aws

Guida per l'amministratore

# Amazon Nimble Studio

# Amazon Nimble Studio: Guida per l'amministratore

# Table of Contents

Avviso di fine del supporto: il 22 ottobre 2024, il supporto per Amazon Nimble Studio AWS verrà interrotto. Dopo il 22 ottobre 2024, non potrai più accedere alla console Nimble Studio o alle risorse di Nimble Studio.

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 Nimble Studio?

Nimble Studio fornisce l'infrastruttura e la gestione centralizzata per una suite di applicazioni e servizi che gli artisti possono utilizzare per produrre effetti visivi, animazioni e contenuti di giochi nel cloud.

Con Nimble Studio, ottieni strumenti essenziali per la gestione di utenti e gruppi. Puoi anche aggiungere e gestire applicazioni, tra cui AWS Thinkbox e Nimble Studio File Transfer.

Nimble Studio offre un'interfaccia unificata che riunisce tutte le risorse del tuo studio in un unico posto. Puoi inserire utenti, assegnare applicazioni e assegnare autorizzazioni specifiche alla loro funzione lavorativa. Nimble Studio non richiede AWS esperienza e puoi configurarlo in circa cinque minuti.

Indice



## Funzionalità e vantaggi

Ecco alcune delle funzionalità e dei vantaggi che ottieni con Nimble Studio:

- Usa Nimble Studio gratuitamente; paghi solo per le risorse di studio utilizzate dalle tue applicazioni.
- Gestisci centralmente il tuo studio, controllane lo stato e ottieni informazioni di alto livello sul suo funzionamento.
- Aggiungi e gestisci applicazioni, utenti e gruppi di Nimble Studio e allega le autorizzazioni.
- Gestisci in modo sicuro l'accesso alle risorse dello studio con policy e AWS Identity and Access Management ruoli (IAM).
- Gestisci la sicurezza dell'accesso per gli utenti dello studio e i provider di identità esterni con AWS IAM Identity Center (IAM Identity Center).
- Organizza e trova facilmente le risorse dello studio inserendo tag nelle tue risorse di studio.

# Applicazioni correlate

Nimble Studio fornisce applicazioni per i creatori di contenuti digitali per gestire uno studio basato su cloud per la produzione di effetti visivi (VFX), animazioni e contenuti interattivi.

Puoi installare queste applicazioni sul tuo computer locale o nel cloud con un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Puoi anche utilizzare Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) per trasferire e archiviare in sicurezza risorse multimediali digitali. Ciò significa che puoi utilizzare Nimble Studio per ridurre i costi dell'infrastruttura fisica, delle apparecchiature e del personale tecnico.

Nimble Studio attualmente fornisce le seguenti applicazioni:

- AWS Thinkbox: Thinkbox il software include il gestore della render farm Thinkbox Deadline e il plugin 3D, Thinkbox Krakatoa. È possibile utilizzare… Thinkbox software per aiutarti ad aumentare la produzione creativa del tuo studio on-premise, nel cloud con Amazon EC2 o una combinazione di entrambi. Per ulteriori informazioni, consulta AWS Thinkbox Prodotti.
- Nimble Studio File Transfer: File Transfer accelera i trasferimenti di risorse multimediali digitali da e verso Amazon S3. File Transfer fornisce un'interfaccia utente grafica che può essere utilizzata per spostare rapidamente migliaia di file multimediali di grandi dimensioni. Per ulteriori informazioni, consulta la sezione Cos'è Nimble Studio File Transferpagina.

# Prezzi per Nimble Studio

Non è previsto alcun costo per configurare Nimble Studio e utilizzarlo per gestire l'infrastruttura, gli utenti, la sicurezza e i servizi dello studio.

Tuttavia, se configuri servizi e applicazioni nel tuo studio, potrebbero esserti addebitati costi per l'archiviazione e altre risorse dello studio. Per ulteriori informazioni sui prezzi delle applicazioni Nimble Studio, consulta la pagina dei prezzi delle singole applicazioni.

Per informazioni sulla gestione dei AWS costi, consulta AWS Cost Explorer Servicee Budget AWS.

# Inizia a usare Nimble Studio

La configurazione e l'implementazione di Nimble Studio richiedono circa cinque minuti.

Dopo aver acquisito familiarità con i concetti e la terminologia di Nimble Studio, consulta Guida introduttiva ad Amazon Nimble Studio. In esso troverai le step-by-step istruzioni per implementare il tuo studio.

# Concetti e terminologia per Amazon Nimble Studio

Per aiutarti a iniziare a usare Amazon Nimble Studio e a capire come funziona, puoi fare riferimento ai concetti e alla terminologia chiave di questa guida.

## Funzionalità principali

Amazon Nimble Studio

Amazon Nimble Studio consente agli studi creativi di produrre effetti visivi, animazioni e contenuti interattivi interamente nel cloud, dallo schizzo dello storyboard al prodotto finale. Servizio AWS

Console Amazon Nimble Studio

La console Nimble Studio è una parte di Console di gestione AWSquella dedicata ai nostri clienti IT amministratori. In questa console gli amministratori creano il loro studio cloud e gestiscono molte impostazioni. Ad esempio, la pagina di gestione di Studio consente di aggiungere o rimuovere risorse, aggiungere applicazioni e concedere autorizzazioni a utenti e gruppi.

Portale Amazon Nimble Studio

Il portale Nimble Studio fornisce un'interfaccia utente per day-to-day le interazioni con le applicazioni e i servizi Nimble Studio. Gli utenti accedono direttamente al portale con il proprio nome utente e password senza dover interagire con. Console di gestione AWS

Nimble Studio File Transfer

File Transfer accelera i trasferimenti di risorse multimediali digitali da e verso Amazon Simple Storage Service (Amazon S3). File Transfer fornisce un'interfaccia utente grafica che può essere utilizzata per spostare rapidamente migliaia di file multimediali di grandi dimensioni. Per ulteriori informazioni, consulta la sezione Cos'è Nimble Studio File Transferpagina.

AWS Thinkbox

Thinkbox il software include il gestore della render farm Thinkbox Deadline e il plugin 3D, Thinkbox Krakatoa. È possibile utilizzare… Thinkbox software per aiutarti ad aumentare la produzione creativa del tuo studio on-premise, nel cloud con Amazon EC2 o una combinazione di entrambi. Per ulteriori informazioni, consulta AWS Thinkbox Prodotti.

# Concetti e terminologia chiave

AWS politiche gestite

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. Policy autonoma significa che la policy ha un proprio Amazon Resource Name (ARN) che include il nome della policy. Ad esempio, arn:aws:iam: IAMRead OnlyAccess :aws:policy/ è una policy gestita. AWS Per ulteriori informazioni su, ARNsconsulta IAM ARNs.

AWS le politiche gestite vengono utilizzate per concedere autorizzazioni a funzioni lavorative comuni. Le policy relative alle funzioni lavorative vengono mantenute e aggiornate AWS quando vengono introdotti nuovi servizi e operazioni API. Ad esempio, la funzione AdministratorAccessjob fornisce l'accesso completo e la delega delle autorizzazioni a ogni servizio e risorsa in AWS uso. Al contrario, le politiche AWS gestite ad accesso parziale come AmazonMobileAnalyticsWriteOnlyAccess Amazon EC2 ReadOnlyAccess possono fornire livelli di accesso specifici Servizi AWS senza consentire l'accesso completo. Per ulteriori informazioni sulle politiche di accesso, consulta Comprendere i riepiloghi dei livelli di accesso all'interno dei riepiloghi delle politiche.

Console di gestione AWS

Console di gestione AWSÈ un'applicazione Web che fornisce l'accesso a un'ampia raccolta di console di servizio per la gestione. Servizi AWS

Ogni servizio include anche la propria console. Queste console offrono un'ampia gamma di strumenti per il cloud computing. C'è anche un servizio che aiuta con la fatturazione e la gestione dei costi.

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center è un AWS servizio che semplifica la gestione centralizzata dell'accesso a più Account AWS applicazioni aziendali. Con IAM Identity Center, puoi fornire agli utenti l'accesso Single Sign-On a tutti gli account e le applicazioni loro assegnati da un'unica posizione. Puoi anche gestire centralmente l'accesso multiaccount e le autorizzazioni utente a tutti i tuoi account in. AWS Organizations Per ulteriori informazioni, consulta AWS IAM Identity Center FAQs.

AWS PrivateLink

AWS PrivateLink fornisce connettività privata tra VPCs e le reti locali, senza esporre il traffico alla rete Internet pubblica. Servizi AWS AWS PrivateLink semplifica la connessione di servizi tra diversi account e. VPCs AWS PrivateLinkè disponibile dietro pagamento di una tariffa mensile fatturata al tuo Account AWS.

### Creazione di contenuti digitali (DCC)

La creazione di contenuti digitali (DCC) si riferisce alla categoria di applicazioni utilizzate per produrre contenuti creativi, tra cui Blender, Nuke, Mayae Houdini.

