN o un endpoint HTTPS creato come parte diprerequisiti. Per ulteriori informazioni su Lambda, consulta la Guida per gli sviluppatori di AWS Lambda.

> **Note**
>
> Se l'endpoint HTTPS in uscita per il bot non è configurato o è vuoto, gli amministratori della chat room non possono aggiungere il bot a una chat room. Inoltre, gli utenti della chat room non possono interagire con il bot.

AWS CLI

Per configurare un endpoint in uscita per il tuo chatbot, usa ilput-events-configurationcomando inAWS CLI. Configura una funzione Lambda ARN o un endpoint HTTPS in uscita.

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 risponde con l'ID bot e l'endpoint HTTPS.

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

API Amazon Chime

Per configurare l'endpoint in uscita per il tuo chatbot, usa Amazon ChimePutEventsConfigurationFunzionamento API inRiferimento API Amazon Chime. Configura una funzione Lambda ARN o un endpoint HTTPS in uscita.

- Se si configura una funzione Lambda ARN— Amazon Chime chiama Lambda per aggiungere l'autorizzazione e consentire all'amministratore di Amazon ChimeAWSaccount per richiamare la funzione Lambda ARN fornita. Segue una chiamata DLQ per verificare che Amazon Chime sia autorizzato a richiamare la funzione. Se l'aggiunta delle autorizzazioni fallisce o se la chiamata dry run fallisce, allora`PutEventsConfiguration`la richiesta restituisce un errore HTTP 4xx.
- Se configuri un endpoint HTTPS in uscita— Amazon Chime verifica il tuo endpoint inviando una richiesta HTTP Post con un payload JSON Challenge all'endpoint HTTPS in uscita fornito nel passaggio precedente. L'endpoint HTTPS in uscita deve rispondere eseguendo l'echoing del parametro Challenge in formato JSON. I seguenti esempi mostrano la richiesta e una risposta valida.

Request

```
HTTPS POST

JSON Payload:
{
   "Challenge":"0000000000000000000",
   "EventType" : "HTTPSEndpointVerification"
}
```

Response

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

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

Se l'handshake Challenge ha esito negativo, la richiesta `PutEventsConfiguration` restituisce un errore HTTP 4xx.

SDK AWS per Java

Il seguente codice di esempio mostra come configurare un endpoint utilizzando ilAWSSDK per 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):
```

Passaggio 3: aggiungi il chatbot a una chat room di Amazon Chime

Solo un amministratore di una chat room può aggiungere un chatbot a una chat room. Usano l'indirizzo email del chatbot creato inFase 1:.

Per aggiungere una chatbot a una chat room

1. Apri il client desktop o l'applicazione Web Amazon Chime.
2. Scegli l'icona DLQ e scegliGestisci webhook e bot.
3. Scegli Add bot (Aggiungi bot).
4. PerIndirizzo e-mail, inserisci l'indirizzo email del bot.
5. Scegli Add (Aggiungi).

Il nome del bot compare nel registro della chat room. Se sono necessarie azioni aggiuntive per aggiungere un chatbot a una chat room, fornisci le azioni all'amministratore della chat room.

Dopo aver aggiunto il chatbot alla chat room, fornisci i comandi del chatbot agli utenti della chat room. Un modo per farlo è programmare il chatbot in modo che invii il comando help alla chat room quando riceve l'invito alla chat room. AWS consiglia inoltre di creare un comando di aiuto da utilizzare per gli utenti del chatbot.

Autentica le richieste DLQ

Puoi autenticare le richieste inviate al tuo chatbot da una chat room di Amazon Chime. A tale scopo, calcola una firma in base alla richiesta. Quindi, verifica che la firma calcolata corrisponda a quella nell'intestazione della richiesta. Amazon Chime utilizza l'hash HMAC SHA256 per generare la firma.

Se il tuo chatbot è configurato per Amazon Chime utilizzando un endpoint HTTPS in uscita, utilizza i seguenti passaggi di autenticazione.

Per convalidare una richiesta firmata da Amazon Chime per un chatbot con un endpoint HTTPS in uscita configurato

1. Ottenere l’intestazione Chime-Signature dalla richiesta HTTP.
2. Ottenere l'intestazione Chime-Request-Timestamp e il body (corpo) della richiesta. Quindi, utilizzare una barra verticale come delimitatore tra i due elementi per creare una stringa.
3. Usa ilSecurityTokendal CreateBot risposta come chiave iniziale diHMAC_SHA_256ed esegui l'hash della stringa creata nel passaggio 2.

4. Codificare il byte con hash con un encoder Base64 in una stringa di firma.
5. Confrontare questa firma elaborata con quella nell'intestazione Chime-Signature.

Il codice di esempio seguente spiega come generare una firma utilizzando 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;
               }
        }
```

L'endpoint HTTPS in uscita deve rispondere alla richiesta Amazon Chime con`200 OK`entro 2 secondi. In caso contrario, la richiesta ha esito negativo. Se l'endpoint HTTPS in uscita non è disponibile dopo 2 secondi, probabilmente a causa di un timeout di connessione o lettura, o se Amazon Chime riceve un codice di risposta 5xx, Amazon Chime ritenta la richiesta due volte. Il primo tentativo viene inviato 200 millisecondi dopo che la richiesta iniziale ha esito negativo. Il primo tentativo viene inviato 400 millisecondi dopo che la richiesta precedente ha esito negativo. Se l'endpoint HTTPS in uscita non è ancora disponibile dopo il secondo tentativo, la richiesta ha esito negativo.

> **Note**
>
> Il Chime-Request-Timestamp cambia ogni volta che la richiesta viene rieseguita.

Se il tuo chatbot è configurato per Amazon Chime utilizzando una funzione Lambda ARN, utilizza i seguenti passaggi di autenticazione.

Per convalidare una richiesta firmata da Amazon Chime per un chatbot con una funzione Lambda (ARN configurato):

1. Ottieni iFirma DLQeChime-Request-Timestampdalla richiesta LambdaClientContext, in formato JSON con codifica Base64.

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

2. Ottenere il body (corpo) della richiesta dal payload della richiesta.
3. Usa ilSecurityTokendal`CreateBot`risposta come chiave iniziale diHMAC_SHA_256e esegui l'hash della stringa che hai creato.
4. Codificare il byte con hash con un encoder Base64 in una stringa di firma.
5. Confrontare questa firma elaborata con quella nell'intestazione Chime-Signature.

Se un`com.amazonaws.SdkClientException`si verifica durante la chiamata Lambda, Amazon Chime ritenta la richiesta due volte.

Aggiorna i chatbot

In qualità di amministratore dell'account Amazon Chime, puoi utilizzare l'API Amazon Chime conAWSSDK oAWS CLIper visualizzare i dettagli del tuo chatbot. Puoi anche abilitare o impedire che i chatbot vengano utilizzati nel tuo account. Puoi anche rigenerare i token di sicurezza per il tuo chatbot.

Per ulteriori informazioni, consultare i seguenti argomenti nellaRiferimento API Amazon Chime:

- GetBot— Ottiene i dettagli del chatbot, come l'indirizzo email e il tipo di bot.

- UpdateBot— Abilita o impedisce l'utilizzo di un chatbot nel tuo account.
- RegenerateSecurityToken— Rigenera il token di sicurezza per il tuo chatbot.

Puoi anche modificare i`PutEventsConfiguration`per il tuo chatbot. Ad esempio, se il chatbot era inizialmente configurato per utilizzare un endpoint HTTPS in uscita, puoi eliminare la configurazione degli eventi precedente e inserire una nuova configurazione degli eventi per un ARN della funzione Lambda.

Per ulteriori informazioni, consultare i seguenti argomenti nellaRiferimento API Amazon Chime:

- DeleteEventsConfiguration
- PutEventsConfiguration

Eventi Amazon Chime inviati ai chatbot

I seguenti eventi vengono inviati al tuo chatbot da Amazon Chime:

- Invita— Inviato quando il tuo chatbot viene aggiunto a una chat room di Amazon Chime
- Menzione— Inviato quando un utente in una chat room @mentions è il tuo chatbot
- Rimuovi— Inviato quando il chatbot viene rimosso da una chat room di Amazon Chime

Gli esempi seguenti mostrano il payload JSON inviato al tuo chatbot per ciascuno di questi eventi.