### Regioni

Nimble Studio ne offre undici tra cui Regioni AWS scegliere per implementare il proprio studio. Le regioni sono quelle in cui esiste l'infrastruttura essenziale dello studio, come i dati e le applicazioni.

La regione deve essere situata più vicina agli utenti del tuo studio. Ciò riduce il ritardo e migliora la velocità di trasferimento dei dati.

### Studio

Uno studio è il contenitore di primo livello per altre risorse relative a Nimble Studio. Il tuo studio cloud gestisce il portale web Nimble Studio e le connessioni alle risorse essenziali del tuo sito, Account AWS come il tuo VPC, la directory utente e le chiavi di crittografia dello storage.

### Applicazioni da studio

I componenti di Studio sono configurazioni all'interno di Nimble Studio di un cliente che indicano al servizio come accedere a risorse come file system, server di licenza e render farm presenti nel tuo. Account AWS

Nimble Studio contiene diversi sottotipi di componenti di studio, tra cui un file system condiviso, una compute farm, Active Directory e un componente di licenza. Questi sottotipi descrivono le risorse che vorresti che il tuo studio usasse.

### Risorse dello studio

Le risorse dello studio sono un termine che riassume le cose di cui uno studio ha bisogno nelle sue operazioni quotidiane. Quando si descrive come le risorse si inseriscono nell'infrastruttura di uno studio cloud, possono essere chiamate anche componenti di studio.

### Tag

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale definiti dall'utente.

I tag consentono di classificare le AWS risorse in diversi modi. Ad esempio, puoi definire un set di tag per le istanze Amazon Elastic Compute Cloud (Amazon EC2) del tuo account che ti aiutano a

monitorare il proprietario e il livello di stack di ogni istanza. I tag ti consentono inoltre di integrare i file system condivisi della tua organizzazione e le render farm con Nimble Studio, per mantenere i flussi di lavoro ininterrotti mentre sposti la forza lavoro sul cloud.

Con i tag, puoi classificare le tue AWS risorse per scopo, proprietario o ambiente. Ciò è utile quando si dispone di molte risorse dello stesso tipo: è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati.

# Configurazione per Nimble Studio

Questo tutorial è destinato agli utenti amministratori che desiderano configurare Amazon Nimble Studio.

Le seguenti sezioni ti guideranno attraverso i passaggi da completare prima di distribuire uno studio in Nimble Studio.

Indice



## Configurazione di IAM

Consulta la seguente documentazione AWS Identity and Access Management (IAM) prima di iniziare.

- Best practice per la sicurezza in IAM
- Accedi Account AWS come utente amministratore per completare la configurazione rimanente.

### 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 https://portal.aws.amazon.com/billing/registrazione.
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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo 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 Console di gestione AWScome 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, assegna 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 l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- 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 a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

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

# Risorse correlate

- Best practice di sicurezza in IAM
- Servizio AWS quote - Riferimenti generali di AWS

# Guida introduttiva ad Amazon Nimble Studio

Questo capitolo mostra come utilizzare la console Nimble Studio per creare l'infrastruttura dello studio, confermare Regione AWS, rivedere le impostazioni e creare lo studio. Puoi anche personalizzare la configurazione con impostazioni aggiuntive.

Per i nuovi AWS clienti, consulta i Configurazione per Nimble Studio tutorial.

Argomenti



## Configurazione di Nimble Studio

Questa guida mostra come configurare l'infrastruttura, rivedere le impostazioni e creare lo studio. Puoi anche personalizzare il tuo studio conImpostazioni di studio aggiuntive.

### Fase 1: Configurare l'infrastruttura dello studio

L'infrastruttura del tuo studio è composta dai seguenti componenti:

- Nome visualizzato Studio: il nome visualizzato di Studio consente di identificare lo studio, ad esempio AnyCompany Studio. Il nome dello studio determina anche l'URL del portale Studio. Puoi modificare il nome visualizzato di Studio dopo aver completato la configurazione, in qualsiasi momento.
- URL del portale Studio: puoi accedere al tuo studio utilizzando l'URL del portale Studio. L'URL si basa sul nome visualizzato di Studio, ad esempio https://anycompanystudio.awsapps.com. Puoi modificare l'URL del portale Studio dopo aver completato la configurazione, in qualsiasi momento.
- Regione AWS: Regione AWSè la posizione fisica per una raccolta di data AWS center. Quando configuri il tuo studio, per impostazione predefinita la regione è la posizione più vicina a te. Dovresti cambiare la regione in modo che sia più vicina ai tuoi utenti. Ciò riduce il ritardo e migliora la velocità di trasferimento dei dati.

> **Important**
>
> Non puoi cambiare la tua regione dopo aver completato la configurazione di Nimble Studio.

Completa le attività in questa sezione per configurare l'infrastruttura del tuo studio.

Per configurare l'infrastruttura del tuo studio

1. Accedi Console di gestione AWSe apri la console Nimble Studio.
2. Scegli Setup Nimble Studio, quindi scegli Avanti.
3. Inserisci il nome visualizzato da Studio, ad esempio**`AnyCompany Studio`**.
4. (Facoltativo) Per modificare il nome del portale Studio, scegliete Modifica URL.
5. (Facoltativo) Per modificarlo Regione AWSin modo che sia più vicino agli utenti del tuo studio, scegli Cambia regione.
   a. Seleziona la regione più vicina ai tuoi utenti.
   b. Scegli Applica regione.
6. (Facoltativo) Per personalizzare ulteriormente la configurazione dello studio, seleziona Impostazioni di studio aggiuntive.
7. Per rivedere le impostazioni prima di creare lo studio, scegli Avanti.

## Passaggio 2: rivedi e crea il tuo studio

Dopo aver configurato l'infrastruttura del tuo studio, puoi rivedere, apportare modifiche e creare il tuo studio.

Per rivedere e creare il tuo studio

1. Nella pagina Rivedi e crea, esamina l'infrastruttura di Studio.
2. Verifica che Regione AWSsia la più vicina agli utenti del tuo studio.
3. (Facoltativo) Scegliete Modifica per apportare modifiche alla configurazione dello studio.
4. Quando sei pronto, scegli Create studio.

# Impostazioni di studio aggiuntive

La configurazione di Nimble Studio include impostazioni di studio aggiuntive. Con queste impostazioni, puoi visualizzare tutte le modifiche apportate dalla configurazione di Nimble Studio al tuo Account AWS, configurare il tuo ruolo utente in studio e modificare il tipo di chiave di crittografia. Puoi anche aggiungere tag opzionali alle risorse del tuo studio.

# Configura il ruolo utente dello studio

Un AWS servizio può assumere un ruolo di servizio per eseguire azioni per conto dell'utente. Nimble Studio richiede un ruolo utente di studio per consentire agli utenti di accedere alle risorse del tuo studio.

Puoi allegare policy gestite AWS Identity and Access Management (IAM) al ruolo utente dello studio. Le policy consentono agli utenti di eseguire determinate azioni, come la creazione di lavori in una specifica applicazione Nimble Studio. Poiché le applicazioni dipendono da condizioni specifiche della politica gestita, se non si utilizzano le politiche gestite, l'applicazione potrebbe non funzionare come previsto.

Puoi modificare il ruolo utente di studio dopo aver completato la configurazione, in qualsiasi momento. Per ulteriori informazioni sui ruoli utente, consulta IAM Roles.

Le seguenti schede contengono istruzioni per due diversi casi d'uso. Per creare e utilizzare un nuovo ruolo di servizio, scegli la scheda Nuovo ruolo di servizio. Per utilizzare un ruolo di servizio esistente, scegli la scheda Ruolo di servizio esistente.

New service role

Per creare e utilizzare un nuovo ruolo di servizio

1. Seleziona Crea e utilizza un nuovo ruolo di servizio.
2. (Facoltativo) Inserisci il nome del ruolo utente del servizio.
3. Scegli Visualizza i dettagli delle autorizzazioni per ulteriori informazioni sul ruolo.

Existing service role

Per utilizzare un ruolo di servizio esistente

1. Seleziona Usa un ruolo di servizio esistente.
2. Apri l'elenco a discesa per scegliere un ruolo di servizio esistente.
3. (Facoltativo) Scegli Visualizza nella console IAM per ulteriori informazioni sul ruolo.

# AWS IAM Identity Center

AWS IAM Identity Center è un servizio Single Sign-On basato sul cloud per la gestione di utenti e gruppi. IAM Identity Center può anche essere integrato con il tuo provider Single Sign-On (SSO) aziendale in modo che gli utenti possano accedere con il proprio account aziendale.

Nimble Studio abilita IAM Identity Center per impostazione predefinita ed è necessario per configurare e utilizzare Nimble Studio. Per ulteriori informazioni, consulta Cos'è. AWS IAM Identity Center

## Configurare AWS KMS la chiave di crittografia

AWS Key Management Service le chiavi (AWS KMS) sono il tipo principale di chiave KMS che puoi utilizzare per crittografare, decrittografare e ricrittografare i dati.

Nimble Studio include i seguenti tipi di chiavi di crittografia: AWS KMS

- AWS chiave proprietaria: le chiavi AWS proprietarie sono chiavi KMS che Servizio AWS possiede e gestisce per essere utilizzate in più lingue. Account AWS AWS le chiavi di proprietà non risiedono nel tuo Account AWS, ma Nimble Studio può utilizzare una chiave AWS proprietaria per proteggere le risorse del tuo account.

  Per AWS KMS utilizzarla, non è necessario creare o mantenere la chiave o la relativa politica chiave. L'utilizzo delle chiavi di AWS proprietà è gratuito e non vengono conteggiate nelle AWS KMS quote assegnate Account AWS.
- AWS KMS Chiave gestita dal cliente: una chiave gestita dal cliente è una chiave KMS Account AWS che crei, possiedi e gestisci.

  Hai il pieno controllo su queste chiavi KMS. Le chiavi gestite dal cliente sono soggette a una tariffa mensile. Inoltre, sono soggette a una commissione per ogni richiesta API AWS KMS oltre il livello gratuito. Per ulteriori informazioni sui AWS KMS prezzi, consulta AWS Key Management Service la pagina dei prezzi.

Il tipo di chiave di crittografia non può essere modificato dopo aver completato la configurazione. Per ulteriori informazioni sui tipi AWS KMS di chiavi di crittografia, consulta la AWS KMS documentazione.

Per scegliere un tipo di chiave di crittografia diverso

1. Seleziona Scegli una AWS KMS chiave diversa (avanzata).
2. Seleziona una AWS KMS chiave o inserisci un Amazon Resource Number (ARN).
3. Scegli Crea AWS KMS chiave.

## Configura i tag

I tag fungono da etichette per organizzare le risorse di Nimble Studio. Puoi aggiungere fino a 50 tag per identificare, organizzare, filtrare e cercare risorse.

Ogni tag è composto da due parti, che definisci: un tag Key e un tag opzionale Value, ad esempio, key: `domain` e value:`anycompanystudio.com`.

Puoi aggiungere o rimuovere tag dopo aver completato la configurazione, in qualsiasi momento. Per ulteriori informazioni sui tag, consulta Etichettare le AWS risorse.

Per aggiungere tag alle risorse del tuo studio

1. Scegli Add new tag (Aggiungi nuovo tag).
2. Inserisci il valore per Key (Chiave) del tag.
3. (Facoltativo) Immettete il valore del tag.

# Eliminare uno studio

Se non hai più bisogno di uno studio, puoi eliminarlo. Quando elimini lo studio, viene eliminata solo l'infrastruttura dello studio. AWS Le altre risorse, come i ruoli utente, le politiche e i dati delle applicazioni, rimangono intatte.

> **Important**
>
> Non puoi ripristinare uno studio dopo averlo eliminato.

Per eliminare il tuo studio

1. Accedi Console di gestione AWS e apri la console Nimble Studio.
2. Seleziona Panoramica dello studio.
3. Scegli Azioni, quindi seleziona Elimina studio.
4. Entra**`delete`**, quindi scegli Elimina.

# Sicurezza in Amazon Nimble Studio

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

La sicurezza è una responsabilità condivisa tra te e te. AWS 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 in Cloud AWS. AWS fornisce inoltre servizi che è possibile 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 saperne di più sui programmi di conformità che si applicano a Amazon Nimble Studio, vedi AWS Servizi rientranti nell'ambito del programma di conformitàAWS .
- 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.

> **Important**
>
> Si consiglia vivamente di leggere e acquisire familiarità con il Security Pillar - Well-Architected AWS Framework. Questo articolo contiene i principi chiave per proteggere l'infrastruttura. AWS

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo Nimble Studio. I seguenti argomenti mostrano come configurare Nimble Studio per raggiungere i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere i Nimble Studio risorse.

## Ulteriori informazioni

- Pilastro della sicurezza - AWS Well-Architected Framework
- Sicurezza per () AWS Cloud Development Kit (AWS CDK)AWS CDK

- Sicurezza nel cloud privato virtuale di Amazon
- AWS credenziali di sicurezza
- Sicurezza in Amazon EC2
  - Linux
  - Windows

# Configura la Account AWS sicurezza

Questa guida mostra come configurare la ricezione Account AWS di notifiche quando le risorse sono compromesse e come consentire a Account AWS utenti specifici di accedervi. Per proteggere Account AWS e monitorare le tue risorse, completa i seguenti passaggi.

Indice



## Elimina le chiavi di accesso del tuo account

Puoi consentire l'accesso programmatico alle tue AWS risorse da AWS Command Line Interface (AWS CLI) o con AWS APIs. Tuttavia, AWS consiglia di non creare o utilizzare le chiavi di accesso associate all'account root per l'accesso programmatico.

Se disponi ancora delle chiavi di accesso, ti consigliamo di eliminarle e creare un utente. Quindi, concedi a quell'utente solo le autorizzazioni necessarie per l'utente APIs che intendi chiamare. Puoi usare quell'utente per emettere le chiavi di accesso.

Per ulteriori informazioni, consulta Managing Access Keys for Your Account AWS nella Riferimenti generali di AWS guida.

## Abilita autenticazione a più fattori

L'autenticazione a più fattori (MFA) è una funzionalità di sicurezza che fornisce un livello di autenticazione oltre al nome utente e alla password.

La MFA funziona in questo modo: dopo aver effettuato l'accesso con il nome utente e la password, è necessario fornire anche un'informazione aggiuntiva a cui solo l'utente ha accesso fisico. Queste informazioni possono provenire da un dispositivo hardware MFA dedicato o da un'app su un telefono.

È necessario selezionare il tipo di dispositivo MFA che si desidera utilizzare dall'elenco dei dispositivi MFA supportati. Se si tratta di un dispositivo hardware, conservare il dispositivo MFA in un luogo sicuro.

Se utilizzi un dispositivo MFA virtuale (come un'app per telefono), pensa a cosa potrebbe succedere in caso di smarrimento o danneggiamento del telefono. Un approccio consiste nel mantenere il dispositivo MFA virtuale utilizzato in un luogo sicuro. Un'altra opzione consiste nell'attivare più di un dispositivo contemporaneamente o utilizzare un'opzione MFA virtuale per il ripristino delle chiavi del dispositivo.

Per ulteriori informazioni sull'MFA, vedere Enabling a Virtual Multi-Factor Authentication (MFA) Device.

### Risorse correlate

- Guida introduttiva all'autenticazione a più fattori
- Protezione dell'accesso all' AWS utilizzo della tecnologia MFA

## Abilita CloudTrail in tutto Regioni AWS

Puoi tenere traccia di tutte le attività nelle tue AWS risorse utilizzando AWS CloudTrail. Ti consigliamo di accenderlo CloudTrail ora. Questo può aiutare Supporto il vostro progettista di AWS soluzioni a risolvere un problema di sicurezza o di configurazione in un secondo momento.

Per abilitare CloudTrail l'accesso in tutte le aree geografiche Regioni AWS, consulta AWS CloudTrail Aggiorna: attiva in tutte le regioni e utilizza percorsi multipli.

Per ulteriori informazioni CloudTrail, consulta Turn On CloudTrail: Log API Activity in Your Account AWS. Per scoprire come CloudTrail monitora Nimble Studio, consulta. Registrazione delle chiamate di Nimble Studio utilizzando AWS CloudTrail

## Configura Amazon GuardDuty e notifiche

Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora quanto segue:

- Origine dati
- Registri di flusso di Amazon VPC
- AWS CloudTrail registri degli eventi di gestione
- CloudTrail registri degli eventi relativi ai dati S3
- Log DNS

Amazon GuardDuty identifica attività impreviste, potenzialmente non autorizzate e dannose all'interno del tuo AWS ambiente. Le attività dannose possono includere problemi come l'aumento dei privilegi, l'uso di credenziali esposte o la comunicazione con indirizzi IP o domini dannosi. Per identificare queste attività, GuardDuty utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, e l'apprendimento automatico. Ad esempio, GuardDuty è in grado di rilevare EC2 istanze Amazon compromesse che utilizzano malware o estraggono bitcoin.

GuardDuty monitora inoltre il comportamento di Account AWS accesso alla ricerca di segnali di compromissione. Ciò include implementazioni di infrastrutture non autorizzate, come istanze distribuite in un Regione AWS ambiente che non è mai stato utilizzato. Include anche chiamate API insolite, come una modifica della politica delle password per ridurre la sicurezza delle password.

GuardDuty ti informa sullo stato del tuo AWS ambiente fornendo risultati di sicurezza. Puoi visualizzare questi risultati nella GuardDuty console o tramite Amazon CloudWatch Events.

## Configurare un argomento e un endpoint di Amazon SNS

Segui le istruzioni contenute nell'argomento Configurazione di un Amazon SNS e nel tutorial sugli endpoint.