Example : Invita un evento

```
{
  "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 : Evento di menzione

```
            {
                "Sender": {
                            "SenderId": "user@example.com",
                            "SenderIdType": "EmailId"
                          },
                "Discussion": {
                                "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                                "DiscussionType": "Room"
                              },
                "EventType": "Mention",
                "InboundHttpsEndpoint": {
                                            "EndpointType": "ShortLived",
                                            "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                        },
                "EventTimestamp": "2019-04-04T21:30:43.181Z",
                "Message": "@botDisplayName@example.com Hello Chatbot"
            }
```

> **Note**
>
> L'URL `InboundHttpsEndpoint` per un evento Mention scade 2 minuti dopo l'invio.

Example : Rimuovi evento

```
            {
                "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"
    }
```

Creazione di webhook per Amazon Chime

I webhook consentono alle applicazioni Web di comunicare tra loro in tempo reale. In genere, i webhook inviano notifiche quando si verifica un'azione. Ad esempio, supponiamo che tu gestisca un sito di shopping online. I webhook possono avvisarti quando un cliente aggiunge articoli a un carrello, paga un ordine o invia un commento. I webhook non richiedono tanta programmazione come le applicazioni tradizionali e non utilizzano la stessa potenza di elaborazione. Senza un webhook, un programma deve interrogare frequentemente i dati per ottenerli in tempo reale. Con un webhook, l'applicazione di invio pubblica immediatamente i dati.

I webhook in entrata che crei possono inviare messaggi a livello di programmazione alle chat room di Amazon Chime. Ad esempio, un webhook può notificare a un team del servizio clienti la creazione di un nuovo ticket ad alta priorità e aggiungere un link al ticket nella chat room.

I messaggi Webhooks possono essere formattati con Markdown e possono includere emoji. I collegamenti HTTP e gli indirizzi e-mail vengono visualizzati come collegamenti attivi. I messaggi possono anche includere annotazioni @All e @Present per avvisare rispettivamente tutti i membri e quelli presenti della chat room. Per @rivolgervi direttamente a un partecipante della chat room, utilizzate il loro alias o l'indirizzo e-mail completo. Ad esempio, `@alias` o `@alias@domain.com`.

I webhook possono solo far parte di una chat room e non possono essere condivisi. Gli amministratori delle chat room di Amazon Chime possono aggiungere fino a 10 webhook per ogni chat room.

Dopo aver creato un webhook, puoi integrarlo con una chat room di Amazon Chime, come illustrato nella procedura seguente.

Per integrare un webhook con una chat room

1. Ottieni l'URL del webhook dall'amministratore della chat room. Per ulteriori informazioni, vedereAggiungere webhook a una chat roomnelGuida per l'utente di Amazon Chime.
2. Usa l'URL del webhook nello script o nell'applicazione che hai creato per inviare messaggi alla chat room:

   a. L'URL accetta una richiesta HTTP POST.

   b. I webhook di Amazon Chime accettano un payload JSON con una sola chiaveContenuto. Di seguito è riportato un esempio di comando curl con un payload di esempio:

   ```
   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"}'
   ```

   Di seguito è riportato un esempioPowerShellcomando per utenti 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"}'
   ```

Dopo che il programma esterno invia la richiesta HTTP POST all'URL del webhook, il server conferma che il webhook è valido e che ha una chat room assegnata. Il webhook viene visualizzato nel registro della chat room con un'icona webhook accanto al nome. I messaggi della chat room inviati dal webhook vengono visualizzati nella chat room sotto il nome del webhook seguito da (Webhook).

> **Note**
>
> CORS non è attualmente abilitato per i webhook.

Risoluzione degli errori del webhook

Di seguito è riportato un elenco di errori correlati ai webhook:

- Il limite di velocità dei webhook in ingresso è di 1 TPS per chat room. Il throttling genera un errore HTTP 429.
- I messaggi pubblicati da un webhook devono essere al massimo di 4 KB. Un payload del messaggio più grande genera un errore HTTP 413.
- I messaggi pubblicati da un webhook con annotazioni @Tutti e @Present funzionano solo per chat con un massimo di 50 membri. Più di 50 membri generano un errore HTTP 400.
- Se l'URL del webhook viene rigenerato, l'utilizzo del vecchio URL genera un errore HTTP 404.
- Se il webhook in una chat room viene eliminato, l'utilizzo del vecchio URL genera un errore HTTP 404.
- Gli URL non validi dei webhook generano errori HTTP 403.
- Se il servizio non è disponibile, l'utente riceve un errore HTTP 503 nella risposta.

Supporto amministrativo per Amazon Chime

> **Note**
>
> Per ricevere assistenza con il tuo account Amazon Shopping, vai al Servizio clienti su amazon.com.

Se devi contattare l'assistenza per Amazon Chime, scegli una delle seguenti opzioni:

- Se disponi di un account di AWS supporto, vai al Centro assistenza e invia un ticket.
- Altrimenti, apri AWS Management Consolee scegli Amazon Chime, Support, Invia richiesta.

Fornisci quante più informazioni possibili tra le seguenti:

- Una descrizione dettagliata del problema.
- L'ora in cui si è verificato il problema, compreso il fuso orario.
- La tua versione di Amazon Chime. Per trovare il numero di versione:
  - In Windows, scegli Aiuto, Informazioni su Amazon Chime.
  - In macOS, scegli Amazon Chime, About Amazon Chime (Informazioni su Amazon Chime).
  - In iOS e Android, scegli Settings (Impostazioni), About (Informazioni su).
- L'ID di riferimento del log. Per trovare questo ID:
  - In Windows e macOS, scegli Help (Aiuto), Send Diagnostic Logs (Invia log diagnostica).
  - In iOS e Android, scegli Settings (Impostazioni), Send Diagnostic Logs (Invia log diagnostica).
- Se il problema è correlato a una riunione, l'ID della riunione.

Sicurezza in Amazon Chime

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon Chime, consulta AWS Services in Scope by Compliance Program AWS Services in Scope Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Chime. I seguenti argomenti mostrano come configurare Amazon Chime per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi AWS che ti aiutano a monitorare e proteggere le tue risorse Amazon Chime.

Argomenti

- Registrazione e monitoraggio in Amazon Chime ime
- Convalida della conformità per Amazon Chime
- Resilienza in Amazon Chime
- Sicurezza dell'infrastruttura in Amazon Chime
- Informazioni sugli aggiornamenti automatici di Amazon Chime

Gestione delle identità e degli accessi per Amazon Chime

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon Chime. IAM è un programma Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon Chime.

Utente del servizio: se utilizzi il servizio Amazon Chime per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon Chime per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon Chime, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Chime

Amministratore del servizio: se sei responsabile delle risorse Amazon Chime della tua azienda, probabilmente hai pieno accesso ad Amazon Chime. È tuo compito determinare a quali funzionalità e risorse di Amazon Chime devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni

contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon Chime, consulta. Come funziona Amazon Chime con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso ad Amazon Chime. Per visualizzare esempi di policy basate sull'identità di Amazon Chime che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità di Amazon Chime

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

AWS account utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per

ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore

IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

AWS politiche gestite per Amazon Chime

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere autonomamente le policy. La creazione di policy gestite dai clienti IAM

che forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso più comuni e sono disponibili nel tuo account AWS . Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy AWS gestita di ReadOnlyAccess fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio avvia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi

limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Chime con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon Chime, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Amazon Chime. Per avere una visione di alto livello di come Amazon Chime e AWS altri servizi funzionano con IAM, AWS consulta i servizi che funzionano con IAM nella IAM User Guide.

Argomenti

- Politiche basate sull'identità di Amazon Chime
- Risorse
- Esempi

Politiche basate sull'identità di Amazon Chime

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Amazon Chime supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Chiavi di condizione

Amazon Chime non fornisce chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione globali di AWS , consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente IAM.

Risorse

Amazon Chime non supporta la specificazione di ARN di risorse in una policy.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Amazon Chime, consulta. Esempi di policy basate sull'identità di Amazon Chime

Prevenzione del problema "confused deputy" tra servizi

Il problema del vicesceriffo è un problema di sicurezza delle informazioni che si verifica quando un'entità senza l'autorizzazione a eseguire un'azione chiama un'entità con più privilegi a eseguire

l'azione. Ciò può consentire ai malintenzionati di eseguire comandi o modificare risorse che altrimenti non avrebbero l'autorizzazione a eseguire o a cui non avrebbero accesso. Per ulteriori informazioni, vedere Il problema del deputato confuso nella Guida AWS Identity and Access Management per l'utente.

Nel AWS, l'impersonificazione tra servizi può portare a uno scenario sostitutivo confuso. L'impersonificazione tra servizi si verifica quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Un malintenzionato può utilizzare il servizio di chiamata per modificare le risorse di un altro servizio utilizzando autorizzazioni che normalmente non avrebbe.

AWS fornisce ai responsabili del servizio l'accesso gestito alle risorse del vostro account per aiutarvi a proteggere la sicurezza delle vostre risorse. Ti consigliamo di utilizzare la chiave `aws:SourceAccount` Global Condition Context nelle tue politiche relative alle risorse. Queste chiavi limitano le autorizzazioni che Amazon Chime concede a un altro servizio per quella risorsa.

L'esempio seguente mostra una policy sui bucket S3 che utilizza la chiave `aws:SourceAccount` global condition context nel bucket `CallDetailRecords` S3 configurato per evitare il confuso problema del vice.

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

Politiche basate sulle risorse di Amazon Chime

Amazon Chime non supporta politiche basate sulle risorse.

Autorizzazione basata sui tag Amazon Chime

Amazon Chime non supporta l'etichettatura delle risorse o il controllo dell'accesso in base ai tag.

Ruoli IAM di Amazon Chime

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon Chime

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Puoi ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo Token. GetFederation

Amazon Chime supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi che completano azioni per tuo conto. I ruoli collegati ai servizi vengono visualizzati nel tuo account IAM e i servizi possiedono i ruoli. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Amazon Chime supporta i ruoli collegati ai servizi. Per dettagli sulla creazione o la gestione di ruoli collegati ai servizi Amazon Chime, consulta. Utilizzo di ruoli collegati ai servizi per Amazon Chime

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Amazon Chime non supporta i ruoli di servizio.

Esempi di policy basate sull'identità di Amazon Chime

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse Amazon Chime. Inoltre, non possono eseguire attività utilizzando l' AWS API AWS Management Console AWS CLI, o. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consultare Creazione di policy nella scheda JSON nella Guida per l'utente di IAM.

Argomenti

- Best practice delle policy
- Utilizzo della console Amazon Chime
- Consenti agli utenti l'accesso completo ad Amazon Chime
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Consentire agli utenti di accedere alle operazioni di gestione degli utenti
- AWS politica gestita: AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- Amazon Chime aggiorna le politiche gestite AWS

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon Chime nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Amazon Chime

Per accedere alla console Amazon Chime, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon Chime nel AWS tuo account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che tali entità possano ancora utilizzare la console Amazon Chime, allega anche la seguente AmazonChimeReadOnlypolitica AWS gestita alle entità. Per ulteriori informazioni, consulta la sezione Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM:

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

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che si sta cercando di eseguire.

Consenti agli utenti l'accesso completo ad Amazon Chime

La seguente AmazonChimeFullAccesspolicy AWS gestita garantisce a un utente IAM l'accesso completo alle risorse di Amazon Chime. La policy consente all'utente di accedere a tutte le operazioni di Amazon Chime, nonché ad altre operazioni che Amazon Chime deve essere in grado di eseguire per tuo conto.