## Organizza un EventBridge evento per i risultati GuardDuty

Crea una regola per EventBridge inviare eventi per tutti i risultati GuardDuty generati.

Per creare un EventBridge evento per GuardDuty i risultati

1. Accedi alla EventBridge console Amazon: https://console.aws.amazon.com/events/
2. Nel pannello di navigazione, scegli Regole. Quindi scegli Create rule (Crea regola).
3. Inserisci un nome e una descrizione per la nuova regola. Quindi scegli Successivo.
4. Lascia AWS gli eventi o gli eventi dei EventBridge partner selezionati per l'origine dell'evento.

5. In Event pattern, scegli AWS i servizi per l'origine dell'evento. Quindi GuardDutyper i AWS servizi e GuardDuty Finding for the Event type. Questo è l'argomento in cui hai creatoConfigurare un argomento e un endpoint di Amazon SNS.
6. Scegli Next (Successivo).
7. Per Target 1, seleziona AWS servizio. Scegli l'argomento SNS nel menu a discesa Seleziona un obiettivo. Quindi scegli l'argomento GuardDuty_to_email.
8. Nella sezione Impostazioni aggiuntive: utilizza il menu a discesa Configura l'input target per scegliere Input transformer. Seleziona Configura il trasformatore di input.
9. Inserisci il seguente codice nel campo Percorso di input nella sezione Target input transformer.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. Per formattare l'e-mail, inserisci il seguente codice nel campo Modello.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Scegli Create (Crea) . Quindi scegli Successivo.
12. (Facoltativo) Aggiungi tag se utilizzi i tag per tenere traccia AWS delle tue risorse.
13. Scegli Next (Successivo).
14. Rivedi la tua regola. Quindi scegli Create rule (Crea regola).

Ora che hai impostato la Account AWS sicurezza, puoi concedere l'accesso a utenti specifici e ricevere notifiche quando le tue risorse sono compromesse.

# Protezione dei dati in Amazon Nimble Studio

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in Amazon Nimble Studio. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Nimble Studio o altro Servizi AWS utilizzando la console AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in Amazon Nimble Studio. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. Sei responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza per Servizi AWS ciò che utilizzi.

Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati nell'Unione europea, visita il Centro GDPR.

## Crittografia a riposo

Nimble Studio protegge i dati sensibili dello studio crittografandoli quando sono inattivi utilizzando chiavi di crittografia archiviate in AWS Key Management Service ()AWS KMS. La crittografia a riposo è disponibile Regioni AWS ovunque sia disponibile Nimble Studio. I dati di studio che crittografiamo includono il nome e le descrizioni di tutti i tipi di risorse, nonché gli script dei componenti di studio, i parametri degli script, i punti di montaggio, i nomi delle condivisioni e altri dati.

La crittografia dei dati significa che i dati sensibili salvati su dischi non sono leggibili da nessun utente o applicazione senza una chiave valida. I dati crittografati possono essere archiviati in modo sicuro su disco e possono essere decrittografati solo da una parte con accesso autorizzato alla chiave gestita.

Per informazioni su come Nimble Studio utilizza AWS KMS per crittografare i dati inattivi, consulta. Gestione delle chiavi per Amazon Nimble Studio

### Usare le sovvenzioni con le chiavi AWS KMS

Una sovvenzione è uno strumento politico che consente ai AWS mandanti di utilizzare AWS KMS le chiavi nelle operazioni crittografiche. Può anche consentire loro di visualizzare una chiave KMS con il comando e di creare e gestire `DescribeKey` le sovvenzioni.

Le sovvenzioni vengono comunemente utilizzate da chi Servizi AWS si integra con AWS KMS per crittografare i dati inattivi. Il servizio crea una concessione per conto di un utente nell'account, ne utilizza le autorizzazioni e la revoca non appena l'attività è completata.

Quando Nimble Studio crea il tuo studio, forniamo due ruoli agli utenti del portale Nimble Studio: ruoli utente e ruoli di amministratore. Nimble Studio concede sovvenzioni sulle chiavi gestite dai clienti per questi ruoli per fornire loro l'accesso ai dati crittografati dello studio.

> **Important**
>
> Se elimini una concessione, il portale Nimble Studio sarà inutilizzabile per gli utenti, finché l'amministratore non creerà una nuova concessione.

Per dettagli su come Servizi AWS utilizzare le concessioni, consulta How Servizi AWS use AWS KMS or the Encryption at rest nella guida per l'utente del servizio o nella guida per sviluppatori.

## Crittografia in transito

Nella tabella seguente vengono fornite informazioni sulla crittografia dei dati in transito. Ove applicabile, sono elencati anche altri metodi di protezione dei dati per Nimble Studio.

| Dati | Percorso di rete | Protezione |
| --- | --- | --- |
| Risorse Web come immagini e file JavaScript | Il percorso di rete è tra gli utenti di Nimble Studio e Nimble Studio. | La crittografia dei dati utilizza TLS 1.2 o versioni successive. |
| Pixel e traffico di streaming correlato | Il percorso di rete è tra gli utenti di Nimble Studio e Nimble Studio. | Crittografato utilizzando Advanced Encryption Standard (AES-256) a 256 bit e trasportato tramite TLS 1.2 o versione successiva. |
| Traffico API | Il percorso è tra gli utenti di Nimble Studio e Nimble Studio. | Crittografato tramite TLS 1.2 o versione successiva. Le richieste di creazione di una connessione vengono firmate utilizzando SigV4. |

## Gestione delle chiavi per Amazon Nimble Studio

Quando crei un nuovo studio, puoi scegliere una delle seguenti chiavi per crittografare i dati dello studio:

- AWS chiave KMS proprietaria: tipo di crittografia predefinito. La chiave è di proprietà di Nimble Studio (senza costi aggiuntivi).
- Chiave KMS gestita dal cliente: la chiave è archiviata nel tuo account e viene creata, posseduta e gestita da te. Hai il pieno controllo della chiave. AWS KMS si applicano costi.

L'eliminazione di una chiave KMS gestita dal cliente in AWS Key Management Service (AWS KMS) è distruttiva e potenzialmente pericolosa. Elimina in modo irreversibile il materiale chiave e tutti i metadati associati alla chiave. Dopo l'eliminazione di una chiave KMS gestita dal cliente, non è più possibile decrittografare i dati crittografati con quella chiave. Ciò significa che i dati diventano irrecuperabili.

Questo è il motivo per cui AWS KMS offre ai clienti un periodo di attesa fino a 30 giorni prima di eliminare la chiave. Il periodo di attesa predefinito è di 30 giorni.

## Informazioni sul periodo di attesa

Poiché eliminare una chiave KMS gestita dal cliente è distruttivo e potenzialmente pericoloso, ti chiediamo di impostare un periodo di attesa di 7-30 giorni. Il periodo di attesa predefinito è di 30 giorni.

Tuttavia, il periodo di attesa effettivo potrebbe essere fino a 24 ore più lungo di quello pianificato. Per ottenere la data e l'ora effettive in cui la chiave verrà eliminata, utilizza l'operazione. DescribeKey È inoltre possibile visualizzare la data di eliminazione pianificata di una chiave nella AWS KMS console nella pagina di dettaglio della chiave, nella sezione Configurazione generale. Nota il fuso orario.

Durante il periodo di attesa, lo stato e lo stato della chiave gestita dal cliente sono In attesa di eliminazione.

- Una chiave KMS gestita dal cliente in attesa di eliminazione non può essere utilizzata in alcuna operazione crittografica.
- AWS KMS non ruota le chiavi di supporto delle AWS KMS chiavi gestite dal cliente in attesa di eliminazione.

Per ulteriori informazioni sull'eliminazione di una AWS KMS chiave gestita dal cliente, consulta Eliminazione delle chiavi master del cliente.

# Misure di sicurezza dei dati

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare account individuali con AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È consigliabile TLS 1.2 o versioni successive.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili, come i numeri di account dei clienti, in campi in formato libero come il campo Nome. Ciò include quando lavori con Amazon Nimble Studio o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS CLI Tutti i dati che inserisci in Amazon Nimble Studio o in altri servizi potrebbero essere raccolti per essere inclusi nei log di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

# Dati e parametri diagnostici

Durante la distribuzione e l'eliminazione di StudioBuilder, Amazon Nimble Studio raccoglie determinate metriche che utilizziamo per diagnosticare problemi e migliorare le funzionalità e l'esperienza utente di Nimble Studio.

## Tipi di metriche raccolte

- Informazioni sull'utilizzo: i comandi e i sottocomandi generici che vengono eseguiti.
- Errori e informazioni diagnostiche: lo stato e la durata dei comandi eseguiti, inclusi i codici di uscita, i nomi delle eccezioni interne e gli errori.
- Informazioni sul sistema e sull'ambiente — La versione di Python, il sistema operativo (Windows, Linux, oppure macOS) e l'ambiente in cui StudioBuilder viene eseguito.

# Identity and Access Management per Amazon Nimble Studio

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 controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Amazon Nimble Studio. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti



## Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Nimble Studio.