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

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o in modo programmatico. 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": "*"
        }
    ]
}
```

Consentire agli utenti di accedere alle operazioni di gestione degli utenti

Utilizza la AmazonChimeUserManagementpolicy AWS gestita per concedere agli utenti l'accesso alle azioni di gestione degli utenti nella console Amazon Chime.

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

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

AWS politica gestita: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`Consente ad Amazon Chime Voice Connectors di trasmettere contenuti multimediali su Amazon Kinesis Video Streams, fornire notifiche di streaming e sintetizzare il parlato utilizzando Amazon Polly. Questa politica concede al servizio Amazon Chime Voice Connector le autorizzazioni per accedere ad Amazon Kinesis Video Streams del cliente, inviare eventi di notifica ad Amazon Simple Notification Service e Amazon Simple Queue Service e utilizzare Amazon Polly per sintetizzare la voce quando si utilizzano le applicazioni e le azioni vocali Amazon Chime SDK. `Speak` `SpeakAndGetDigits` Per ulteriori informazioni, consulta gli esempi di policy basate sull'identità di Amazon Chime SDK nella Amazon Chime SDK Administrator Guide.

Amazon Chime aggiorna le politiche gestite AWS

La tabella seguente elenca e descrive gli aggiornamenti apportati alla policy IAM di Amazon Chime.

Modifica	Descrizione	Data
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` : aggiornamento a una policy esistente	Amazon Chime Voice Connectors ha aggiunto nuove autorizzazioni per consentirti di utilizzare Amazon Polly per sintetizzare il parlato. Queste autorizzazioni sono necessarie per utilizzare le azioni `Speak` e `SpeakAndGetDigits` nelle applicazioni vocali SDK di Amazon Chime.	15 marzo 2022
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` : aggiornamento a una policy esistente	Amazon Chime Voice Connector ha aggiunto nuove autorizzazioni per consentire l'accesso ad Amazon Kinesis Video Streams e inviare eventi di notifica a SNS e SQS. Queste autorizzazioni sono necessarie per Amazon Chime Voice Connectors per trasmettere contenuti multimediali su Amazon Kinesis Video Streams e fornire notifiche di streaming.	20 dicembre 2021
Modifica alla politica esistente. Creazione di utenti o ruoli IAM con la policy Chime SDK.	Amazon Chime ha aggiunto nuove azioni per supportare una convalida estesa. Sono state aggiunte diverse azioni per consentire l'elenco e l'etichettatura dei partecipanti	23 settembre 2021

Modifica	Descrizione	Data
	e delle risorse per le riunioni e per avviare e interrompere la trascrizione delle riunioni.	
Amazon Chime ha iniziato a tracciare le modifiche	Amazon Chime ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	23 settembre 2021

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Chime

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Chime e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Amazon Chime

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `chime:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `chime:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Chime.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Chime. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Chime

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Chime supporta queste funzionalità, consulta. Come funziona Amazon Chime con IAM

- Per sapere come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Utilizzo di ruoli collegati ai servizi per Amazon Chime

Amazon Chime utilizza ruoli collegati ai serviziAWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Amazon Chime. I ruoli collegati ai servizi sono definiti automaticamente da Amazon Chime e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altriAWS servizi per conto dell'utente.

Un ruolo collegato ai servizi semplifica la configurazione di Amazon Chime perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Amazon Chime definisce le autorizzazioni del ruolo collegato ai servizi e, salvo diversamente definito, solo Amazon Chime può assumerne il ruolo. Le autorizzazioni definite includono policy di trust e di autorizzazioni. Le policy di autorizzazioni non possono essere collegate a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Amazon Chime perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS supportati da IAM. Cerca i servizi che hanno Sì nella colonna Service-Linked Role (Ruolo collegato ai servizi). Scegli Yes (Sì) in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- Utilizzo dei ruoli con dispositivi Alexa for Business condivisi
- Utilizzo dei ruoli con trascrizione in tempo reale

- Utilizzo dei ruoli con le pipeline multimediali di Amazon Chime SDK

Utilizzo dei ruoli con dispositivi Alexa for Business condivisi

Le informazioni nelle sezioni seguenti spiegano come utilizzare i ruoli collegati ai servizi e concedere ad Amazon Chime l'accesso alle risorse Alexa for Business nel tuoAWS account.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per Amazon Chime
- Creazione di un ruolo collegato ai servizi per Amazon Chime
- Modifica di un ruolo collegato ai servizi per Amazon Chime
- Eliminazione di un ruolo collegato ai servizi per Amazon Chime
- Regioni supportate per i ruoli collegati ai servizi di Amazon Chime

Autorizzazioni del ruolo collegato ai servizi per Amazon Chime

Amazon Chime utilizza il ruolo collegato ai servizi denominato AWSServiceRoleForAmazonChime: consente l'accesso aiAWS servizi e alle risorse utilizzati o gestiti da Amazon Chime, ad esempio i dispositivi condivisi Alexa for Business.

Ai fini dell' AWSServiceRoleForAmazonChime assunzione del ruolo, il ruolo collegato ai servizi considera attendibili i seguenti servizi:

- `chime.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Amazon Chime di eseguire le seguenti operazioni sulla risorsa specificata:

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

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon Chime

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando Alexa for Business automaticamente ilAWS Management Console Amazon Chime collegato ai servizi per tuo conto.AWS CLIAWS

Puoi utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il caso d'uso Amazon Chime. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `chime.amazonaws.com`. Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per Amazon Chime

Amazon Chime non consente di modificare il ruolo AWSServiceRoleForAmazonChime collegato ai servizi. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Amazon Chime

Se non occorre più utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare tale ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo.

> **Note**
>
> Se Amazon Chime sta utilizzando il ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non riesca. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Amazon Chime utilizzate dalla AWSServiceRoleForAmazonChime (console)

- Disattiva Alexa for Business per tutti i dispositivi condivisi nel tuo account Amazon Chime.

a. Apri la console Amazon Chime all'indirizzo https://chime.aws.amazon.com/.
b. Scegli Users (Utenti), Shared devices (Dispositivi condivisi).
c. Seleziona un dispositivo.
d. Scegli Actions (Azioni).
e. Scegli Disabilita Alexa for Business.

Eliminazione manuale del ruolo collegato ai servizi

Utilizzare la console IAM, AWS CLI, la AWS o l'API per eliminare i ruoli collegati ai servizi AWSServiceRoleForAmazonChime. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Amazon Chime

Amazon Chime supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote di Amazon Chime.

Utilizzo dei ruoli con trascrizione in tempo reale

Le informazioni nelle seguenti sezioni spiegano come creare un ruolo collegato ai servizi per la trascrizione in tempo reale di Amazon Chime. Per ulteriori informazioni sul servizio di trascrizione in tempo reale, consulta Utilizzo della trascrizione in tempo reale di Amazon Chime SDK.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per la trascrizione di Amazon Chime
- Creazione di un ruolo collegato ai servizi per la trascrizione di Amazon Chime
- Modifica di un ruolo collegato ai servizi per la trascrizione di Amazon Chime
- Eliminazione di un ruolo collegato ai servizi per la trascrizione di Amazon Chime
- Regioni supportate per i ruolo collegato ai servizi di Amazon Chime

Autorizzazioni del ruolo collegato ai servizi per la trascrizione di Amazon Chime

Amazon Chime Live Transcription utilizza un ruolo collegato al servizio denominato AWSServiceRoleForAmazonChimeTranscription: consente ad Amazon Chime di accedere ad Amazon Transcribe e Amazon Transcribe Medical per tuo conto.

Ai fini dell' AWSServiceRoleForAmazonChimeTranscription assunzione del ruolo, il ruolo collegato ai servizi considera attendibili i seguenti servizi:

- `transcription.chime.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Amazon Chime di eseguire le seguenti operazioni sulle risorse seguenti:

- Operazione: `transcribe:StartStreamTranscription` su `all AWS resources`
- Operazione: `transcribe:StartMedicalStreamTranscription` su `all AWS resources`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per la trascrizione di Amazon Chime

Puoi utilizzare la console IAM per creare un ruolo collegato ai servizi con il caso d'uso Chime Transcription.

> **Note**
>
> Devi disporre delle autorizzazioni amministrative IAM per completare questi passaggi. In caso contrario, contatta un amministratore di sistema.

Come creare il ruolo

1. Registrarsi alla Console di gestione di AWS e aprire la console di IAM alla pagina https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Ruoli, quindi Crea ruolo,
3. Scegli il tipo di ruolo del servizio AWS, quindi scegli Chime, quindi scegli Chime Transcription.
4. Seleziona Successivo.
5. Seleziona Successivo.
6. Modifica la descrizione secondo necessità, quindi scegli Crea ruolo.

Per creare un ruolo collegato ai servizi, è possibile utilizzare l'AWSAPIAWS CLI o l'API.

Nella CLI, esegui questo comando:`aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per la trascrizione di Amazon Chime

Amazon Chime non consente di modificare il ruolo AWSServiceRoleForAmazonChimeTranscription collegato ai servizi. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché potrebbero farvi riferimento varie entità. Per modificare la descrizione del ruolo, è possibile utilizzare IAM per modificare la descrizione del ruolo. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per la trascrizione di Amazon Chime

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi AWSServiceRoleForAmazonChimeTranscription. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruolo collegato ai servizi di Amazon Chime

Amazon Chime supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote Amazon Chime e Utilizzo delle regioni multimediali Amazon Chime SDK.

Utilizzo dei ruoli con le pipeline multimediali di Amazon Chime SDK

Le informazioni nelle seguenti sezioni spiegano come creare e gestire un ruolo collegato ai servizi per Amazon Chime SDK Media Pipelines.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK
- Creazione di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK

- Modifica di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK
- Eliminazione di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK
- Regioni supportate per i ruoli collegati ai servizi delle pipeline multimediali di Amazon Chime

Autorizzazioni del ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK

Amazon Chime utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonChimeSDKMediaPipelines: consente alle pipeline multimediali Amazon Chime SDK di accedere alle riunioni Amazon Chime SDK per tuo conto.

Ai fini dell' AWSServiceRoleForAmazonChimeSDKMediaPipelines assunzione del ruolo, il ruolo collegato ai servizi considera attendibili i seguenti servizi:

- `mediapipelines.chime.amazonaws.com`

Il ruolo consente ad Amazon Chime di eseguire le seguenti operazioni sulle risorse specificate:

- Operazione: `chime:CreateAttendee` su `all AWS resources`
- Operazione: `chime:DeleteAttendee` su `all AWS resources`
- Operazione: `chime:GetMeeting` su `all AWS resources`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK

Utilizzi la console IAM per creare un ruolo collegato ai servizi con il caso d'uso Amazon Chime SDK Media Pipelines*.

> **Note**
>
> Devi disporre delle autorizzazioni amministrative IAM per completare questi passaggi. In caso contrario, contatta un amministratore di sistema.

Come creare il ruolo

1. Registrarsi alla Console di gestione di AWS e aprire la console di IAM alla pagina https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Ruoli, quindi Crea ruolo.
3. Scegli il tipo di ruolo di AWSservizio, quindi scegli Chime, quindi scegli Chime SDK Media Pipelines.
4. Seleziona Successivo.
5. Seleziona Successivo.
6. Modifica la descrizione secondo necessità, quindi scegli Crea ruolo.

Puoi utilizzare l'APIAWS CLI o l'AWSAPI per creare un ruolo collegato ai servizi denominato mediapipelines.chime.amazonaws.com.

NelAWS CLI, esegui questo comando:`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK

Amazon Chime non consente di modificare il ruolo AWSServiceRoleForAmazonChimeSDKMediaPipelines collegato ai servizi. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per le pipeline multimediali di Amazon Chime SDK

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi AWSServiceRoleForAmazonChimeSDKMediaPipelines. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi delle pipeline multimediali di Amazon Chime

Amazon Chime SDK supporta l'utilizzo di ruoli collegati ai servizi in tutte leAWS regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote di Amazon Chime.

Registrazione e monitoraggio in Amazon Chime ime

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Amazon Chime e delle tue altreAWS soluzioni. AWSfornisce i seguenti strumenti per monitorare Amazon Chime ime, segnalare i problemi e intervenire automaticamente quando necessario:

- Amazon CloudWatch monitora in tempo reale leAWS risorse e le applicazioni che esegui suAWS. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi impostare perché CloudWatch tenga traccia dell'uso della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.
- Amazon EventBridge fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche nelleAWS risorse. EventBridge consente il calcolo automatizzato basato sugli eventi. Puoi scrivere le regole che controllano determinati eventi e attivano operazioni automatiche in altri servizi AWS quando tali eventi si verificano. Per ulteriori informazioni, consulta la Guida per EventBridge l'utente di Amazon.
- Amazon CloudWatch Logs consente di monitorare, archiviare e accedere ai file di log da istanze Amazon EC2 e da altre origini. CloudTrail CloudWatch I log possono monitorare le informazioni nei file di log e notificare quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Guida per l'utente CloudWatch di Amazon Logs.
- AWS CloudTrail acquisisce chiamate API ed eventi correlati da parte di o per conto di un account AWS. Distribuisce quindi i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le

chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoraggio di Amazon Chime con Amazon CloudWatch

Puoi monitorare Amazon Chime ime CloudWatch, che raccoglie i dati grezzi e li elabora trasformandoli in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Guida per CloudWatch l'utente di Amazon.

CloudWatch parametri per Amazon Chime per Amazon Chime per Amazon Chime

Amazon Chime ime invia i parametri seguenti a CloudWatch.

llAWS/ChimeVoiceConnector namespace include le seguenti metriche per i numeri di telefono assegnati al tuoAWS account e ai connettori vocali Amazon Chime.

Parametro	Descrizione
InboundCallAttempts	Il numero di chiamate in entrata tentate. Unità: numero
InboundCallFailures	Il numero di chiamate in entrata non riuscite. Unità: numero
InboundCallsAnswered	Il numero di chiamate in entrata con risposta. Unità: numero

Parametro	Descrizione
`InboundCallsActive`	Il numero di chiamate in entrata attualmente attive. Unità: numero
`OutboundCallAttempts`	Il numero di chiamate in uscita tentate. Unità: numero
`OutboundCallFailures`	Il numero di chiamate in uscita non riuscite. Unità: numero
`OutboundCallsAnswered`	Il numero di chiamate in uscita con risposta. Unità: numero
`OutboundCallsActive`	Il numero di chiamate in uscita attualmente attive. Unità: numero
`Throttles`	Il numero di volte in cui l'account viene limitato quando si tenta di effettuare una chiamata. Unità: numero
`Sip1xxCodes`	Il numero di messaggi SIP con codici di stato 1xx-level. Unità: numero
`Sip2xxCodes`	Il numero di messaggi SIP con codici di stato 2xx-level. Unità: numero

Parametro	Descrizione
`Sip3xxCodes`	Il numero di messaggi SIP con codici di stato 3xx-level. Unità: numero
`Sip4xxCodes`	Il numero di messaggi SIP con codici di stato 4xx-level. Unità: numero
`Sip5xxCodes`	Il numero di messaggi SIP con codici di stato 5xx-level. Unità: numero
`Sip6xxCodes`	Il numero di messaggi SIP con codici di stato 6xx-level. Unità: numero
`CustomerToVcRtpPackets`	Il numero di pacchetti RTP inviati dal cliente all'infrastruttura Amazon Chime Voice Connector. Unità: numero
`CustomerToVcRtpBytes`	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime ime in pacchetti RTP. Unità: numero
`CustomerToVcRtcpPackets`	Il numero di pacchetti RTCP inviati dal cliente all'infrastruttura Amazon Chime Voice Connector. Unità: numero

Parametro	Descrizione
`CustomerToVcRtcpBytes`	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime. Unità: numero
`CustomerToVcPacketsLost`	Il numero di pacchetti persi durante il trasporto dal cliente all'infrastruttura Amazon Chime Voice Connector. Unità: numero
`CustomerToVcJitter`	Il jitter medio dei pacchetti inviati dal cliente all'infrastruttura Amazon Chime Voice Connector. Unità: microsecondi
`VcToCustomerRtpPackets`	Il numero di pacchetti RTP inviati dall'infr astruttura Amazon Chime Voice Connector al cliente. Unità: numero
`VcToCustomerRtpBytes`	Numero di connettori Amazon Chime ime Conime al cliente in pacchetti RTP. Unità: numero
`VcToCustomerRtcpPackets`	Il numero di pacchetti RTCP inviati dall'infr astruttura Amazon Chime Voice Connector al cliente. Unità: numero

Parametro	Descrizione
VcToCustomerRtcpBytes	Numero di connettori Amazon Chime ime Conime al cliente in pacchetti RTCime al cliente in pacchetti RTCime in pacchetti RTCime al connettore Amazon Chime Conime al cliente in pacchetti RTCime. Unità: numero
VcToCustomerPacketsLost	Il numero di pacchetti persi durante il transito dall'infrastruttura Amazon Chime Voice Connector al cliente. Unità: numero
VcToCustomerJitter	Il jitter medio dei pacchetti inviati dall'infr astruttura Amazon Chime Voice Connector al cliente. Unità: microsecondi
RTTBetweenVcAndCustomer	Il tempo medio di andata e ritorno tra il cliente e l'infrastruttura Amazon Chime Voice Connector. Unità: microsecondi
MOSBetweenVcAndCustomer	Il punteggio medio di opinione (MOS) stimato associato ai flussi vocali tra il cliente e l'infrast ruttura Amazon Chime Voice Connector. Unità: Punteggio tra 1.0-4.4. Un punteggio più alto indica una migliore qualità audio percepita.
RemoteToVcRtpPackets	Il numero di pacchetti RTP inviati dall'estremità remota all'infrastruttura Amazon Chime Voice Connector. Unità: numero

Parametro	Descrizione
`RemoteToVcRtpBytes`	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime ime ime ime in pacchetti RTP. Unità: numero
`RemoteToVcRtcpPackets`	Il numero di pacchetti RTCP inviati dall'estr emità remota all'infrastruttura Amazon Chime Voice Connector. Unità: numero
`RemoteToVcRtcpBytes`	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime. Unità: numero
`RemoteToVcPacketsLost`	Il numero di pacchetti persi durante il transito dall'estremità remota all'infrastruttura Amazon Chime Voice Connector. Unità: numero