Utente del servizio: se utilizzi il servizio Nimble Studio per svolgere il tuo lavoro, allora sei un utente del servizio. In questo caso, l'amministratore ti fornirà le credenziali e le autorizzazioni necessarie per accedere alle risorse assegnate. Man mano che utilizzi più funzionalità di Nimble Studio 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 Nimble Studio, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Nimble Studio

Amministratore del servizio: se sei responsabile delle risorse di Nimble Studio presso la tua azienda, probabilmente hai pieno accesso a Nimble Studio. È tuo compito determinare a quali funzionalità e risorse di Nimble Studio devono accedere i tuoi dipendenti. Quindi, invia richieste all'amministratore per modificare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa

pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Nimble Studio, consulta. Come funziona Amazon Nimble Studio con IAM

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Per ulteriori informazioni sull'accesso utilizzando il Console di gestione AWS, consulta Accedere Console di gestione AWS come utente IAM o utente root nella Guida per l'utente IAM.

È necessario autenticarsi (accedere a AWS) come utente Account AWS root, utente o assumere un ruolo IAM. Puoi anche utilizzare l'autenticazione Single Sign-On della tua azienda o persino accedere tramite Google o Facebook. In questi casi, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando le credenziali di un'altra azienda, assumi un ruolo indirettamente.

Per accedere direttamente a Console di gestione AWS, utilizza la password con l'indirizzo e-mail dell'utente root o il nome utente. È possibile accedere a AWS livello di programmazione utilizzando l'utente root o le chiavi di accesso utente.

AWS fornisce strumenti SDK e da riga di comando per firmare crittograficamente la richiesta utilizzando le credenziali dell'utente. Se non utilizzi AWS strumenti, firma tu stesso la richiesta. A questo scopo, utilizza Signature Version 4, un protocollo per l'autenticazione di richieste API in entrata. Per ulteriori informazioni sulle richieste di autenticazione, consulta la pagina relativa al processo di firma Signature Version 4 nella Riferimenti generali di AWS .

Indipendentemente 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 saperne di più, consulta Using Multi-Factor Authentication (MFA) AWS nella IAM User Guide.

### Account AWS utente root

La prima volta che si crea un account Account AWS, si inizia con un'identità di accesso singolo che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità si chiama utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Ti consigliamo vivamente di non utilizzare l'utente root per le tue attività quotidiane, nemmeno quelle amministrative. Rispettare piuttosto la best practice di utilizzare l'utente root soltanto per creare il tuo primo utente IAM. Quindi conservare al sicuro le credenziali dell'utente root e utilizzarle per eseguire solo alcune attività di gestione dell'account e del servizio.

## Utenti e gruppi

Un utente è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Un utente può avere credenziali a lungo termine o un set di chiavi di accesso. Per scoprire come generare chiavi di accesso, consulta Managing access keys for IAM users nella IAM User Guide. Quando generi le chiavi di accesso per un utente, visualizza e salva in modo sicuro la coppia di chiavi. Non potrai recuperare la chiave di accesso segreta in futuro. Genera invece una nuova coppia di key pair di accesso.

Un gruppo IAM è un'identità che specifica una raccolta di utenti. 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 (anziché 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, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in Console di gestione AWS cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, consulta Using IAM roles nella IAM User Guide.

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

- Autorizzazioni utente temporanee: un utente può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso utente federato: invece di creare un utente, puoi utilizzare le identità esistenti della tua directory utenti aziendale o di un provider di identità web. Directory Service Sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta Federated users and roles nella IAM User Guide.

- Iscrizione: Nimble Studio utilizza un concetto chiamato «iscrizione» per fornire a un utente l'accesso a un particolare profilo di lancio. L'iscrizione consente agli amministratori dello studio di delegare l'accesso alle risorse agli utenti, senza dover scrivere o comprendere le politiche IAM. Quando un amministratore di Nimble Studio crea un'iscrizione per un utente in un profilo di avvio, l'utente è autorizzato a eseguire le azioni IAM necessarie per utilizzare un profilo di avvio, come visualizzarne le proprietà e avviare una sessione di streaming utilizzando quel profilo di avvio.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. I ruoli di servizio forniscono l'accesso solo all'interno del tuo account e non possono essere utilizzati per concedere l'accesso ai servizi in altri account. Un amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella 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. Nimble Studio non supporta i ruoli collegati ai servizi.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Per sapere se utilizzare i ruoli o gli utenti IAM, consulta Quando creare un ruolo IAM (anziché un utente) nella Guida per l'utente IAM.

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o AWS risorse IAM. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. Puoi accedere come utente root o utente oppure puoi assumere un ruolo IAM. Quando poi effettui una richiesta, AWS valuta le relative politiche basate sull'identità o sulle risorse. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata come documenti JSON. AWS Per ulteriori informazioni sulla struttura e

il contenuto dei documenti relativi alle policy JSON, consulta Panoramica delle policy JSON nella IAM User Guide.

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

Ogni entità IAM (utente o ruolo) inizialmente non dispone di autorizzazioni. Ovvero, di default, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore fornisce le autorizzazioni a un gruppo, le autorizzazioni vengono concesse a tutti gli utenti in tale gruppo.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente 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' Console di gestione AWS AWS CLI, dall'o dall' AWS API.

### Policy basate sull'identità

Le politiche basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità, ad esempio un utente, un gruppo di utenti o un ruolo. Queste politiche controllano le azioni che gli utenti e i ruoli possono eseguire, su quali risorse e in quali condizioni. Per scoprire come creare una policy basata sull'identità, consulta Creazione di policy IAM nella IAM User Guide.

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 policy gestite sono policy autonome che puoi allegare a più utenti, gruppi e ruoli all'interno della tua azienda. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per scoprire come scegliere tra una policy gestita o una politica in linea, consulta Choosing between managed policy e inline policy nella IAM User Guide.

### Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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. Per la risorsa a cui è allegata la policy, la policy definisce quali azioni uno specifico principale può eseguire su quella risorsa e a quali

condizioni. Specificare un principale in una politica 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.

### Accedi agli elenchi di controllo (ACLs) in Nimble Studio

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

### 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 di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM (utente o ruolo). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione tra le politiche basate sull'identità dell'entità e i suoi limiti di autorizzazione. Le politiche basate sulle risorse che specificano l'utente o il ruolo nel campo non sono limitate dal limite delle `Principal` 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.
- Policy di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in Organizations. Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, incluso ogni utente Account AWS root. Per ulteriori informazioni su Organizations and SCPs, consulta How SCPs work nella AWS Organizations User Guide.
- 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 sull'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 le politiche 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 scoprire 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 Nimble Studio con IAM

Prima di utilizzare IAM per gestire l'accesso a Nimble Studio, scopri quali funzionalità IAM sono disponibili per l'uso con Nimble Studio.

Funzionalità IAM che puoi usare con Amazon Nimble Studio

| Funzionalità IAM | Supporto per Nimble Studio |
|---|---|
| Azioni politiche per Nimble Studio | Sì |
| Risorse politiche per Nimble Studio | Sì |
| Chiavi relative alle condizioni delle politiche per Nimble Studio | Sì |
| Accedi agli elenchi di controllo () ACLs in Nimble Studio | No |
| Controllo degli accessi basato sugli attributi (ABAC) con Nimble Studio | Sì |
| Utilizzo di credenziali temporanee con Nimble Studio | Sì |
| Autorizzazioni principali multiservizio per Nimble Studio | Sì |
| Ruoli di servizio per Nimble Studio | Sì |

| Funzionalità IAM | Supporto per Nimble Studio |
| --- | --- |
| Ruoli collegati ai servizi per Nimble Studio | No |

Per avere una panoramica generale del Servizi AWS funzionamento di Nimble Studio e altri con la maggior parte delle funzionalità IAM, consulta Servizi AWS la sezione dedicata alla compatibilità con IAM nella IAM User Guide.

## Politiche basate sull'identità per Nimble Studio

| | |
| --- | --- |
| Supporta le policy basate su identità | Sì |

Le politiche basate sull'identità sono documenti di policy di autorizzazione JSON che puoi allegare a un'identità, ad esempio un utente, un gruppo di utenti o un ruolo. Queste politiche controllano le azioni che gli utenti e i ruoli possono eseguire, su quali risorse e in quali condizioni. Per scoprire come creare una policy basata sull'identità, consulta Creazione di policy IAM nella IAM User Guide.

Con le policy basate sull'identità IAM, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare il principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associata. Per maggiori informazioni su tutti gli elementi che puoi utilizzare in una policy JSON, consulta il riferimento agli elementi della policy JSON di IAM nella IAM User Guide.