`RemoteToVcJitter`	Il jitter medio dei pacchetti inviati dall'estremità remota all'infrastruttura Amazon Chime Voice Connector. Unità: microsecondi
`VcToRemoteRtpPackets`	Il numero di pacchetti RTP inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota. Unità: numero

Parametro	Descrizione
`VcToRemoteRtpBytes`	Numero di connettori Amazon Chime ime all'estremità remota in pacchetti RTP. Unità: numero
`VcToRemoteRtcpPackets`	Il numero di pacchetti RTCP inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota. Unità: numero
`VcToRemoteRtcpBytes`	Numero di connettori Amazon Chime ime all'estremità remota in pacchetti RTCime all'estremità remota in pacchetti RTCime all'estremità remota in pacchetti RTCime all'estremità remota. Unità: numero
`VcToRemotePacketsLost`	Il numero di pacchetti persi durante il transito dall'infrastruttura Amazon Chime Voice Connector all'estremità remota. Unità: numero
`VcToRemoteJitter`	Il jitter medio dei pacchetti inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota. Unità: microsecondi
`RTTBetweenVcAndRemote`	Il tempo medio di andata e ritorno tra l'estremità remota e l'infrastruttura Amazon Chime Voice Connector. Unità: microsecondi

Parametro	Descrizione
`MOSBetweenVcAndRemote`	Il punteggio medio di opinione (MOS) stimato associato ai flussi vocali tra l'estremità remota e l'infrastruttura Amazon Chime Voice Connector. Unità: Unità: Punteggio tra 1.0-4.4. Un punteggio più alto indica una migliore qualità audio percepita.

CloudWatch dimensioni per Amazon Chime per Amazon Chime

Le CloudWatch dimensioni che puoi utilizzare con Amazon Chime sono elencate di seguito.

Dimensione	Descrizione
`VoiceConnectorId`	L'identificatore di Amazon Chime Voice Connector per cui visualizzare le metriche.
`Region`	La Regione AWS associata all'evento.

CloudWatch log per Amazon Chime per Amazon Chime per Amazon Chime

Puoi inviare le metriche di Amazon Chime Voice Connector ai CloudWatch log. Per ulteriori informazioni, consulta Modifica delle impostazioni di Amazon Chime Voice Connector nella Amazon Chime SDK Administration Guide.

Log dei parametri di qualità dei supporti multimediali

Puoi scegliere di ricevere i log delle metriche sulla qualità multimediale per il tuo Amazon Chime Voice Connector. Quando lo fai, Amazon Chime invia metriche dettagliate al minuto per tutte le tue chiamate Amazon Chime Voice Connector a un gruppo di log CloudWatch Logs creato per te. Il nome del gruppo di log è `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. I seguenti campi sono inclusi nei log, in formato JSON.

Campo	Descrizione
voice_connector_id	L'ID Amazon Chime Voice Connector che trasporta la chiamata.
event_timestamp	L'ora in cui i parametri vengono emessi, in numero di millisecondi dalla UNIX Epoch (mezzanotte del 1 gennaio 1970) in UTC.
call_id	Corrisponde all'ID della transazione.
from_sip_user	L'utente che avvia la chiamata.
from_country	Il paese che ha avviato la chiamata.
to_sip_user	L'utente ricevente per la chiamata.
to_country	Il paese ricevente per la chiamata.
endpoint_id	Un identificatore opaco che indica l'altro endpoint della chiamata. Utilizzalo con CloudWatch Logs Insights. Per ulteriori informazioni, consulta Analisi dei dati di registro con CloudWatch Logs Insights nella Amazon CloudWatch Logs User Guide.
aws_region	La Regione AWS per la chiamata.
cust2vc_rtp_packets	Il numero di pacchetti RTP inviati dal cliente all'infrastruttura Amazon Chime Voice Connector.
cust2vc_rtp_bytes	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime ime in pacchetti RTP.
cust2vc_rtcp_packets	Il numero di pacchetti RTCP inviati dal cliente all'infrastruttura Amazon Chime Voice Connector.

Campo	Descrizione
cust2vc_rtcp_bytes	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime.
cust2vc_packets_lost	Il numero di pacchetti persi durante il trasporto dal cliente all'infrastruttura Amazon Chime Voice Connector.
cust2vc_jitter	Il jitter medio dei pacchetti inviati dal cliente all'infrastruttura Amazon Chime Voice Connector.
vc2cust_rtp_packets	Il numero di pacchetti RTP inviati dall'infr astruttura Amazon Chime Voice Connector al cliente.
vc2cust_rtp_bytes	Numero di connettori Amazon Chime ime Conime al cliente in pacchetti RTP.
vc2cust_rtcp_packets	Il numero di pacchetti RTCP inviati dall'infr astruttura Amazon Chime Voice Connector al cliente.
vc2cust_rtcp_bytes	Numero di connettori Amazon Chime ime Conime al cliente in pacchetti RTCime al cliente in pacchetti RTCime in pacchetti RTCime al connettore Amazon Chime Conime al cliente in pacchetti RTCime.
vc2cust_packets_lost	Il numero di pacchetti persi durante il transito dall'infrastruttura Amazon Chime Voice Connector al cliente.

Campo	Descrizione
vc2cust_jitter	Il jitter medio dei pacchetti inviati dall'infr astruttura Amazon Chime Voice Connector al cliente.
rtt_btwn_vc_and_cust	Il tempo medio di andata e ritorno tra il cliente e l'infrastruttura Amazon Chime Voice Connector.
mos_btwn_vc_and_cust	Il punteggio medio di opinione (MOS) stimato associato ai flussi vocali tra il cliente e l'infrast ruttura Amazon Chime Voice Connector.
rem2vc_rtp_packets	Il numero di pacchetti RTP inviati dall'estremità remota all'infrastruttura Amazon Chime Voice Connector.
rem2vc_rtp_bytes	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime ime ime ime ime in pacchetti RTP.
rem2vc_rtcp_packets	Il numero di pacchetti RTCP inviati dall'estr emità remota all'infrastruttura Amazon Chime Voice Connector.
rem2vc_rtcp_bytes	Numero di connettori Amazon Chime ime ime ime ime ime ime ime ime ime ime ime ime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime in pacchetti RTCime.
rem2vc_packets_lost	Il numero di pacchetti persi durante il transito dall'estremità remota all'infrastruttura Amazon Chime Voice Connector.
rem2vc_jitter	Il jitter medio dei pacchetti inviati dall'estremità remota all'infrastruttura Amazon Chime Voice Connector.

Campo	Descrizione
vc2rem_rtp_packets	Il numero di pacchetti RTP inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota.
vc2rem_rtp_bytes	Numero di connettori Amazon Chime ime all'estremità remota in pacchetti RTP.
vc2rem_rtcp_packets	Il numero di pacchetti RTCP inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota.
vc2rem_rtcp_bytes	Numero di connettori Amazon Chime ime all'estremità remota in pacchetti RTCime all'estremità remota in pacchetti RTCime all'estremità remota in pacchetti RTCime all'estremità remota.
vc2rem_packets_lost	Il numero di pacchetti persi durante il transito dall'infrastruttura Amazon Chime Voice Connector all'estremità remota.
vc2rem_jitter	Il jitter medio dei pacchetti inviati dall'infr astruttura Amazon Chime Voice Connector all'estremità remota.
rtt_btwn_vc_and_rem	Il tempo medio di andata e ritorno tra l'estremità remota e l'infrastruttura Amazon Chime Voice Connector.
mos_btwn_vc_and_rem	Il punteggio medio di opinione (MOS) stimato associato ai flussi vocali tra l'estremità remota e l'infrastruttura Amazon Chime Voice Connector.

Log dei messaggi SIP

Puoi scegliere di ricevere i log dei messaggi SIP per il tuo Amazon Chime Voice Connector. Quando lo fai, Amazon Chime acquisisce i messaggi SIP in entrata e in uscita e li invia a un gruppo di log CloudWatch Logs creato per te. Il nome del gruppo di log è `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. I seguenti campi sono inclusi nei log, in formato JSON.

Campo	Descrizione
voice_connector_id	L'connettore Amazon Chime ime.
aws_region	La Regione AWS associata all'evento.
event_timestamp	L'ora in cui il messaggio viene acquisito, in numero di millisecondi da UNIX Epoch (mezzanotte del 1 gennaio 1970) in UTC.
call_id	L'ID di connettore Amazon Chime.
sip_message	Il messaggio SIP completo che viene acquisito.

Automazione di Amazon Chime con EventBridge

Amazon ti EventBridge consente di automatizzare iAWS servizi e rispondere automaticamente agli eventi di sistema, come i problemi relativi alla disponibilità delle applicazioni o le modifiche delle risorse. Per ulteriori informazioni sugli eventi delle riunioni, consulta Eventi di riunione nella Amazon Chime Developer Guide.

Quando Amazon Chime genera eventi, li invia a EventBridge : Amazon Chime tenta di inviare tutti gli eventi EventBridge, ma in rari casi un evento potrebbe non essere distribuito. Per ulteriori informazioni, consulta la sezione Eventi deiAWS servizi nella Guida per l' EventBridge utente di Amazon.

> **Note**
>
> Se devi crittografare i dati, devi usare Amazon S3 Managed Keys. Non supportiamo la crittografia lato server utilizzando le chiavi master del cliente archiviate nel servizio di gestione delleAWS chiavi.

Container Container Conime con EventBridge

Le azioni che possono essere attivate automaticamente per Amazon Chime ime ime ime ime ime ime ime ime ime ime ime ime ime includono le seguenti:

- Richiamo di una funzione AWS Lambda
- Avvio di un'attività Amazon Elastic Container Container Container
- Inoltro dell'evento a Amazon Kinesis Video Container Container Container Container Con
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS

Alcuni esempi di utilizzo EventBridge con Amazon Chime Voice Connectors includono:

- Attivazione di una funzione Lambda per scaricare l'audio di una chiamata al termine della chiamata.
- Avvio di un'attività Amazon ECS per abilitare la trascrizione in tempo reale dopo l'avvio di una chiamata.

Per ulteriori informazioni, consulta la Guida per EventBridge l'utente di Amazon.

Eventi di connettori Amazon Chime ime ime Conime Conime Conime

I connettori vocali Amazon Chime supportano l'invio di eventi nel EventBridge momento in cui si verificano gli eventi discussi in questa sezione.

Inizio dello connettori Amazon Chime ime Conime Conime Conime

I connettori vocali Amazon Chime inviano questo evento all'avvio dello streaming multimediale su Kinesis Video Streams.

Example Dati eventi

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "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"
    }
}
```