Esempi di policy basate sull'identità per Amazon Nimble Studio

Per visualizzare esempi di politiche basate sull'identità di Nimble Studio, consulta. Esempi di policy basate sull'identità per Amazon Nimble Studio

## Politiche basate sulle risorse all'interno di Nimble Studio

| | |
| --- | --- |
| Supporta le policy basate su risorse | No |

Nimble Studio non supporta politiche basate sulle risorse o l'accesso tra account. Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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. Per la risorsa a cui è allegata la policy, la policy definisce quali azioni uno specifico principale può eseguire su quella risorsa e a quali condizioni. Specificare un principale in una politica basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

## Azioni politiche per Nimble Studio

| | |
|---|---|
| Supporta le operazioni di policy | Sì |

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

L'elemento `Action`di una policy JSON descrive le operazioni 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. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni 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.

Per visualizzare un elenco delle azioni di Nimble Studio, consulta Azioni definite da Amazon Nimble Studio nel Service Authorization Reference.

Le azioni politiche in Nimble Studio utilizzano il seguente prefisso prima dell'azione:

```
nimble
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di Nimble Studio, consulta. Esempi di policy basate sull'identità per Amazon Nimble Studio

## Risorse politiche per Nimble Studio

| | |
|---|---|
| Supporta le risorse di policy | Sì |

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

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, come le operazioni di elenco, usa un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare esempi di politiche basate sull'identità di Nimble Studio, consulta. Esempi di policy basate sull'identità per Amazon Nimble Studio

## Chiavi relative alle condizioni delle politiche per Nimble Studio

| | |
|---|---|
| Supporta chiavi di condizione delle policy | Sì |

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

L'`Condition`elemento (o `Condition` **`block`**`) lets you specify conditions in which a statement is in effect. The `Condition` elemento) è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione

0Rlogica. Tutte le condizioni devono essere soddisfatte prima che vengano concesse le autorizzazioni della dichiarazione.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere a un utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome utente. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e 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 di IAM.

Per visualizzare esempi di politiche basate sull'identità di Nimble Studio, consulta. Esempi di policy basate sull'identità per Amazon Nimble Studio

## Accedi agli elenchi di controllo () ACLs in Nimble Studio

| | |
|---|---|
| Supporti ACLs | No |

Nimble Studio non supporta gli elenchi di controllo degli accessi (ACLs). ACLs controlla quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

## Controllo degli accessi basato sugli attributi (ABAC) con Nimble Studio

| | |
|---|---|
| Supporta ABAC (tag nelle policy) | Sì |

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. Quindi si progettano politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per configurare ABAC, consulta Use Attribute-based access control (ABAC) nella IAM User Guide.

## Utilizzo di credenziali temporanee con Nimble Studio

| | |
|---|---|
| Supporta le credenziali temporanee | Sì |

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi Console di gestione AWS utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Switching to a role (console) nella IAM User Guide.

Puoi creare manualmente credenziali temporanee utilizzando l' AWS API AWS CLI or. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

## Autorizzazioni principali multiservizio per Nimble Studio

| | |
|---|---|
| Supporta le autorizzazioni delle entità principali | Sì |

## Ruoli di servizio per Nimble Studio

| | |
|---|---|
| Supporta i ruoli di servizio | Sì |

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. I ruoli di servizio forniscono l'accesso solo all'interno del tuo account e non possono essere utilizzati per concedere l'accesso ai servizi di altri account. Un amministratore può creare, modificare ed

eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Nimble Studio. Modifica i ruoli di servizio solo quando Nimble Studio fornisce indicazioni in tal senso.

### Ruoli collegati ai servizi per Nimble Studio

| | |
|---|---|
| Supporta i ruoli collegati ai servizi | No |

Nimble Studio non supporta i ruoli collegati ai servizi. 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 conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta Servizi AWS That work with IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Esempi di policy basate sull'identità per Amazon Nimble Studio

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Nimble Studio. Inoltre, non possono eseguire attività utilizzando l' AWS API Console di gestione AWS AWS CLI, o. Un amministratore deve creare policy IAM che concedano a utenti e ruoli l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno. L'amministratore devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating policies on the JSON nella IAM User Guide.

Argomenti

- Best practice delle policy

### Best practice delle policy

Le policy basate su identità sono molto efficaci. Determinano se qualcuno può creare, accedere o eliminare le risorse di Nimble Studio nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia a utilizzare le politiche AWS gestite: per iniziare a utilizzare Nimble Studio rapidamente, utilizza le politiche AWS gestite per concedere ai dipendenti le autorizzazioni di cui hanno bisogno. Queste policy sono già disponibili nell'account e sono gestite e aggiornate da AWS. Per ulteriori informazioni, consulta Introduzione all'utilizzo delle autorizzazioni con policy AWS gestite nella Guida per l'utente IAM.
- Assegna il privilegio minimo: quando crei policy personalizzate, concedi solo le autorizzazioni indispensabili per eseguire un'attività. Inizia con un set di autorizzazioni minimo e concedi autorizzazioni aggiuntive quando necessario. Questo è più sicuro che iniziare con autorizzazioni che siano troppo permissive e cercare di limitarle in un secondo momento. Per ulteriori informazioni, consulta Assegnare il privilegio minimo nella Guida per l'utente IAM.
- Abilita l'MFA per operazioni sensibili: per una maggiore sicurezza, richiedi agli utenti di utilizzare l'autenticazione a più fattori (MFA) per accedere a risorse sensibili o operazioni API. Per ulteriori informazioni, consulta Using Multi-Factor Authentication (MFA) AWS nella IAM User Guide.
- Utilizza le condizioni delle policy per una maggiore sicurezza: nella misura in cui è pratico, definisci le condizioni in cui le policy basate sull'identità consentono l'accesso a una risorsa. Ad esempio, è possibile scrivere condizioni per specificare un intervallo di indirizzi IP consentiti dai quali deve provenire una richiesta. È anche possibile scrivere condizioni per consentire solo le richieste all'interno di un intervallo di date o ore specificato oppure per richiedere l'utilizzo di SSL o MFA. Per ulteriori informazioni, consulta IAM JSON Policy elements: Condition nella IAM User Guide.

## AWS politiche gestite per Amazon Nimble Studio

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle da soli. Creare policy gestite dal cliente IAM per fornire 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 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 occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS 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 policy gestita da AWS quando viene avviata 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 ReadOnlyAccess AWS gestita 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.

I tuoi utenti finali accederanno ad Amazon Nimble Studio principalmente utilizzando il portale Nimble Studio. Quando crei il tuo studio utilizzando StudioBuilder o la console Nimble Studio, viene creato un ruolo IAM per ogni persona dello studio: l'amministratore dello studio e l'utente dello studio. Ciascuno ha la rispettiva policy gestita da IAM allegata. Il portale Nimble Studio offre un'esperienza in cui gli utenti possono solo elencare e utilizzare le risorse a cui hanno il permesso di accedere.

Il portale Nimble Studio offre un'esperienza in cui gli utenti possono solo elencare e utilizzare le risorse a cui hanno accesso e il portale dipende dal contenuto di queste politiche per funzionare correttamente. Gli utenti finali di Nimble Studio utilizzeranno il portale per accedere al proprio studio cloud. Pertanto, quando gli amministratori creano il proprio studio utilizzando StudioBuilder, viene creato un ruolo IAM per ogni persona che deve accedere allo studio. Ciò include l'amministratore dello studio e l'utente dello studio, ciascuno con la rispettiva policy gestita da IAM allegata.

Per un elenco e le descrizioni delle politiche relative alle funzioni lavorative, consulta le politiche AWS gestite per le funzioni lavorative nella Guida per l'utente IAM.

## AWS politica gestita: **`AmazonNimbleStudio-LaunchProfileWorker`**

È possibile allegare la policy `AmazonNimbleStudio-LaunchProfileWorker` alle identità IAM.

Allega questa policy alle EC2 istanze create da Nimble Studio Builder per concedere l'accesso alle risorse necessarie agli addetti ai profili di lancio di Nimble Studio.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- ds - Consente LaunchProfile ai lavoratori di scoprire le informazioni di connessione relative a ciò che è associato a un. AWS Managed Microsoft AD LaunchProfile
- ec2 - Consente agli LaunchProfile operatori di scoprire le informazioni sui gruppi di sicurezza e sulle sottoreti per connettersi a un. LaunchProfile
- fsx: consente agli LaunchProfile operatori di scoprire le informazioni di connessione ai FSx volumi Amazon associati a un LaunchProfile.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

## AWS politica gestita: **AmazonNimbleStudio-StudioAdmin**

È possibile allegare la policy AmazonNimbleStudio-StudioAdmin alle identità IAM.

Associa questa policy al ruolo di amministratore associato al tuo studio per concedere l'accesso alle risorse di Amazon Nimble Studio associate all'amministratore dello studio e alle risorse di studio correlate in altri servizi.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- nimble: consente agli utenti di Studio di accedere alle risorse Nimble che sono state loro delegate da. StudioAdmins
- sso - Consente agli utenti di Studio la possibilità di visualizzare i nomi degli altri utenti dello studio.
- identitystore - Consente agli utenti di Studio la possibilità di visualizzare i nomi degli altri utenti dello studio.
- ds - Consente a Nimble Studio di aggiungere workstation virtuali a quelle AWS Managed Microsoft AD associate allo studio.
- ec2 - Consente a Nimble Studio di collegare workstation virtuali al VPC configurato.
- fsx: consente a Nimble Studio di connettere workstation virtuali ai volumi Amazon configurati. FSx
- cloudwatch: consente a Nimble Studio di recuperare le metriche. CloudWatch

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
```

```
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
```

```
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

## AWS politica gestita: **AmazonNimbleStudio-StudioUser**

È possibile allegare la policy AmazonNimbleStudio-StudioUser alle identità IAM.

Allega questa policy al ruolo Utente associato al tuo studio per concedere l'accesso alle risorse di Amazon Nimble Studio associate all'utente dello studio e alle risorse di studio correlate in altri servizi.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- nimble: consente agli utenti di Studio di accedere alle risorse Nimble che sono state loro delegate da. StudioAdmins
- sso - Consente agli utenti di Studio la possibilità di visualizzare i nomi degli altri utenti dello studio.
- identitystore - Consente agli utenti di Studio la possibilità di visualizzare i nomi degli altri utenti dello studio.
- ds - Consente a Nimble Studio di aggiungere workstation virtuali a quelle AWS Managed Microsoft AD associate allo studio.

- ec2 - Consente a Nimble Studio di collegare workstation virtuali al VPC configurato.
- fsx: consente a Nimble Studio di connettere workstation virtuali ai volumi Amazon configurati. FSx

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
```

```
}
```