Conime Amazon Chime Conime Conime Conime Conime Conime

I connettori vocali Amazon Chime inviano questo evento al termine dello streaming multimediale su Kinesis Video Streams.

Example Dati eventi

Di seguito vengono riportati dati di esempio per questo evento.


```
{
    "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"
    }
}
```

Aggiornamenti di connettore Amazon Chime ime ime Conime Conime Conime

I connettori vocali Amazon Chime inviano questo evento quando lo streaming multimediale su Kinesis Video Streams viene aggiornato.

Example Dati eventi

Di seguito vengono riportati dati di esempio per questo evento.

```
{
    "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"
    }
}
```

Lo connettore Amazon Chime ime ime Conime Conime Conime Conime

I connettori vocali Amazon Chime inviano questo evento quando lo streaming multimediale a Kinesis Video Streams fallisce.

Example Dati eventi

Di seguito vengono riportati dati di esempio per questo evento.

```
{
  "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"
  }
}
```

Registrazione delle chiamate API Amazon Chime conAWS CloudTrail

Amazon Chime è integrato conAWS CloudTrail, un servizio che offre un registro delle operazioni eseguite da un utente, un ruolo o unAWS servizio in Amazon Chime. CloudTrail acquisisce tutte le chiamate API per Amazon Chime come eventi, incluse le chiamate dalla console Amazon Chime e dal codice alle API Amazon Chime. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Amazon Chime. Se non configuri un trail, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia eventi. Le informazioni raccolte da consentono CloudTrail di determinare la richiesta effettuata ad Amazon Chime, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida perAWS CloudTrail l'utente.

Informazioni su Amazon Chime in CloudTrail

CloudTrail è abilitato sull'AWSaccount al momento della sua creazione. Quando le chiamate API vengono eseguite dalla console di amministrazione Amazon Chime, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi delAWS servizio nella Cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi.

Per una registrazione continua degli eventi nell'AWSaccount, inclusi gli eventi per Amazon Chime, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail . Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail log da più regioni e Ricezione di file di CloudTrail log da più account

Tutte le azioni Amazon Chime vengono registrate CloudTrail e documentate nell'Amazon Chime API Reference. Ad esempio, le chiamate alle`ResetPersonalPIN` sezioni`InviteUsers` e generano voci nei file di CloudTrail log.`CreateAccount` Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del file di log Amazon Chime ime ime.

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log contengono una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

Le voci relative ad Amazon Chime sono identificate dalla fonte dell'evento chime.amazonaws.com.

Se hai configurato Active Directory per il tuo account Amazon Chime, consulta Registrazione delle chiamate API di AWS Directory Service utilizzando CloudTrail. Questo descrive come monitorare i problemi che potrebbero influire sulla capacità di accesso degli utenti Amazon Chime.

L'esempio seguente mostra una voce di CloudTrail log per 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"
     }
```

Convalida della conformità per Amazon Chime

I revisori di terze parti valutano la sicurezza e la conformità dei AWS servizi nell'ambito di più programmi di AWS conformità, come SOC, PCI, FedRAMP e HIPAA.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Ambito per programma di conformitàServizi AWS in Ambito di applicazione per programma Servizi AWS di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon Chime

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Amazon Chime offre diverse funzionalità per supportare le tue esigenze di resilienza e backup dei dati. Per ulteriori informazioni, consulta Gestione dei gruppi di Amazon Chime Voice Connector e Streaming dei contenuti multimediali di Amazon Chime Voice Connector su Kinesis nella Guida all'amministrazione di Amazon Chime SDK.

Sicurezza dell'infrastruttura in Amazon Chime

In quanto servizio gestito, Amazon Chime è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Informazioni sugli aggiornamenti automatici di Amazon Chime

Amazon Chime offre diversi modi per aggiornare i propri client. Il metodo varia a seconda che gli utenti eseguano Amazon Chime in un browser, sul desktop o su un dispositivo mobile.

L'applicazione web Amazon Chime, https://app.chime.aws, viene sempre caricata con le funzionalità e le correzioni di sicurezza più recenti.

Il client desktop Amazon Chime verifica la presenza di aggiornamenti ogni volta che un utente sceglie Esci o Esci. Questo vale per le macchine Windows e macOS. Man mano che gli utenti eseguono il client, quest'ultimo verifica la presenza di aggiornamenti ogni tre ore. Gli utenti possono anche

verificare la presenza di aggiornamenti selezionando Verifica aggiornamenti nel menu Aiuto di Windows o nel menu Amazon Chime di macOS.

Quando il client desktop rileva un aggiornamento, Amazon Chime richiede agli utenti di installarlo a meno che non siano coinvolti in una riunione in corso. Gli utenti partecipano a una riunione continua quando:

- Partecipano a una riunione.
- Sono stati invitati a una riunione che è ancora in corso.

Amazon Chime richiede loro di installare la versione più recente e dà loro un conto alla rovescia di 15 secondi in modo che possano posticipare l'installazione. Scegli Riprova più tardi per posticipare l'aggiornamento.

Quando gli utenti posticipano un aggiornamento e non partecipano a una riunione in corso, il client verifica la presenza dell'aggiornamento dopo tre ore e chiede loro nuovamente di installarlo. L'installazione inizia al termine del conto alla rovescia.

> **Note**
>
> Su un computer macOS, gli utenti devono scegliere Riavvia ora per iniziare l'aggiornamento.

Su un dispositivo mobile: le applicazioni mobili di Amazon Chime utilizzano le opzioni di aggiornamento fornite da App Store e Google Play per fornire la versione più recente del client Amazon Chime. Puoi anche distribuire gli aggiornamenti tramite il tuo sistema di gestione dei dispositivi mobili. Questo argomento presuppone che tu sappia come fare.

Cronologia dei documenti per Amazon Chime

La tabella seguente descrive le modifiche importanti alla Amazon Chime Administrator Guide, a partire da marzo 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicata la guida all'amministrazione dell'SDK Amazon Chime	Gli argomenti dell'SDK Amazon Chime sono ora pubblicati nella Amazon Chime SDK Administration Guide. Per informazioni, consulta la Amazon Chime SDK Administration Guide.	24 marzo 2022
Aggiornamenti delle policy IAM	Le modifiche alle politiche IAM gestite da AWS sono ora registrate in questa guida per l'amministratore. Guarda gli esempi di policy basate sull'identità di Amazon Chime.	23 settembre 2021
Ruoli collegati al servizio	Gli amministratori possono ora creare ruoli collegati ai servizi per Amazon Live Transcription e visualizzare i messaggi degli eventi all'inizio e al termine di un'operazione di trascrizione live di Amazon Chime. Per ulteriori informazioni, consulta Utilizzo dei ruoli con trascrizione in tempo reale e Automazione di Amazon Chime con eventi. CloudWatch	12 agosto 2021

Applicazioni e regole multimediali SIP	Gli amministratori possono creare applicazioni multimedi ali SIP e regole da utilizzar e con Amazon Chime Voice Connector e le sue funzioni. AWS Lambda Per ulteriori informazioni, consulta Managing SIP application and rules, nella Amazon Chime Administrator Guide.	18 novembre 2020
Numeri di routing delle chiamate di emergenza di Amazon Chime Voice Connector	Gli amministratori di Amazon Chime possono configura re i numeri di routing delle chiamate di emergenza per un Amazon Chime Voice Connector. Per ulteriori informazioni, consulta Configurazione dei numeri di routing delle chiamate di emergenza per Amazon Chime Voice Connector, nella Amazon Chime Administrator Guide.	1 luglio 2020
Amazon Chime su Dolby Voice Huddle	Amazon Chime offre un'esperi enza di riunione nativa o proprietaria su hardware per conferenze audio e video Dolby Voice Huddle. Per ulteriori informazioni, consulta Configurazione di Amazon Chime su hardware Dolby, nella Amazon Chime Administr ator Guide.	3 giugno 2020

Impostazione delle politiche di conservazione delle chat	Gli amministratori di Amazon Chime possono impostare politiche di conservazione delle chat per i propri account Enterprise. Per ulteriori informazioni, consulta la sezione Gestione delle politiche di conservazione delle chat, nella Amazon Chime Administrator Guide.	21 maggio 2020
Rimuovere i messaggi di chat	Se hai la capacità di programmare, puoi utilizzare un paio di API Amazon Chime per rimuovere i messaggi dalle chat room e dalle conversazioni del tuo account. Per ulteriori informazioni, consulta Eliminazione di singoli messaggi, nella Amazon Chime Administrator Guide.	18 maggio 2020
CloudWatch metriche di qualità multimediale per Amazon Chime Voice Connector	Amazon Chime supporta l'invio di parametri di qualità multimediale per Amazon Chime Voice Connector a. CloudWatch Per ulteriori informazioni, consulta Monitoring Amazon Chime with CloudWatch, nella Amazon Chime Administrator Guide.	23 gennaio 2020

App Amazon Chime Meetings per Slack	Amazon Chime supporta l'app Amazon Chime Meetings per Slack. Per ulteriori informazioni, consulta Configurazione dell'app Amazon Chime Meetings per Slack, nella Amazon Chime Administrator Guide.	4 dicembre 2019
Impostazioni della regione delle riunioni	Amazon Chime supporta l'elaborazione delle riunioni nella AWS regione ottimale per tutti i partecipanti. Per ulteriori informazioni, consulta le impostazioni della regione di riunione, nella Amazon Chime Administrator Guide.	3 dicembre 2019
Compatibilità con la registrazione multimediale basata su SIP (SIPREC)	I connettori vocali Amazon Chime supportano lo streaming di contenuti multimediali da un'infrastruttura vocale compatibile con SIPREC a Kinesis Video Streams. Per ulteriori informazioni, consulta la compatibilità della registrazione multimediale basata su SIP (SIPREC), nella Amazon Chime Administrator Guide.	25 novembre 2019

Amazon Chime su Dolby Voice Room	Se desideri che gli utenti partecipino comodamente alle riunioni, Amazon Chime offre un'esperienza di riunione nativa o proprietaria su hardware per conferenze e audio e video Dolby Voice Room. Per ulteriori informazioni, consulta Configurazione di Amazon Chime su Dolby Voice Room, nella Amazon Chime Administrator Guide.	29 ottobre 2019
Aggiornamento dei nomi delle chiamate in uscita	Imposta un nome di chiamata predefinito che venga visualizzato dai destinatari delle chiamate in uscita effettuate utilizzando i numeri di telefono nel tuo inventario Amazon Chime. Per ulteriori informazioni, consulta la sezione Aggiornamento dei nomi delle chiamate in uscita, nella Amazon Chime Administrator Guide.	24 ottobre 2019

Streaming di contenuti multimediali su Amazon Kinesis	Trasmetti l'audio delle chiamate telefoniche da Amazon Chime Voice Connectors a Kinesis Video Streams per analisi, apprendimento automatic o e altre elaborazioni. Per ulteriori informazioni, consulta Streaming dei contenuti multimediali di Amazon Chime Voice Connector su Kinesis e Utilizzo del ruolo collegato al servizio Amazon Chime Voice Connector, nella Amazon Chime Administrator Guide.	24 ottobre 2019
Monitoraggio di Amazon Chime con Amazon CloudWatch	Monitora l'utilizzo di Amazon Chime CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Per ulteriori informazioni, consulta Monitoring Amazon Chime with CloudWatch, nella Amazon Chime Administrator Guide.	24 ottobre 2019

Gruppi di Amazon Chime Voice Connector	Crea un gruppo Amazon Chime Voice Connector che includa Amazon Chime Voice Connectors creati in diverse regioni. AWS Ciò consente alle chiamate in entrata di eseguire il failover tra regioni, creando un meccanismo tollerant e ai guasti per il fallback in caso di eventi di disponibi lità. Per ulteriori informazi oni, consulta Lavorare con i gruppi di Amazon Chime Voice Connector, nella Amazon Chime Administrator Guide.	24 ottobre 2019
Aggiornamenti della configura zione di rete	Amazon Chime sta semplific ando i requisiti del firewall. Per ulteriori informazioni, consulta Configurazione di rete e requisiti di larghezza di banda, nella Amazon Chime Administrator Guide.	6 settembre 2019
Riunioni moderate	Amazon Chime supporta le riunioni con moderazione. Per ulteriori informazioni, consulta Partecipare a una riunione moderata, nella Amazon Chime Administrator Guide.	25 luglio 2019

Convalida della conformità per Amazon Chime	Amazon Chime è un servizio idoneo alla normativa HIPAA. Per ulteriori informazioni, consulta la sezione Convalida della conformità per Amazon Chime nella Amazon Chime Administrator Guide.	11 giugno 2019
Trasferimento di numeri di telefono gratuiti	Amazon Chime supporta il trasferimento di numeri di telefono gratuiti degli Stati Uniti da utilizzare con Amazon Chime Voice Connectors. Per ulteriori informazioni, consulta Portare i numeri di telefono esistenti, nella Amazon Chime Administrator Guide.	28 maggio 2019
Gestione dei numeri di telefono in Amazon Chime	Usa Amazon Chime Business Calling per fornire e assegnare numeri di telefono agli utenti Amazon Chime. Integra un Amazon Chime Voice Connector con un sistema telefonico esistente. Per ulteriori informazioni, consulta la sezione Gestione dei numeri di telefono in Amazon Chime nella Amazon Chime Administrator Guide.	18 marzo 2019

Componente aggiuntivo Amazon Chime per Outlook	Amazon Chime offre due componenti aggiuntivi per Microsoft Outlook: il componente aggiuntivo Amazon Chime per Outlook su Windows e il componente aggiuntivo Amazon Chime per Outlook. Questi componenti aggiuntivi offrono le stesse caratteristiche di programmazione, ma supportano tipi di utenti diversi. Per ulteriori informazioni, consulta la sezione Distribuzione del componente aggiuntivo per Outlook, nella Amazon Chime Administrator Guide.	12 marzo 2019
Vari aggiornamenti	Vari aggiornamenti per il layout e l'organizzazione dell'argomento.	11 febbraio 2019
Funzione «Chiamami» di Amazon Chime	Gli amministratori possono abilitare la funzione Amazon Chime call me nelle impostazioni delle riunioni. Per ulteriori informazioni, consulta Managing meeting settings, nella Amazon Chime Administrator Guide.	22 agosto 2018

Connect a Okta SSO	Se disponi di un account aziendale, puoi connetterti al servizio SSO di Okta per autenticare e assegnare le autorizzazioni utente. Per ulteriori informazioni, consulta Connect to Okta SSO, nella Amazon Chime Administrator Guide.	1 agosto 2018
Richiedi gli allegati utente	Ricevi allegati caricati in Amazon Chime dagli utenti. Per ulteriori informazioni, consulta Request user attachments, nella Amazon Chime Administrator Guide.	23 aprile 2018
Visualizza dati aggiuntivi del report	Visualizzazione dei dati di report aggiuntivi. Per ulteriori informazioni, consulta Visualizza report, nella Amazon Chime Administrator Guide.	30 marzo 2018
Assegna agli utenti le autorizzazioni Pro o Basic	Assegnazione delle autorizza zioni Pro o Basic agli utenti. Per ulteriori informazioni, consulta Gestire l'accesso e le autorizzazioni degli utenti, nella Amazon Chime Administr ator Guide.	29 marzo 2018