## Nimble Studio si aggiorna alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Nimble Studio da quando questo servizio ha iniziato a tracciare queste modifiche.

| Modifica | Descrizione | Data |
| --- | --- | --- |
| AWS politica gestita: `AmazonNimbleStudio-StudioUser` : policy aggiornata | Amazon Nimble Studio ha aggiornato una policy per utilizzare la versione più recente del servizio Identity Store. | 22 settembre 2023 |
| AWS politica gestita: `AmazonNimbleStudio-StudioAdmin` : policy aggiornata | Amazon Nimble Studio ha aggiornato una policy per utilizzare la versione più recente del servizio Identity Store. | 22 settembre 2023 |
| AWS politica gestita: `AmazonNimbleStudio-StudioUser` : policy aggiornata | Amazon Nimble Studio ha aggiornato una policy per consentire agli utenti dello studio di visualizzare i backup delle proprie workstation. | 20 dicembre 2022 |
| AWS politica gestita: `AmazonNimbleStudio-StudioAdmin` : policy aggiornata | Amazon Nimble Studio ha aggiornato la policy per consentire agli amministratori dello studio di visualizzare i backup delle proprie workstation. | 20 dicembre 2022 |
| AWS politica gestita: `AmazonNimbleStudio-StudioUser` : policy aggiornata | Amazon Nimble Studio ha aggiornato una policy per consentire agli amministratori | 11 novembre 2021 |

| Modifica | Descrizione | Data |
| --- | --- | --- |
| | dello studio di recuperare i parametri. CloudWatch | |
| AWS politica gestita: AmazonNimbleStudio-StudioUser: policy aggiornata | Amazon Nimble Studio ha aggiornato la policy per consentire agli utenti dello studio di avviare e arrestare le proprie workstation. | 1° novembre 2021 |
| AWS politica gestita: AmazonNimbleStudio-StudioAdmin: policy aggiornata | Amazon Nimble Studio ha aggiornato la policy per consentire agli amministratori dello studio di avviare e arrestare le proprie workstation. | 1° novembre 2021 |
| AWS politica gestita: AmazonNimbleStudio-StudioUser: policy aggiornata | Amazon Nimble Studio ha aggiornato la policy per consentire in modo condizionale l'accesso alle risorse della sessione di streaming basate su invece di. `nimble:ownedBy` `nimble:createdBy` | 16 agosto 2021 |
| AWS politica gestita: AmazonNimbleStudio-StudioUser: nuova policy | Amazon Nimble Studio ha aggiunto una nuova policy che consente l'accesso alle risorse associate all'utente dello studio e alle risorse di studio correlate in altri servizi. | 28 Aprile 2021 |

| Modifica | Descrizione | Data |
| --- | --- | --- |
| AWS politica gestita: `AmazonNimbleStudio-StudioAdmin` : nuova policy | Amazon Nimble Studio ha aggiunto una nuova policy che consente l'accesso alle risorse associate all'amministratore dello studio e alle risorse di studio correlate in altri servizi. | 28 Aprile 2021 |
| AWS politica gestita: `AmazonNimbleStudio-LaunchProfileWorker` : nuova policy | Amazon Nimble Studio ha aggiunto una nuova policy che consente l'accesso alle risorse necessarie agli addetti ai profili di lancio di Nimble Studio. | 28 Aprile 2021 |
| Amazon Nimble Studio ha iniziato a tracciare le modifiche | Amazon Nimble Studio ha iniziato a tracciare le modifiche per le sue politiche AWS gestite. | 28 Aprile 2021 |

## Prevenzione del problema "confused deputy" tra servizi

Il problema della confusione degli agenti delegati è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità con maggiori privilegi a eseguire l'azione. In effetti AWS, l'impersonificazione tra diversi servizi può portare alla confusione del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio di chiamata può essere manipolato in modo da utilizzare le sue autorizzazioni per agire sulle risorse di un altro cliente in un modo a cui altrimenti non dovrebbe avere l'autorizzazione di accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi contestuali `aws:SourceArn` e le condizioni `aws:SourceAccount` globali nelle politiche delle risorse per limitare le autorizzazioni che Identity and Access Management (IAM) concede ad Amazon Nimble Studio per accedere alle tue risorse. Se utilizzi entrambe le chiavi di contesto della condizione globale, il `aws:SourceAccount` valore

e l'account nel `aws:SourceArn` valore devono utilizzare lo stesso ID account quando vengono utilizzati nella stessa dichiarazione politica.

Il valore di `aws:SourceArn` deve essere l'ARN dello studio e `aws:SourceAccount` deve essere l'ID del tuo account. Non saprai cos'è l'ID dello studio finché non verrà creato lo studio, perché è generato da Nimble Studio. Una volta creato lo studio, puoi aggiornare la politica di fiducia con l'ID dello studio finale impostato come. `aws:SourceArn`

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o se stai specificando più risorse, usa la chiave di condizione di contesto `aws:SourceArn` globale con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio `arn:aws:nimble::123456789012:*`.

I tuoi utenti finali assumono il tuo ruolo di studio quando accedono al portale Nimble Studio. Quando crei il tuo studio, AWS configura il ruolo e valuta la politica. AWS valuta la policy ogni volta che uno dei tuoi utenti accede al portale Nimble Studio. Quando crei uno studio, non puoi modificare il. `aws:SourceArn` Dopo aver finito di creare il tuo studio, puoi usare StudioARN per. `aws:SourceArn`

L'esempio seguente è una politica relativa all'assunzione del ruolo che mostra come utilizzare le chiavi di contesto `aws:SourceArn` e di contesto della condizione `aws:SourceAccount` globale in Nimble Studio per evitare il confuso problema del vice.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
```

```
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

# Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Nimble Studio

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

Argomenti



## Non sono autorizzato a eseguire un'azione in Nimble Studio.

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 `nimble:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 nimble: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 `nimble:`*`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 che indica che non sei autorizzato a eseguire l'`iam:PassRole`azione, contatta l'amministratore per ricevere assistenza. Chiedi loro di aggiornare le tue politiche per consentirti di trasferire un ruolo a Nimble Studio.

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. A tale scopo, sono necessarie le autorizzazioni per trasferire il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente denominato `johndoe` tenta di utilizzare la console per eseguire un'azione in Nimble Studio. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. John non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, John chiede al suo amministratore di aggiornare le sue politiche per concedere l'autorizzazione a eseguire l'`iam:PassRole`azione.

## Desidero visualizzare le mie chiavi di accesso.

Amazon Nimble Studio non fornisce chiavi di accesso. Per ulteriori informazioni sulle chiavi di accesso segrete, consulta Managing access keys nella IAM User Guide.

> **Important**
>
> Non fornire le tue chiavi di accesso a terzi, nemmeno per aiutarti a trovare il tuo ID utente canonico. Se lo facessi, daresti a qualcuno accesso permanente al tuo account.

Quando crei una coppia di chiavi di accesso, ti viene richiesto di salvare l'ID della chiave di accesso e la chiave di accesso segreta in un luogo sicuro. La chiave di accesso segreta è disponibile solo al momento della creazione. Se perdi la chiave di accesso segreta, aggiungi nuove chiavi di accesso all'utente. È possibile avere massimo due chiavi di accesso. Se ne hai già due, elimina una key pair prima di crearne una nuova. Per visualizzare le istruzioni, consulta Managing access keys nella IAM User Guide.

## Sono un amministratore e voglio consentire ad altri di accedere a Nimble Studio.

Per consentire ad altri di accedere a Nimble Studio, crea un'entità IAM (utente o ruolo) per la persona o l'applicazione che necessita di accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Quindi, allega una policy all'entità che concede loro le autorizzazioni corrette.

Nimble Studio ti fornisce tutto il `AmazonNimbleStudio-StudioUser` necessario. Console di gestione AWS L'amministratore IT che gestisce la console utilizza questa politica per concedere l'accesso allo studio ad altri.

Per un tutorial sull'utilizzo della politica di amministrazione, Configurazione per Nimble Studio consulta la guida. Per scoprire come collegare le policy esistenti agli utenti, come le policy relative agli utenti e ai profili di avvio, consulta Creazione di utenti IAM (console).

Per informazioni sull'importazione delle policy, consulta Creazione del primo utente e gruppo delegati IAM nella IAM User Guide.

## Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Nimble Studio.

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Nimble Studio supporta queste funzionalità, consulta. Come funziona Amazon Nimble Studio con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS 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 scoprire come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.

- Per scoprire la differenza tra l'utilizzo dei ruoli e delle politiche basate sulle risorse per l'accesso tra account diversi, consulta In che modo i ruoli IAM differiscono dalle politiche basate sulle risorse nella Guida per l'utente IAM.

# Registrazione e monitoraggio degli eventi di sicurezza con Nimble Studio

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon Nimble Studio e delle tue AWS soluzioni. Raccogli i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica uno.

AWS e Nimble Studio forniscono strumenti per monitorare le risorse e rispondere a potenziali incidenti, tra cui una Guida per l'utente. Registrazione delle chiamate di Nimble Studio utilizzando AWS CloudTrailAWS CloudFormation

Per ulteriori informazioni su come funziona Amazon Nimble Studio CloudFormation, inclusi esempi di modelli JSON e YAML, consulta il riferimento alle risorse e alle proprietà di Amazon Nimble Studio nella Guida per l'utente. AWS CloudFormation Per capire come usare i modelli, consulta i concetti CloudFormation.CloudFormation

Argomenti

- Registrazione delle chiamate di Nimble Studio utilizzando AWS CloudTrail

## Registrazione delle chiamate di Nimble Studio utilizzando AWS CloudTrail

Amazon Nimble Studio è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Nimble Studio. CloudTrail acquisisce tutte le chiamate API per Nimble Studio come eventi. Le chiamate acquisite includono chiamate dalla console Nimble Studio e chiamate in codice alle operazioni di Amazon Nimble Studio.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Nimble Studio. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta a Nimble Studio, l'indirizzo IP

da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

## Informazioni su Nimble Studio in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in Nimble Studio, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per Nimble Studio, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail

Per ulteriori informazioni, consulta gli argomenti seguenti:

Panoramica della creazione di un percorso

CloudTrail servizi e integrazioni supportati

Configurazione delle notifiche Amazon SNS per CloudTrail

Ricezione di file di CloudTrail registro da più regioni

Ricezione di file di CloudTrail registro da più account

Le azioni di Nimble Studio vengono registrate CloudTrail e documentate nell'Amazon Nimble Studio API Reference. Ad esempio, le chiamate alle CreateStudio DeleteStudio azioni GetStudio e generano voci nei file di registro. CloudTrail

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 credenziali utente root o AWS Identity and Access Management (IAM).
- 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 .

Per ulteriori informazioni, vedete l'elemento CloudTrail user Identity.

## Comprendere le voci dei file di registro di Nimble Studio

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

Questo esempio JSON mostra tre azioni:

- ACTION_1: CreateStudio
- AZIONE_2: GetStudio
- AZIONE_3: DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
```

```
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
```

```
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
```

```
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


Nell'esempio, noterai che gli eventi mostrano la regione, l'indirizzo IP e altri «RequestParameters» come "" e userRoleArn "adminRoleArn" che ti aiuteranno a identificare l'evento. Puoi vedere l'ora e

la data nel campo «CreationDate» e l'origine della richiesta, contrassegnata come «EventSource»: «nimble.amazonaws.com».

CloudTrail è abilitato sul tuo account quando crei l'account. Account AWS Quando si verifica un'attività in IAM o AWS STS, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS.

AWS CloudTrail acquisisce tutte le chiamate API per IAM e AWS Security Token Service (AWS STS) come eventi, incluse le chiamate dalla console e le chiamate API. Per ulteriori informazioni sull'utilizzo CloudTrail con IAM and AWS STS, consulta Registrazione delle chiamate IAM e AWS STS API con. AWS CloudTrail

Per ulteriori informazioni su CloudTrail, consulta la Guida per AWS CloudTrail l'utente.

Per informazioni su altri servizi di monitoraggio offerti da Amazon, consulta la Amazon CloudWatch User Guide.

# Convalida della conformità per Amazon Nimble Studio

Amazon Nimble Studio segue il modello di responsabilità condivisa e la conformità è condivisa tra AWS i nostri clienti.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di 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 CSPM— 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.

## Sicurezza dell'infrastruttura in Amazon Nimble Studio

In quanto servizio gestito, Amazon Nimble Studio 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.

Utilizzi chiamate API AWS pubblicate per accedere a Nimble Studio 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.

# Le migliori pratiche di sicurezza per Nimble Studio

Amazon Nimble Studio offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

## Monitoraggio

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Nimble Studio e delle tue AWS soluzioni. Per ulteriori informazioni sul monitoraggio e sulla risposta agli eventi, consulta. Registrazione e monitoraggio degli eventi di sicurezza con Nimble Studio

## Protezione dei dati

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare account individuali con AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È consigliabile TLS 1.2 o versioni successive.

- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Consigliamo di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero come un campo Nome. Ciò include quando lavori con Amazon Nimble Studio o altro Servizi AWS utilizzando la console, l'API o AWS SDKs. AWS CLI Tutti i dati che inserisci in Amazon Nimble Studio o in altri servizi potrebbero essere raccolti per essere inclusi nei log di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

## Autorizzazioni

Gestisci l'accesso alle AWS risorse utilizzando utenti, ruoli IAM e concedendo il minimo privilegio agli utenti. Stabilisci politiche e procedure di gestione delle credenziali per creare, distribuire, ruotare e revocare le credenziali di accesso. AWS Per ulteriori informazioni, consulta la sezione best practice IAM nella guida per l'utente IAM.

# Support per Nimble Studio

Questa sezione fornisce le opzioni di supporto per Nimble Studio, ad esempio come ottenere assistenza durante la distribuzione o l'utilizzo del servizio e delle relative applicazioni.

Indice



## Forum di Nimble Studio

Se hai domande su Nimble Studio, puoi visitare il forum di Nimble Studio. Qui puoi ottenere risposte dai moderatori della community e del AWS forum sulle funzionalità di Nimble Studio, sui problemi tecnici e sulla risoluzione dei problemi.

## Supporto per le applicazioni

Nimble Studio fornisce documentazione aggiuntiva per le seguenti applicazioni.

### AWSThinkboxDeadline

Per assistenza con la tua render farm o per scoprire come Deadline funziona, vedi AWSThinkboxDeadline documentazione.

### Nimble Studio File Transfer

Per sapere come funziona File Transfer, consulta la Guida per l'utente di Nimble Studio File Transfer.

## Supporto Centro

Il Supporto Centro è un hub per la creazione e la gestione dei casi di supporto. Fornisce accesso a una varietà di risorse, tra cui soluzioni tecniche e di fatturazione, un centro di conoscenza, video del knowledge center, AWS documentazione, oltre a formazione e certificazione.

# Supporto piani

Supporto i piani consentono di ottimizzare le prestazioni, garantire la sicurezza, evitare tempi di inattività e controllare i costi. Per ulteriori informazioni sui Supporto piani, consulta Confronta Supporto i piani.

Per ulteriori informazioni su come AWS possiamo supportarti, visita la pagina Contattaci.

# Cronologia dei documenti

- Versione API: ultima
- Ultimo aggiornamento della documentazione: 2 ottobre 2024

La tabella seguente descrive le modifiche importanti in ogni versione della Nimble Studio Administrator Guide.

| Modifica | Descrizione | |
|---|---|---|
| Avviso di fine del supporto | Avviso di fine del supporto: il 22 ottobre 2024, il supporto per Amazon Nimble Studio AWS verrà interrotto. Dopo il 22 ottobre 2024, non potrai più accedere alla console Nimble Studio o alle risorse di Nimble Studio. | 2 ottobre 2024 |
| AWS aggiornamenti delle politiche gestite | Sono state aggiornate le `AmazonNimbleStudio-StudioAdmin` politiche `AmazonNimbleStudio-StudioUser` e per utilizzare la versione più recente del AWS IAM Identity Center servizio. | 22 settembre 2023 |
| Nuovo servizio e guida | Questa è la versione iniziale di Amazon Nimble Studio e della Amazon Nimble Studio Administrator Guide. | 19 giugno 2023 |

# AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS