POST EDIT. ADDED PROOFREAD. ADDED PP1

Amazon Nimble Studio

Amazon Nimble Studio: POST EDIT. ADDED PROOFREAD. ADDED PP1

Table of Contents

Hinweis zum Ende des Supports: Am 22. Oktober 2024 AWS wird der Support für Amazon Nimble Studio eingestellt. Nach dem 22. Oktober 2024 können Sie nicht mehr auf die Nimble Studio-Konsole oder die Nimble Studio-Ressourcen zugreifen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Was ist Amazon Nimble Studio?

Nimble Studio bietet Infrastruktur und zentrales Management für eine Reihe von Anwendungen und Diensten, mit denen Künstler visuelle Effekte, Animationen und Spielinhalte in der Cloud produzieren können.

Mit Nimble Studio erhalten Sie wichtige Tools für die Benutzer- und Gruppenverwaltung. Sie können auch Anwendungen hinzufügen und verwalten, darunter AWS Thinkbox und Nimble Studio File Transfer.

Nimble Studio verfügt über eine einheitliche Oberfläche, die all Ihre Studioressourcen an einem Ort vereint. Sie können Benutzer einbinden, Anwendungen zuweisen und ihnen spezifische Berechtigungen für ihre jeweilige Funktion zuweisen. Nimble Studio erfordert keine AWS Erfahrung und Sie können es in etwa fünf Minuten einrichten.

Inhalt

Features und Vorteile

Hier sind einige der Funktionen und Vorteile, die Sie mit Nimble Studio erhalten:

- Verwenden Sie Nimble Studio kostenlos; zahlen Sie nur für die Studioressourcen, die Ihre Anwendungen nutzen.
- Verwalten Sie Ihr Studio zentral, überprüfen Sie seinen Status und gewinnen Sie umfassende Einblicke in den Betrieb.
- Fügen Sie Nimble Studio-Anwendungen, Benutzer und Gruppen hinzu und verwalten Sie sie und fügen Sie Berechtigungen hinzu.
- Verwalten Sie den Zugriff auf Studio-Ressourcen sicher mit AWS Identity and Access Management (IAM-) Richtlinien und Rollen.
- Verwalten Sie die Anmeldesicherheit für Studio-Benutzer und externe Identitätsanbieter mit AWS IAM Identity Center (IAM Identity Center).

- Organisieren und finden Sie mühelos Studio-Ressourcen mit Tags zu Ihren Studio-Ressourcen.

Verwandte Anwendungen

Nimble Studio bietet Anwendungen für Ersteller digitaler Inhalte, um ein Cloud-basiertes Studio für die Produktion von visuellen Effekten (VFX), Animationen und interaktiven Inhalten zu betreiben.

Sie können diese Anwendungen auf Ihrem lokalen Computer oder in der Cloud mit einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance installieren. Sie können auch Amazon Simple Storage Service (Amazon S3) verwenden, um digitale Medienressourcen sicher zu übertragen und zu speichern. Das bedeutet, dass Sie Nimble Studio verwenden können, um die Kosten für physische Infrastruktur, Ausrüstung und technisches Personal zu senken.

Nimble Studio bietet derzeit die folgenden Anwendungen:

- AWS Thinkbox: Thinkbox Die Software beinhaltet den Render-Farm-Manager Thinkbox Deadline und das 3D-Plugin Thinkbox Krakatoa. Sie können Folgendes verwenden … Thinkbox Software, mit der Sie die kreative Leistung Ihres Studios vor Ort, in der Cloud mit Amazon EC2 oder einer Kombination aus beidem steigern können. Weitere Informationen finden Sie unter AWS Thinkbox Produkte.
- Nimble Studio File Transfer: File Transfer beschleunigt die Übertragung von Medieninhalten digitaler Medienressourcen zu und von Amazon S3. File Transfer bietet eine grafische Benutzeroberfläche, mit der Sie schnell Tausende großer Mediendateien verschieben können. Weitere Informationen finden Sie unter Was ist Nimble Studio File TransferSeite.

Preise für Nimble Studio

Die Einrichtung von Nimble Studio und die Nutzung zur Verwaltung Ihrer Studio-Infrastruktur, Benutzer, Sicherheit und Dienste sind kostenlos.

Wenn Sie jedoch Dienste und Anwendungen in Ihrem Studio einrichten, werden Ihnen möglicherweise Speicherplatz und andere Studioressourcen in Rechnung gestellt. Weitere Informationen zu den Preisen für Nimble Studio-Anwendungen finden Sie auf der Preisseite der jeweiligen Anwendung.

Informationen zur Verwaltung Ihrer AWS Kosten finden Sie unter AWS Cost Explorer Serviceund AWS Budgets.

Fangen Sie mit Nimble Studio an

Die Einrichtung und Bereitstellung von Nimble Studio dauert etwa fünf Minuten.

Nachdem Sie sich mit den Konzepten und der Terminologie von Nimble Studio vertraut gemacht haben, finden Sie weitere Informationen unter Erste Schritte mit Amazon Nimble Studio. Darin finden Sie step-by-step Anweisungen zur Bereitstellung Ihres Studios.

Konzepte und Terminologie für Amazon Nimble Studio

Um Ihnen die ersten Schritte mit Amazon Nimble Studio zu erleichtern und zu verstehen, wie es funktioniert, können Sie sich auf die wichtigsten Konzepte und Begriffe in diesem Handbuch beziehen.

Schlüsselfeatures

Amazon Nimble Studio

Amazon Nimble Studio ermöglicht es Kreativstudios AWS-Service , visuelle Effekte, Animationen und interaktive Inhalte vollständig in der Cloud zu produzieren, von der Storyboard-Skizze bis zum endgültigen Ergebnis.

Amazon Nimble Studio-Konsole

Die Nimble Studio-Konsole ist ein Teil der AWS Management Console, der unseren Admin-IT-Kunden gewidmet ist. In dieser Konsole erstellen Administratoren ihr Cloud-Studio und verwalten viele Einstellungen. Auf der Studio-Manager-Seite können Sie beispielsweise Ressourcen hinzufügen oder entfernen, Anwendungen hinzufügen und Benutzern und Gruppen Berechtigungen gewähren.

Amazon Nimble Studio-Portal

Das Nimble Studio-Portal bietet eine Benutzeroberfläche für day-to-day Interaktionen mit Nimble Studio-Anwendungen und -Diensten. Benutzer melden sich mit ihrem Benutzernamen und Passwort direkt beim Portal an, ohne mit dem interagieren zu müssen. AWS Management Console

Nimble Studio File Transfer

File Transfer beschleunigt die Übertragung von Medieninhalten digitaler Medienressourcen zu und von Amazon Simple Storage Service (Amazon S3). File Transfer bietet eine grafische Benutzeroberfläche, mit der Sie schnell Tausende großer Mediendateien verschieben können. Weitere Informationen finden Sie unter Was ist Nimble Studio File TransferSeite.

AWS Thinkbox

Thinkbox Die Software beinhaltet den Render-Farm-Manager Thinkbox Deadline und das 3D-Plugin Thinkbox Krakatoa. Sie können Folgendes verwenden … Thinkbox Software, mit der Sie die kreative Leistung Ihres Studios vor Ort, in der Cloud mit Amazon EC2 oder einer Kombination aus beidem steigern können. Weitere Informationen finden Sie unter AWS Thinkbox Produkte.

Schlüsselbegriffe und Terminologie

AWS verwaltete Richtlinien

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Eigenständige Richtlinie bedeutet, dass die Richtlinie ihren eigenen Amazon-Ressourcennamen (ARN) hat, der den Richtliniennamen enthält. Zum Beispiel ist arn:aws:iam: IAMRead OnlyAccess :aws:policy/ eine verwaltete Richtlinie. AWS Weitere Informationen dazu ARNs finden Sie unter ARNsIAM.

AWS verwaltete Richtlinien werden verwendet, um Berechtigungen für allgemeine Aufgabenfunktionen zu gewähren. Die Richtlinien für Jobfunktionen werden beibehalten und aktualisiert AWS , sobald neue Dienste und API-Operationen eingeführt werden. Zum Beispiel bietet die AdministratorAccessJob-Funktion vollen Zugriff und die Delegierung von Berechtigungen für jeden Dienst und jede Ressource in AWS. AWS Verwaltete Richtlinien mit teilweisem Zugriff wie AmazonMobileAnalyticsWriteOnlyAccess Amazon EC2 ReadOnlyAccess können dagegen bestimmte Zugriffsebenen bereitstellen, AWS-Services ohne vollen Zugriff zu gewähren. Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Grundlegendes zu Zusammenfassungen der Zugriffsebenen in den Richtlinienzusammenfassungen.

AWS Management Console

Das AWS Management Consoleist eine Webanwendung, die Zugriff auf eine breite Palette von Servicekonsolen für die Verwaltung bietet. AWS-Services

Jeder Dienst umfasst auch eine eigene Konsole. Diese Konsolen bieten eine breite Palette von Tools für Cloud Computing. Es gibt sogar einen Service, der bei der Abrechnung und beim Kostenmanagement hilft.

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center ist ein AWS Service, der es einfach macht, den Zugriff auf mehrere AWS-Konten Geschäftsanwendungen zentral zu verwalten. Mit IAM Identity Center können Sie Benutzern von einem zentralen Ort aus Single Sign-On-Zugriff auf alle ihnen zugewiesenen Konten und Anwendungen gewähren. Sie können den Zugriff mehrerer Konten und die Benutzerberechtigungen für alle Ihre Konten auch zentral verwalten. AWS Organizations Weitere Informationen finden Sie unter AWS IAM Identity Center FAQs.

AWS PrivateLink

AWS PrivateLink bietet private Konnektivität zwischen VPCs AWS-Services, und Ihren lokalen Netzwerken, ohne dass Ihr Datenverkehr dem öffentlichen Internet ausgesetzt wird. AWS PrivateLink macht es einfach, Dienste über verschiedene Konten hinweg zu verbinden und. VPCs AWS PrivateLinkist gegen eine monatliche Gebühr erhältlich, die Ihnen AWS-Konto in Rechnung gestellt wird.

Erstellung digitaler Inhalte (DCC)

Die Erstellung digitaler Inhalte (DCC) bezieht sich auf die Kategorie von Anwendungen, die zur Erstellung kreativer Inhalte verwendet werden, darunter Blender, Nuke, Maya, und Houdini.

Regionen

Nimble Studio bietet elf Optionen zur AWS-Regionen Auswahl und Bereitstellung Ihres Studios. In den Regionen ist die grundlegende Studio-Infrastruktur vorhanden, z. B. Ihre Daten und Anwendungen.

Die Region sollte Ihren Studio-Benutzern am nächsten liegen. Dies reduziert die Verzögerung und verbessert die Datenübertragungsgeschwindigkeit.

Studio

Ein Studio ist der Container auf oberster Ebene für andere Ressourcen im Zusammenhang mit Nimble Studio. Ihr Cloud-Studio verwaltet das Nimble Studio-Webportal und die Verbindungen zu wichtigen Ressourcen in Ihrem Unternehmen, AWS-Konto wie z. B. Ihrer VPC, Ihrem Benutzerverzeichnis und Ihren Speicherverschlüsselungsschlüsseln.

Studio-Anwendungen

Studio-Komponenten sind Konfigurationen im Nimble Studio eines Kunden, die dem Service mitteilen, wie er auf Ressourcen wie Dateisysteme, Lizenzserver und Renderfarmen in Ihrem AWS-Konto zugreifen kann.

Nimble Studio enthält eine Reihe von Untertypen von Studio-Komponenten, darunter ein gemeinsam genutztes Dateisystem, eine Rechenfarm, Active Directory und eine Lizenzkomponente. Diese Untertypen beschreiben Ressourcen, die Ihr Studio verwenden soll.

Studio-Ressourcen

Studioressourcen sind ein Begriff, der die Dinge zusammenfasst, die ein Studio für seinen täglichen Betrieb benötigt. Bei der Beschreibung, wie Ressourcen in die Infrastruktur eines Cloud-Studios passen, können sie auch als Studiokomponenten bezeichnet werden.

Tags

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, den Sie definieren.

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren. Sie könnten beispielsweise eine Reihe von Tags für die Amazon Elastic Compute Cloud (Amazon EC2) -Instances Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können. Mithilfe von Tags können Sie auch die gemeinsam genutzten Dateisysteme und Renderfarmen Ihres Unternehmens in Nimble Studio integrieren, sodass Ihre Arbeitsabläufe nicht unterbrochen werden, während Sie Ihre Belegschaft in die Cloud verlagern.

Mithilfe von Tags können Sie Ihre AWS Ressourcen nach Zweck, Eigentümer oder Umgebung kategorisieren. Dies ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen. Sie können eine bestimmte Ressource anhand der Tags, die Sie ihr zugewiesen haben, schnell identifizieren.

Einrichtung für Nimble Studio

Dieses Tutorial richtet sich an Administratorbenutzer, die ein Amazon Nimble Studio einrichten möchten.

In den folgenden Abschnitten werden Sie durch die Schritte geführt, die Sie ausführen müssen, bevor Sie ein Studio in Nimble Studio bereitstellen.

Inhalt

IAM-einrichten

Lesen Sie die folgende AWS Identity and Access Management (IAM-) Dokumentation, bevor Sie beginnen.

- Bewährte Methoden für die Sicherheit in IAM
- Melden Sie sich AWS-Konto als Admin-Benutzer an, um die restlichen Einstellungen abzuschließen.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und

verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Zugehörige Ressourcen

- Bewährte Sicherheitsmethoden in IAM
- AWS-Service Kontingente - Allgemeine AWS-Referenz

Erste Schritte mit Amazon Nimble Studio

Dieses Kapitel zeigt, wie Sie die Nimble Studio-Konsole verwenden, um die Infrastruktur Ihres Studios zu erstellen, diese zu bestätigen AWS-Region, die Einstellungen zu überprüfen und Ihr Studio zu erstellen. Sie können Ihr Setup auch mit zusätzlichen Einstellungen anpassen.

Informationen für AWS Erstkunden finden Sie in den Einrichtung für Nimble Studio Tutorials.

Themen

Nimble Studio einrichten

Diese Anleitung zeigt Ihnen, wie Sie Ihre Infrastruktur konfigurieren, Ihre Einstellungen überprüfen und Ihr Studio erstellen. Sie können Ihr Studio auch mit anpassenZusätzliche Studioeinstellungen.

Schritt 1: Studio-Infrastruktur konfigurieren

Die Infrastruktur Ihres Studios besteht aus den folgenden Komponenten:

- Studio-Anzeigename: Anhand des Studio-Anzeigenamens können Sie Ihr Studio identifizieren — zum Beispiel AnyCompany Studio. Der Name Ihres Studios bestimmt auch die URL Ihres Studio-Portals. Sie können den Studio-Anzeigenamen nach Abschluss der Einrichtung jederzeit ändern.
- Studio-Portal-URL: Sie können über die Studio-Portal-URL auf Ihr Studio zugreifen. Die URL basiert auf dem Studio-Anzeigenamen — zum Beispiel https://anycompanystudio.awsapps.com. Sie können die URL des Studio-Portals nach Abschluss der Einrichtung jederzeit ändern.
- AWS-Region: Das AWS-Regionist der physische Standort für eine Sammlung von AWS Rechenzentren. Wenn Sie Ihr Studio einrichten, wird als Region standardmäßig der Standort ausgewählt, der Ihnen am nächsten liegt. Sie sollten die Region so ändern, dass sie Ihren Benutzern am nächsten ist. Dies reduziert die Verzögerung und verbessert die Datenübertragungsgeschwindigkeit.

> **Important**
>
> Sie können Ihre Region nicht ändern, nachdem Sie die Einrichtung von Nimble Studio abgeschlossen haben.

Erledigen Sie die Aufgaben in diesem Abschnitt, um die Infrastruktur Ihres Studios zu konfigurieren.

Um die Infrastruktur Ihres Studios zu konfigurieren

1. Melden Sie sich bei der Nimble Studio-Konsole an AWS Management Consoleund öffnen Sie sie.
2. Wählen Sie Nimble Studio einrichten und dann Weiter.
3. Geben Sie den Studio-Anzeigenamen ein — zum Beispiel**`AnyCompany Studio`**.
4. (Optional) Um den Namen des Studio-Portals zu ändern, wählen Sie URL bearbeiten aus.
5. (Optional) Um den AWS-Regionso zu ändern, dass er Ihren Studio-Benutzern am nächsten ist, wählen Sie Region ändern.
   a. Wählen Sie die Region aus, die Ihren Benutzern am nächsten ist.
   b. Wählen Sie „Region anwenden“.
6. (Optional) Um Ihr Studio-Setup weiter anzupassen, wählen Sie Zusätzliche Studioeinstellungen.
7. Um Ihre Einstellungen zu überprüfen, bevor Sie Ihr Studio erstellen, wählen Sie Weiter.

Schritt 2: Überprüfe und erstelle dein Studio

Nachdem Sie die Infrastruktur Ihres Studios konfiguriert haben, können Sie Ihr Studio überprüfen, Änderungen vornehmen und erstellen.

Um dein Studio zu überprüfen und zu erstellen

1. Überprüfen Sie auf der Seite Überprüfen und erstellen Ihre Studio-Infrastruktur.
2. Vergewissern Sie AWS-Regionsich, dass die Ihren Studio-Benutzern am nächsten ist.
3. (Optional) Wählen Sie Bearbeiten, um Änderungen an Ihrem Studio-Setup vorzunehmen.
4. Wenn Sie bereit sind, wählen Sie Studio erstellen.

Zusätzliche Studioeinstellungen

Das Nimble Studio-Setup umfasst zusätzliche Studioeinstellungen. Mit diesen Einstellungen können Sie alle Änderungen anzeigen, die das Nimble Studio-Setup an Ihnen vornimmt AWS-Konto, Ihre Studio-Benutzerrolle konfigurieren und Ihren Verschlüsselungsschlüsseltyp ändern. Sie können Ihren Studio-Ressourcen auch optionale Tags hinzufügen.

Konfigurieren Sie die Studio-Benutzerrolle

Ein AWS Dienst kann eine Dienstrolle übernehmen, um Aktionen in Ihrem Namen auszuführen. Nimble Studio benötigt eine Studio-Benutzerrolle, um Benutzern Zugriff auf Ressourcen in Ihrem Studio zu gewähren.

Sie können AWS Identity and Access Management (IAM) verwaltete Richtlinien an die Studio-Benutzerrolle anhängen. Die Richtlinien ermöglichen es Benutzern, bestimmte Aktionen auszuführen, z. B. das Erstellen von Jobs in einer bestimmten Nimble Studio-Anwendung. Da Anwendungen von bestimmten Bedingungen in der verwalteten Richtlinie abhängen, funktioniert die Anwendung möglicherweise nicht wie erwartet, wenn Sie die verwalteten Richtlinien nicht verwenden.

Sie können die Studio-Benutzerrolle nach Abschluss der Installation jederzeit ändern. Weitere Informationen zu Benutzerrollen finden Sie unter IAM-Rollen.

Die folgenden Registerkarten enthalten Anweisungen für zwei verschiedene Anwendungsfälle. Um eine neue Servicerolle zu erstellen und zu verwenden, wählen Sie die Registerkarte Neue Servicerolle. Um eine bestehende Servicerolle zu verwenden, wählen Sie die Registerkarte Bestehende Servicerolle.

New service role

Um eine neue Servicerolle zu erstellen und zu verwenden

1. Wählen Sie Neue Servicerolle erstellen und verwenden aus.
2. (Optional) Geben Sie einen Namen für die Dienstbenutzerrolle ein.
3. Wählen Sie Berechtigungsdetails anzeigen aus, um weitere Informationen zur Rolle zu erhalten.

Existing service role

Um eine bestehende Servicerolle zu verwenden

1. Wählen Sie Bestehende Servicerolle verwenden aus.
2. Öffnen Sie die Dropdownliste, um eine bestehende Servicerolle auszuwählen.
3. (Optional) Wählen Sie In der IAM-Konsole anzeigen aus, um weitere Informationen zur Rolle zu erhalten.

AWS IAM Identity Center

AWS IAM Identity Center ist ein cloudbasierter Single-Sign-On-Service zur Verwaltung von Benutzern und Gruppen. IAM Identity Center kann auch in den Single Sign-On (SSO) -Anbieter Ihres Unternehmens integriert werden, sodass sich Benutzer mit ihrem Unternehmenskonto anmelden können.

Nimble Studio aktiviert IAM Identity Center standardmäßig und ist für die Einrichtung und Verwendung von Nimble Studio erforderlich. Weitere Informationen finden Sie unter Was ist. AWS IAM Identity Center

AWS KMS Verschlüsselungsschlüssel konfigurieren

AWS Key Management Service (AWS KMS) Schlüssel sind der primäre Typ von KMS-Schlüsseln, den Sie zum Verschlüsseln, Entschlüsseln und erneuten Verschlüsseln Ihrer Daten verwenden können.

Nimble Studio umfasst die folgenden Verschlüsselungsschlüsseltypen: AWS KMS

- AWS Eigener Schlüssel — AWS Eigene Schlüssel sind KMS-Schlüssel, die er AWS-Service besitzt und verwaltet, sodass er sie in mehreren AWS-Konten Fällen verwenden kann. AWS Eigene Schlüssel befinden sich nicht in Ihrem AWS-Konto, aber Nimble Studio kann einen AWS eigenen Schlüssel verwenden, um die Ressourcen in Ihrem Konto zu schützen.

  Um ihn verwenden zu können AWS KMS, müssen Sie weder den Schlüssel noch seine Schlüsselrichtlinie erstellen oder verwalten. Die Verwendung AWS eigener Schlüssel ist kostenlos und sie werden nicht auf Ihre AWS KMS Kontingente angerechnet AWS-Konto.
- Vom Kunden verwalteter AWS KMS Schlüssel — Ein vom Kunden verwalteter Schlüssel ist ein KMS-Schlüssel in Ihrem AWS-Konto System, den Sie selbst erstellen, besitzen und verwalten.

  Sie haben die volle Kontrolle über diese KMS-Schlüssel. Für vom Kunden verwaltete Schlüssel fällt eine monatliche Gebühr an. Außerdem fällt für jede API-Anfrage eine Gebühr an, die AWS KMS

über das kostenlose Kontingent hinausgeht. Weitere Informationen zur AWS KMS Preisgestaltung finden Sie unter AWS Key Management Service Preise.

Der Typ des Verschlüsselungsschlüssels kann nach Abschluss der Installation nicht geändert werden. Weitere Informationen zu AWS KMS und zu den Typen von Verschlüsselungsschlüsseln finden Sie in der AWS KMS Dokumentation.

Um einen anderen Verschlüsselungsschlüsseltyp auszuwählen

1. Wählen Sie Anderen AWS KMS Schlüssel auswählen (erweitert) aus.
2. Wählen Sie einen AWS KMS Schlüssel aus oder geben Sie eine Amazon-Ressourcennummer (ARN) ein.
3. Wählen Sie AWS KMS Schlüssel erstellen.

Tags konfigurieren

Tags dienen als Beschriftungen für die Organisation Ihrer Nimble Studio-Ressourcen. Sie können bis zu 50 Tags hinzufügen, um Ressourcen zu identifizieren, zu organisieren, zu filtern und nach ihnen zu suchen.

Jedes Tag besteht aus zwei Teilen, die Sie definieren: einem Tag-Schlüssel und einem optionalen Tag-Wert — zum Beispiel Schlüssel: `domain` und Wert:`anycompanystudio.com`.

Sie können nach Abschluss der Einrichtung jederzeit Tags hinzufügen oder entfernen. Weitere Informationen zu Tags finden Sie unter AWS Ressourcen taggen.

So fügen Sie Ihren Studio-Ressourcen Tags hinzu

1. Wählen Sie Add new tag (Neues Tag hinzufügen) aus.
2. Geben Sie das Tag Key (Schlüssel) ein.
3. (Optional) Geben Sie den Tag-Wert ein.

Ein Studio löschen

Wenn du ein Studio nicht mehr benötigst, kannst du es löschen. Wenn Sie Ihr Studio löschen, wird nur die Studio-Infrastruktur gelöscht. Ihre anderen AWS Ressourcen, wie Benutzerrollen, Richtlinien und Anwendungsdaten, bleiben erhalten.

> **Important**
>
> Sie können ein Studio nicht wiederherstellen, nachdem Sie es gelöscht haben.

Um dein Studio zu löschen

1. Melden Sie sich bei der Nimble Studio-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie Studio-Übersicht aus.
3. Wählen Sie „Aktionen“ und anschließend „Studio löschen“.
4. Geben Sie ein **`delete`** und wählen Sie dann Löschen.

Sicherheit bei Amazon Nimble Studio

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Um mehr über die Compliance-Programme zu erfahren, die gelten für Amazon Nimble Studio, siehe AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

> **Important**
>
> Es wird dringend empfohlen, dass Sie das Security Pillar — AWS Well-Architected Framework lesen und sich damit vertraut machen. Dieser Artikel enthält wichtige Prinzipien zur Sicherung Ihrer AWS Infrastruktur.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung anwenden können, wenn Sie Nimble Studio. In den folgenden Themen erfahren Sie, wie Sie konfigurieren Nimble Studio um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Nimble Studio Ressourcen schätzen.

Weitere Informationen

- Säule der Sicherheit — AWS Well-Architected Framework
- Sicherheit für die AWS Cloud Development Kit (AWS CDK) ()AWS CDK

- Sicherheit in der Amazon Virtual Private Cloud
- AWS Sicherheitsnachweise
- Sicherheit bei Amazon EC2
  - Linux
  - Windows

Richten Sie die AWS-Konto Sicherheit ein

In dieser Anleitung erfahren Sie, wie Sie Ihr System so einrichten AWS-Konto , dass Sie Benachrichtigungen erhalten, wenn Ihre Ressourcen gefährdet sind, und wie Sie bestimmten AWS-Konto Benutzern den Zugriff darauf ermöglichen. Gehen Sie wie folgt vor, um Ihre Ressourcen zu sichern AWS-Konto und nachzuverfolgen.

Inhalt

- Löschen Sie die Zugangsschlüssel Ihres Kontos
- Multifaktor-Authentifizierung aktivieren
- CloudTrail In allen aktivieren AWS-Regionen
- Amazon GuardDuty und Benachrichtigungen einrichten

Löschen Sie die Zugangsschlüssel Ihres Kontos

Sie können den programmatischen Zugriff auf Ihre AWS Ressourcen über AWS Command Line Interface (AWS CLI) oder mit AWS APIs zulassen. AWS Empfiehlt jedoch, die mit Ihrem Root-Konto verknüpften Zugriffsschlüssel nicht für den programmatischen Zugriff zu erstellen oder zu verwenden.

Wenn Sie noch über Zugriffsschlüssel verfügen, empfehlen wir Ihnen, diese zu löschen und einen Benutzer zu erstellen. Erteilen Sie diesem Benutzer dann nur die Berechtigungen, die für den Benutzer erforderlich sind APIs , den Sie anrufen möchten. Sie können diesen Benutzer verwenden, um Zugriffsschlüssel auszustellen.

Weitere Informationen finden Sie AWS-Konto im Allgemeine AWS-Referenz Handbuch unter Zugriffstasten für Sie verwalten.

Multifaktor-Authentifizierung aktivieren

Die Multi-Faktor-Authentifizierung (MFA) ist eine Sicherheitsfunktion, die zusätzlich zu Ihrem Benutzernamen und Passwort eine Authentifizierungsebene bietet.

MFA funktioniert wie folgt: Nachdem Sie sich mit Ihrem Benutzernamen und Passwort angemeldet haben, müssen Sie auch zusätzliche Informationen angeben, auf die nur Sie physischen Zugriff haben. Diese Informationen können von einem speziellen MFA-Hardwaregerät oder von einer App auf einem Telefon stammen.

Sie müssen den MFA-Gerätetyp, den Sie verwenden möchten, aus der Liste der unterstützten MFA-Geräte auswählen. Bewahren Sie bei einem Hardwaregerät das MFA-Gerät an einem sicheren Ort auf.

Wenn Sie ein virtuelles MFA-Gerät (z. B. eine Telefon-App) verwenden, denken Sie darüber nach, was passieren könnte, wenn Ihr Telefon verloren geht oder beschädigt wird. Ein Ansatz besteht darin, das virtuelle MFA-Gerät, das Sie verwenden, an einem sicheren Ort aufzubewahren. Eine weitere Option besteht darin, mehr als ein Gerät gleichzeitig zu aktivieren oder eine virtuelle MFA-Option für die Wiederherstellung von Geräteschlüsseln zu verwenden.

Weitere Informationen zu MFA finden Sie unter Aktivieren eines Geräts mit virtueller Multi-Factor Authentication (MFA).

Zugehörige Ressourcen

- Erste Schritte mit der Multi-Faktor-Authentifizierung
- Sicherung des Zugriffs auf die AWS Verwendung von MFA

CloudTrail In allen aktivieren AWS-Regionen

Sie können alle Aktivitäten in Ihren AWS Ressourcen verfolgen, indem Sie AWS CloudTrail Wir empfehlen, dass Sie es CloudTrail jetzt einschalten. Auf diese Weise Support kann Ihr AWS Lösungsarchitekt später ein Sicherheits- oder Konfigurationsproblem beheben.

Informationen zur Aktivierung der CloudTrail Anmeldung für alle AWS-Regionen finden Sie unter AWS CloudTrail Update — In allen Regionen aktivieren und mehrere Trails verwenden.

Weitere Informationen dazu findest CloudTrail du unter Einschalten CloudTrail: API-Aktivität protokollieren in deinem AWS-Konto. Informationen zur CloudTrail Überwachung von Nimble Studio finden Sie unterNimble Studio-Anrufe protokollieren mit AWS CloudTrail.

Amazon GuardDuty und Benachrichtigungen einrichten

Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Folgendes analysiert und verarbeitet:

- Datenquellen
- Amazon VPC-Flussprotokolle
- AWS CloudTrail Verwaltungs-Ereignisprotokolle
- CloudTrail S3-Datenereignisprotokolle
- DNS-Protokolle

Amazon GuardDuty identifiziert unerwartete und potenziell nicht autorisierte und böswillige Aktivitäten in Ihrer AWS Umgebung. Zu böswilligen Aktivitäten können Probleme wie die Eskalation von Rechten, die Verwendung offengelegter Anmeldeinformationen oder die Kommunikation mit bösartigen IP-Adressen oder Domänen gehören. Zur Identifizierung dieser Aktivitäten werden Feeds mit Bedrohungsinformationen wie Listen bösartiger IP-Adressen und Domänen sowie maschinelles Lernen GuardDuty verwendet. GuardDuty Kann beispielsweise kompromittierte EC2 Amazon-Instances erkennen, die Malware bereitstellen oder Bitcoin minen.

GuardDuty überwacht auch das AWS-Konto Zugriffsverhalten auf Anzeichen einer Sicherheitslücke. Dazu gehören nicht autorisierte Infrastrukturbereitstellungen, z. B. Instanzen, die in einem System bereitgestellt werden AWS-Region , das noch nie genutzt wurde. Dazu gehören auch ungewöhnliche API-Aufrufe, wie z. B. eine Änderung der Passwortrichtlinie zur Verringerung der Passwortstärke.

GuardDuty informiert Sie anhand von Sicherheitsergebnissen über den Status Ihrer AWS Umgebung. Sie können diese Ergebnisse in der GuardDuty Konsole oder über Amazon CloudWatch Events einsehen.

Ein Amazon SNS SNS-Thema und einen Endpunkt einrichten

Folgen Sie den Anweisungen im Thema Amazon SNS einrichten und im Tutorial Endpoint.

Richten Sie eine EventBridge Veranstaltung zur GuardDuty Präsentation der Ergebnisse ein

Erstellen Sie eine Regel für EventBridge das Senden von Ereignissen für alle GuardDuty generierten Ergebnisse.

Um ein EventBridge Ereignis für GuardDuty Ergebnisse zu erstellen

1. Melden Sie sich bei der EventBridge Amazon-Konsole an: https://console.aws.amazon.com/events/
2. Wählen Sie im Navigationsbereich Regeln aus. Wählen Sie dann Create rule (Regel erstellen) aus.
3. Geben Sie einen Namen und eine Beschreibung für die neue Regel ein. Wählen Sie anschließend Weiter.
4. Behalten Sie die Option AWS Ereignisse oder EventBridge Partnerereignisse als Ereignisquelle bei.
5. Wählen Sie unter Ereignismuster die AWS Dienste für die Ereignisquelle aus. Dann GuardDutyfür die AWS Dienste und GuardDuty Finding für den Ereignistyp. Dies ist das Thema, das Sie in erstellt habenEin Amazon SNS SNS-Thema und einen Endpunkt einrichten.
6. Wählen Sie Weiter.
7. Wählen Sie für Ziel 1 AWS Service aus. Wählen Sie in der Dropdownliste „Ziel auswählen“ das SNS-Thema aus. Wählen Sie dann Ihr GuardDuty_to_Email-Thema aus.
8. Im Abschnitt Zusätzliche Einstellungen: Wählen Sie im Drop-down-Menü Zieleingang konfigurieren die Option Eingangstransformator aus. Wählen Sie Eingabe-Transformator konfigurieren aus.
9. Geben Sie den folgenden Code in das Feld Eingabepfad im Abschnitt Zieleingangstransformator ein.

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

10. Um die E-Mail zu formatieren, geben Sie den folgenden Code in das Feld Vorlage ein.

```
"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. Wählen Sie Create (Erstellen) aus. Wählen Sie anschließend Weiter.
12. (Optional) Fügen Sie Tags hinzu, wenn Sie Tags verwenden, um Ihre AWS Ressourcen nachzuverfolgen.
13. Wählen Sie Weiter.
14. Überprüfe deine Regel. Wählen Sie dann Create rule (Regel erstellen) aus.

Nachdem Sie Ihre AWS-Konto Sicherheit eingerichtet haben, können Sie bestimmten Benutzern Zugriff gewähren und Benachrichtigungen erhalten, wenn Ihre Ressourcen gefährdet sind.

Datenschutz in Amazon Nimble Studio

Das AWS Modell der der , gilt für den Datenschutz in Amazon Nimble Studio. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.

- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dazu gehört auch, wenn Sie mit arbeiten Nimble Studio oder andere, die die AWS-Services Konsole, die API oder verwenden AWS SDKs. AWS CLI Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon Nimble Studio. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für die AWS-Services , die Sie verwenden.

Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in der Europäischen Union finden Sie im DSGVO-Zentrum.

Verschlüsselung im Ruhezustand

Nimble Studio schützt sensible Studiodaten, indem es sie im Ruhezustand mithilfe von Verschlüsselungsschlüsseln verschlüsselt, die in AWS Key Management Service ()AWS KMS gespeichert sind. Verschlüsselung im Ruhezustand ist überall verfügbar, AWS-Regionen wo Nimble Studio verfügbar ist. Zu den Studio-Daten, die wir verschlüsseln, gehören die Namen und Beschreibungen aller Ressourcentypen sowie Skripts für Studiokomponenten, Skriptparameter, Einhängepunkte, Freigabenamen und andere Daten.

Das Verschlüsseln von Daten bedeutet, dass sensible Daten, die auf Festplatten gespeichert sind, für keinen Benutzer oder keine Anwendung ohne gültigen Schlüssel lesbar sind. Verschlüsselte Daten können sicher gespeichert werden und können nur von einer Partei mit autorisiertem Zugriff auf den verwalteten Schlüssel entschlüsselt werden.

Informationen darüber, wie Nimble Studio Daten im Ruhezustand verschlüsselt, finden Sie unter. AWS KMS Schlüsselverwaltung für Amazon Nimble Studio

Verwendung von Zuschüssen mit Schlüsseln AWS KMS

Ein Zuschuss ist ein politisches Instrument, das es AWS Prinzipalen ermöglicht, AWS KMS Schlüssel für kryptografische Operationen zu verwenden. Außerdem können sie mit dem Befehl einen KMS-Schlüssel einsehen und `DescribeKey` Zuschüsse erstellen und verwalten.

Grants werden häufig von Integrated With verwendet AWS-Services , AWS KMS um Ihre Daten im Ruhezustand zu verschlüsseln. Der Service erstellt eine Erteilung im Namen eines Benutzers im Konto, verwendet seine Berechtigungen und hebt die Erteilung auf, sobald die Aufgabe abgeschlossen ist.

Wenn Nimble Studio Ihr Studio erstellt, stellen wir Benutzern des Nimble Studio-Portals zwei Rollen zur Verfügung: Benutzer- und Administratorrollen. Nimble Studio gewährt diesen Rollen Zuschüsse für vom Kunden verwaltete Schlüssel, um ihnen Zugriff auf verschlüsselte Studio-Daten zu gewähren.

> **Important**
>
> Wenn Sie einen Grant löschen, ist das Nimble Studio-Portal für Benutzer unbrauchbar, bis der Administrator einen neuen Grant erstellt.

Einzelheiten zur AWS-Services Verwendung von Zuschüssen finden Sie unter AWS-Services Verwendung AWS KMS oder dem Thema Verschlüsselung im Ruhezustand im Benutzer- oder Entwicklerhandbuch des Dienstes.

Verschlüsselung während der Übertragung

Die folgende Tabelle enthält Informationen darüber, wie Daten während der Übertragung verschlüsselt werden. Gegebenenfalls sind auch andere Datenschutzmethoden für Nimble Studio aufgeführt.

Daten	Netzwerkpfad	Schutz
Web-Assets wie Bilder und Dateien JavaScript	Der Netzwerkpfad verläuft zwischen Nimble Studio-Be nutzern und Nimble Studio.	Die Datenverschlüsselung verwendet TLS 1.2 oder höher.

Pixel und zugehöriger Streaming-Datenverkehr	Der Netzwerkpfad verläuft zwischen Nimble Studio-Benutzern und Nimble Studio.	Mit dem 256-Bit-Advanced Encryption Standard (AES-256) verschlüsselt und mit TLS 1.2 oder höher übertragen.
API-Datenverkehr	Der Pfad verläuft zwischen Nimble Studio-Benutzern und Nimble Studio.	Verschlüsselt mit TLS 1.2 oder höher. Anfragen zum Herstellen einer Verbindung werden mit Sigv4 signiert.

Schlüsselverwaltung für Amazon Nimble Studio

Wenn Sie ein neues Studio erstellen, können Sie einen der folgenden Schlüssel wählen, um Ihre Studiodaten zu verschlüsseln:

- AWS eigener KMS-Schlüssel — Standardverschlüsselungstyp. Der Schlüssel gehört Nimble Studio (ohne zusätzliche Kosten).
- Vom Kunden verwalteter KMS-Schlüssel — Der Schlüssel wird in Ihrem Konto gespeichert und wird von Ihnen erstellt, gehört und verwaltet. Sie haben die volle Kontrolle über den Schlüssel. AWS KMS Gebühren fallen an.

Das Löschen eines vom Kunden verwalteten KMS-Schlüssels in AWS Key Management Service (AWS KMS) ist destruktiv und potenziell gefährlich. Dadurch werden das Schlüsselmaterial und alle mit dem Schlüssel verknüpften Metadaten unwiderruflich gelöscht. Nachdem ein vom Kunden verwalteter KMS-Schlüssel gelöscht wurde, können Sie die mit diesem Schlüssel verschlüsselten Daten nicht mehr entschlüsseln. Das bedeutet, dass die Daten nicht mehr wiederhergestellt werden können.

Aus diesem Grund AWS KMS haben Kunden eine Wartezeit von bis zu 30 Tagen, bevor der Schlüssel gelöscht wird. Die Standardwartezeit beträgt 30 Tage.

Über die Wartezeit

Da das Löschen eines vom Kunden verwalteten KMS-Schlüssels zerstörerisch und potenziell gefährlich ist, müssen Sie eine Wartezeit von 7 bis 30 Tagen festlegen. Die Standardwartezeit beträgt 30 Tage.

Die tatsächliche Wartezeit kann jedoch bis zu 24 Stunden länger sein als die, die Sie geplant haben. Verwenden Sie den DescribeKeyVorgang, um das tatsächliche Datum und die Uhrzeit der Löschung des Schlüssels zu ermitteln. Sie können das geplante Löschdatum eines Schlüssels auch in der AWS KMS Konsole auf der Detailseite des Schlüssels im Abschnitt Allgemeine Konfiguration sehen. Beachten Sie die Zeitzone.

Während der Wartezeit lautet der Status und der Schlüsselstatus des vom Kunden verwalteten Schlüssels Ausstehende Löschung.

- Ein vom Kunden verwalteter KMS-Schlüssel, dessen Löschung aussteht, kann für keine kryptografischen Operationen verwendet werden.
- AWS KMS rotiert nicht die Backing-Keys von vom Kunden verwalteten AWS KMS Schlüsseln, deren Löschung noch aussteht.

Weitere Informationen zum Löschen eines vom Kunden verwalteten AWS KMS Schlüssels finden Sie unter Kundenhauptschlüssel löschen.

Maßnahmen zur Datensicherheit

Aus Datenschutzgründen empfehlen wir Ihnen, Ihre AWS-Konto Anmeldeinformationen zu schützen und individuelle Konten bei AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, niemals vertrauliche Identifikationsinformationen wie Kundenkontonummern in Freiformfelder wie ein Namensfeld einzugeben. Dies gilt auch, wenn Sie mit Amazon Nimble

Studio oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Amazon Nimble Studio oder andere Dienste eingeben, werden möglicherweise zur Aufnahme in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Diagnosedaten und Metriken

Während der Bereitstellung und Löschung von erfasst Amazon Nimble Studio bestimmte Kennzahlen StudioBuilder, die wir verwenden, um Probleme zu diagnostizieren und die Funktionen und das Benutzererlebnis von Nimble Studio zu verbessern.

Arten der gesammelten Metriken

- Nutzungsinformationen — Die generischen Befehle und Unterbefehle, die ausgeführt werden.
- Fehler und Diagnoseinformationen — Status und Dauer der ausgeführten Befehle, einschließlich Exit-Codes, Namen interner Ausnahmen und Fehler.
- System- und Umgebungsinformationen — Die Python-Version, das Betriebssystem (Windows, Linux, oder macOS) und Umgebung, in der ausgeführt StudioBuilder wird.

Identity and Access Management für Amazon Nimble Studio

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Nimble Studio-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Serviceübergreifende Confused-Deputy-Prävention
- Fehlerbehebung bei Identität und Zugriff auf Amazon Nimble Studio

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Nimble Studio ausführen.

Dienstbenutzer — Wenn Sie den Nimble Studio-Dienst für Ihre Arbeit verwenden, sind Sie ein Dienstbenutzer. In diesem Fall stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie für den Zugriff auf Ihre zugewiesenen Ressourcen benötigen. Wenn Sie mehr Nimble Studio-Funktionen für Ihre Arbeit verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Nimble Studio nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Fehlerbehebung bei Identität und Zugriff auf Amazon Nimble Studio

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Nimble Studio-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Nimble Studio. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Nimble Studio Ihre Mitarbeiter zugreifen sollen. Senden Sie dann Anfragen an Ihren Administrator, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Nimble Studio verwenden kann, finden Sie unter. So funktioniert Amazon Nimble Studio mit IAM

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Weitere Informationen zur Anmeldung mit dem AWS Management Console finden Sie unter AWS Management Console Als IAM-Benutzer oder Root-Benutzer anmelden im IAM-Benutzerhandbuch.

Sie müssen als AWS-Konto Root-Benutzer oder als Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Sie können auch die Single-Sign-On-Authentifizierung Ihres Unternehmens verwenden oder sich sogar über Google oder Facebook anmelden. In diesen Fällen hat Ihr Administrator vorher einen Identitätsverbund unter Verwendung von IAM-Rollen eingerichtet. Wenn Sie AWS mit Anmeldeinformationen eines anderen Unternehmens zugreifen, übernehmen Sie indirekt eine Rolle.

Um sich direkt bei der anzumelden AWS Management Console, verwenden Sie Ihr Passwort zusammen mit Ihrer Root-Benutzer-E-Mail-Adresse oder Ihrem Benutzernamen. Sie können AWS programmgesteuert mit Ihrem Root-Benutzer oder Ihren Benutzerzugriffsschlüsseln darauf zugreifen.

AWS bietet SDK- und Befehlszeilentools, mit denen Sie Ihre Anfrage mit Ihren Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, signieren Sie die Anfrage selbst. Hierzu verwenden Sie Signature Version 4, ein Protokoll für die Authentifizierung eingehender API-Anforderungen. Weitere Informationen zu diesen Authentifizierungsanfragen finden Sie unter Signature Version 4-Signaturprozess im Allgemeine AWS-Referenz .

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie zum ersten Mal einen erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir empfehlen dringend, den Root-Benutzer nicht für Ihre täglichen Aufgaben zu verwenden, auch nicht für die administrativen. Folgen Sie stattdessen dem bewährten Verfahren, den Stammbenutzer ausschließlich zur Erstellung des ersten IAM-Benutzers zu verwenden. Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

Benutzer und Gruppen

Ein Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Ein Benutzer kann über langfristige Anmeldeinformationen oder eine Reihe von Zugriffsschlüsseln verfügen. Informationen zum Generieren von Zugriffsschlüsseln finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. Wenn Sie Zugriffsschlüssel für einen Benutzer generieren, können Sie das key pair anzeigen und sicher speichern. Sie können den geheimen Zugriffsschlüssel in future nicht wiederherstellen. Generieren Sie stattdessen ein neues Zugriffsschlüsselpaar.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von Benutzern spezifiziert. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Wann sollte ein Benutzer (statt einer Rolle) erstellt werden?

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens, für AWS-Konto die bestimmte Berechtigungen gelten. Sie ähnelt einem Benutzer, ist aber keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Temporäre Benutzerberechtigungen – Ein Benutzer kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Föderierter Benutzerzugriff — Anstatt einen Benutzer zu erstellen, können Sie vorhandene Identitäten aus AWS Directory Service Ihrem Unternehmensbenutzerverzeichnis oder einem Web-Identitätsanbieter verwenden. Diese werden als Verbundbenutzer bezeichnet. AWS weist einem Verbundbenutzer eine Rolle zu, wenn Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu Verbundbenutzern finden Sie unter Verbundbenutzer und Rollen im IAM-Benutzerhandbuch.
    - Mitgliedschaft — Nimble Studio verwendet ein Konzept namens „Mitgliedschaft“, um einem Benutzer Zugriff auf ein bestimmtes Startprofil zu gewähren. Durch die Mitgliedschaft können Studio-Administratoren den Zugriff auf Ressourcen an Benutzer delegieren, ohne IAM-Richtlinien schreiben oder verstehen zu müssen. Wenn ein Nimble Studio-Administrator eine Mitgliedschaft für einen Benutzer in einem Startprofil erstellt, ist der Benutzer berechtigt, IAM-Aktionen

durchzuführen, die für die Verwendung eines Startprofils erforderlich sind, wie z. B. das Anzeigen seiner Eigenschaften und das Starten einer Streaming-Sitzung mit diesem Startprofil.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Servicerollen bieten Zugriff nur innerhalb Ihres Kontos und können nicht verwendet werden, um Zugriff auf Dienste in anderen Konten zu gewähren. Ein Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an eine AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle — Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Nimble Studio unterstützt keine dienstbezogenen Rollen.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM-Rollen oder Benutzer verwenden sollten, finden Sie unter Wann sollte eine IAM-Rolle (anstelle eines Benutzers) erstellt werden? im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an IAM-Identitäten oder -Ressourcen anhängen. AWS Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. Sie können sich als Root-Benutzer oder als Benutzer anmelden oder eine IAM-Rolle übernehmen. Wenn Sie dann eine Anfrage stellen, werden die zugehörigen identitäts- oder ressourcenbasierten Richtlinien AWS bewertet. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden als JSON-Dokumente gespeichert. AWS Weitere Informationen zur Struktur und zum Inhalt von JSON-Richtliniendokumenten finden Sie im IAM-Benutzerhandbuch unter Überblick über JSON-Richtlinien.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Principal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Eine IAM-Entität (Benutzer oder Rolle) besitzt zunächst keine Berechtigungen. Anders ausgedrückt, können Benutzer standardmäßig keine Aktionen ausführen und nicht einmal ihr Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen Benutzer und Rollen auf welchen Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen zur Auswahl zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie finden Sie im IAM-Benutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an die die Richtlinie angehängt ist, definiert die Richtlinie, welche Aktionen ein

bestimmter Principal für diese Ressource ausführen kann und unter welchen Bedingungen. Geben Sie einen Prinzipal in einer ressourcenbasierten Richtlinie an. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten (ACLs) in Nimble Studio

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) Berechtigungen für den Zugriff auf eine Ressource haben. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM-Entität (Benutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen stellen die Schnittmenge zwischen den identitätsbasierten Richtlinien der Entität und ihren Berechtigungsgrenzen dar. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle in dem `Principal` Feld angeben, sind nicht durch die Berechtigungsgrenze begrenzt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in Organizations festlegen. Organizations ist ein Service zur Gruppierung und zentralen Verwaltung mehrerer AWS-Konten Unternehmenseigentümer. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich jedes AWS-Konto

Root-Benutzers. Weitere Informationen zu Organizations und SCPs finden Sie unter So SCPs arbeiten Sie im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind die Schnittmenge der identitätsbasierten Richtlinien des Benutzers oder der Rolle und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon Nimble Studio mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Nimble Studio zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Nimble Studio verfügbar sind.

IAM-Funktionen, die Sie mit Amazon Nimble Studio verwenden können

IAM-Feature	Nimble Studio-Unterstützung
Richtlinienaktionen für Nimble Studio	Ja
Richtlinienressourcen für Nimble Studio	Ja
Bedingungsschlüssel für Richtlinien für Nimble Studio	Ja
Zugriffskontrolllisten (ACLs) in Nimble Studio	Nein
Attributbasierte Zugriffskontrolle (ABAC) mit Nimble Studio	Ja

IAM-Feature	Nimble Studio-Unterstützung
Temporäre Anmeldeinformationen mit Nimble Studio verwenden	Ja
Serviceübergreifende Prinzipalberechtigungen für Nimble Studio	Ja
Servicerollen für Nimble Studio	Ja
Mit Diensten verknüpfte Rollen für Nimble Studio	Nein

Einen allgemeinen Überblick darüber, wie Nimble Studio und andere AWS-Services mit den meisten IAM-Funktionen funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Nimble Studio

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen Benutzer und Rollen auf welchen Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zugelassen oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, der er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON-Richtlinie verwenden können, finden Sie unter Referenz zu den IAM-JSON-Richtlinienelementen im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Beispiele für identitätsbasierte Richtlinien von Nimble Studio finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Ressourcenbasierte Richtlinien in Nimble Studio

Unterstützt ressourcenbasierte Richtlinien	Nein

Nimble Studio unterstützt keine ressourcenbasierten Richtlinien oder kontoübergreifenden Zugriff. Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an die die Richtlinie angehängt ist, definiert die Richtlinie, welche Aktionen ein bestimmter Principal für diese Ressource ausführen kann und unter welchen Bedingungen. Geben Sie einen Prinzipal in einer ressourcenbasierten Richtlinie an. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Richtlinienaktionen für Nimble Studio

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Principal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Nimble Studio-Aktionen finden Sie unter Von Amazon Nimble Studio definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Nimble Studio verwenden vor der Aktion das folgende Präfix:

```
nimble
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Richtlinien von Nimble Studio finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Richtlinienressourcen für Nimble Studio

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Principal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie bei Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, wie z. B. das Auflisten von Vorgängen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Beispiele für identitätsbasierte Richtlinien von Nimble Studio finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Bedingungsschlüssel für Richtlinien für Nimble Studio

Unterstützt Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Principal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Condition` Element (oder `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition` Element) ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt sein, bevor die Berechtigungen für die Anweisung erteilt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem Benutzer nur dann Zugriff auf eine Ressource gewähren, wenn diese mit seinem Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Liste aller globalen AWS -Bedingungsschlüssel finden Sie unter Globale AWS -Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien von Nimble Studio finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Zugriffskontrolllisten (ACLs) in Nimble Studio

Unterstützt ACLs	Nein

Nimble Studio unterstützt keine Zugriffskontrolllisten (ACLs). ACLs steuern Sie, welche Principals (Kontomitglieder, Benutzer oder Rollen) Berechtigungen für den Zugriff auf eine Ressource haben.

ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das Format für JSON-Richtliniendokumente.

Attributbasierte Zugriffskontrolle (ABAC) mit Nimble Studio

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese AWS Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys`Bedingung verwenden.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung von ABAC finden Sie unter Verwenden der attributebasierten Zugriffskontrolle (ABAC) im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Nimble Studio verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden

und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für Nimble Studio

Unterstützt Prinzipal-Berechtigungen	Ja

Servicerollen für Nimble Studio

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Servicerollen bieten Zugriff nur innerhalb Ihres Kontos und können nicht verwendet werden, um Zugriff auf Dienste in anderen Konten zu gewähren. Ein Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an eine AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Nimble Studio beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Nimble Studio Sie dazu anleitet.

Mit Diensten verknüpfte Rollen für Nimble Studio

Unterstützt serviceverknüpfte Rollen	Nein

Nimble Studio unterstützt keine dienstbezogenen Rollen. Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein -Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS-Services Diese Rollen funktionieren mit IAM. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon Nimble Studio

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Nimble Studio-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung gewähren, Aktionen mit den Ressourcen durchzuführen, die sie benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen zum Erstellen einer identitätsbasierten IAM-Richtlinie mithilfe dieser Beispieldokumente zu JSON-Richtlinien finden Sie unter Erstellen von Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand Nimble Studio-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien — Um Nimble Studio schnell nutzen zu können, verwenden Sie AWS verwaltete Richtlinien, um Ihren Mitarbeitern die Berechtigungen zu geben, die sie benötigen. Diese Richtlinien sind bereits in Ihrem Konto verfügbar und werden von AWS.

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

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

AWS verwaltete Richtlinien für Amazon Nimble Studio

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine

Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Ihre Endbenutzer greifen hauptsächlich über das Nimble Studio-Portal auf Amazon Nimble Studio zu. Wenn Sie Ihr Studio mithilfe StudioBuilder der Nimble Studio-Konsole erstellen, wird für jede Studio-Persona eine IAM-Rolle erstellt: den Studio-Administrator und den Studio-Benutzer. Jedem ist die entsprechende IAM-verwaltete Richtlinie beigefügt. Das Nimble Studio-Portal bietet Benutzern nur die Ressourcen, für deren Zugriff sie berechtigt sind, auflisten und verwenden können.

Das Nimble Studio-Portal bietet eine Oberfläche, in der Benutzer nur die Ressourcen auflisten und verwenden können, auf die sie Zugriff haben, und das Portal hängt vom Inhalt dieser Richtlinien ab, um ordnungsgemäß zu funktionieren. Nimble Studio-Endbenutzer werden das Portal verwenden, um auf ihr Cloud-Studio zuzugreifen. Wenn Administratoren ihr Studio also mit erstellen, wird für jede Person StudioBuilder, die auf das Studio zugreifen muss, eine IAM-Rolle erstellt. Dazu gehören der Studio-Administrator und der Studio-Benutzer, denen jeweils ihre jeweilige IAM-verwaltete Richtlinie beigefügt ist.

Eine Liste und eine Beschreibung der Richtlinien für Jobfunktionen finden Sie unter AWS Verwaltete Richtlinien für Jobfunktionen im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: **`AmazonNimbleStudio-LaunchProfileWorker`**

Sie können die `AmazonNimbleStudio-LaunchProfileWorker`-Richtlinie an Ihre IAM-Identitäten anfügen.

Hängen Sie diese Richtlinie an EC2 Instanzen an, die von Nimble Studio Builder erstellt wurden, um Zugriff auf Ressourcen zu gewähren, die von Nimble Studio Launch Profile Worker benötigt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- ds — Ermöglicht es LaunchProfile Mitarbeitern, Verbindungsinformationen über die mit a AWS Managed Microsoft AD verknüpften Personen zu ermitteln. LaunchProfile

- ec2 — Ermöglicht es LaunchProfile Mitarbeitern, Sicherheitsgruppen- und Subnetzinformationen für die Verbindung mit einem zu ermitteln. LaunchProfile
- fsx — Ermöglicht es LaunchProfile Mitarbeitern, Verbindungsinformationen zu FSx Amazon-Volumes zu ermitteln, die mit einem LaunchProfile verknüpft sind.

```
{
  "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 verwaltete Richtlinie: **AmazonNimbleStudio-StudioAdmin**

Sie können die AmazonNimbleStudio-StudioAdmin-Richtlinie an Ihre IAM-Identitäten anfügen.

Fügen Sie diese Richtlinie der Administratorrolle hinzu, die Ihrem Studio zugeordnet ist, um Zugriff auf Amazon Nimble Studio-Ressourcen zu gewähren, die mit dem Studio-Administrator verknüpft sind, und auf verwandte Studio-Ressourcen in anderen Diensten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- nimble — Ermöglicht Studio-Benutzern den Zugriff auf Nimble-Ressourcen, die ihnen von delegiert wurden. StudioAdmins
- sso — Ermöglicht Studio-Benutzern, die Namen anderer Benutzer im Studio einzusehen.
- identitystore — Ermöglicht Studio-Benutzern die Möglichkeit, die Namen anderer Benutzer im Studio einzusehen.
- ds — Ermöglicht Nimble Studio, virtuelle Workstations zu den mit dem Studio verknüpften Workstations hinzuzufügen. AWS Managed Microsoft AD
- ec2 — Ermöglicht Nimble Studio, virtuelle Workstations an Ihre konfigurierte VPC anzuhängen.
- fsx — Ermöglicht Nimble Studio, virtuelle Workstations mit Ihren konfigurierten Amazon-Volumes zu verbinden. FSx
- cloudwatch — Ermöglicht Nimble Studio das Abrufen von Metriken. 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 verwaltete Richtlinie: **AmazonNimbleStudio-StudioUser**

Sie können die AmazonNimbleStudio-StudioUser-Richtlinie an Ihre IAM-Identitäten anfügen.

Fügen Sie diese Richtlinie der Benutzerrolle hinzu, die Ihrem Studio zugeordnet ist, um Zugriff auf Amazon Nimble Studio-Ressourcen zu gewähren, die dem Studio-Benutzer zugeordnet sind, und auf zugehörige Studio-Ressourcen in anderen Diensten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- nimble — Ermöglicht Studio-Benutzern den Zugriff auf Nimble-Ressourcen, die ihnen von delegiert wurden. StudioAdmins
- sso — Ermöglicht Studio-Benutzern, die Namen anderer Benutzer im Studio einzusehen.
- identitystore — Ermöglicht Studio-Benutzern die Möglichkeit, die Namen anderer Benutzer im Studio einzusehen.
- ds — Ermöglicht Nimble Studio, virtuelle Workstations zu den mit dem Studio verknüpften Workstations hinzuzufügen. AWS Managed Microsoft AD
- ec2 — Ermöglicht Nimble Studio, virtuelle Workstations an Ihre konfigurierte VPC anzuhängen.
- fsx — Ermöglicht Nimble Studio, virtuelle Workstations mit Ihren konfigurierten Amazon-Volumes zu verbinden. 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 aktualisiert verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon Nimble Studio an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Richtlinie aktualisieren	Amazon Nimble Studio hat eine Richtlinie aktualisiert, um die neueste Version des Identity Store-Service zu verwenden.	22. September 2023
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioAdmin` – Richtlinie aktualisieren	Amazon Nimble Studio hat eine Richtlinie aktualisiert, um die neueste Version des Identity Store-Service zu verwenden.	22. September 2023
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Richtlinie aktualisieren	Amazon Nimble Studio hat eine Richtlinie aktualisiert, die es Studio-Benutzern ermöglicht, ihre Workstation-Backups einzusehen.	20. Dezember 2022
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioAdmin` – Richtlinie aktualisieren	Amazon Nimble Studio hat die Richtlinie aktualisiert, sodass Studio-Administratoren ihre Workstation-Backups einsehen können.	20. Dezember 2022
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Richtlinie aktualisieren	Amazon Nimble Studio hat eine Richtlinie aktualisiert, die es Studio-Administratoren ermöglicht, Metriken abzurufen CloudWatch.	11. November 2021

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Richtlinie aktualisieren	Amazon Nimble Studio hat die Richtlinie aktualisiert, sodass Studio-Benutzer ihre Workstations starten und beenden können.	1. November 2021
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioAdmin` – Richtlinie aktualisieren	Amazon Nimble Studio hat die Richtlinie aktualisiert, sodass Studio-Administratoren ihre Workstations starten und beenden können.	1. November 2021
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Richtlinie aktualisieren	Amazon Nimble Studio hat die Richtlinie aktualisiert, um den Zugriff auf Streaming-Sitzungsressourcen unter bestimmten Bedingungen zu ermöglichen, die auf statt auf basieren. `nimble:ownedBy` `nimble:createdBy`	16. August 2021
AWS verwaltete Richtlinie: `AmazonNimbleStudio-StudioUser` – Neue Richtlinie	Amazon Nimble Studio hat eine neue Richtlinie hinzugefügt, die den Zugriff auf Ressourcen ermöglicht, die dem Studio-Benutzer zugeordnet sind, und auf zugehörige Studio-Ressourcen in anderen Diensten.	28. April 2021

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: AmazonNimbleStudio-StudioAdmin – Neue Richtlinie	Amazon Nimble Studio hat eine neue Richtlinie hinzugefügt, die den Zugriff auf Ressourcen ermöglicht, die mit dem Studio-Administrator verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten.	28. April 2021
AWS verwaltete Richtlinie: AmazonNimbleStudio-LaunchProfileWorker – Neue Richtlinie	Amazon Nimble Studio hat eine neue Richtlinie hinzugefügt, die den Zugriff auf Ressourcen ermöglicht, die von Nimble Studio-Startprofil-Workern benötigt werden.	28. April 2021
Amazon Nimble Studio hat mit der Nachverfolgung von Änderungen begonnen	Amazon Nimble Studio hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	28. April 2021

Serviceübergreifende Confused-Deputy-Prävention

Bei dem Problem mit verwirrten Stellvertretern handelt es sich um ein Sicherheitsproblem, bei dem eine Entität, die nicht zur Durchführung einer Aktion berechtigt ist, eine Entität mit mehr Rechten dazu zwingen kann, die Aktion auszuführen. In AWS: Dienstübergreifendes Identitätswechsels kann zum Problem des verwirrten Stellvertreters führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der Anruf-Service) einen anderen Service anruft (den aufgerufenen Service). Der anrufende Service kann so manipuliert werden, dass er seine Berechtigungen nutzt, um auf die Ressourcen eines anderen Kunden in einer Weise zu agieren, für die er sonst keine Zugriffsberechtigung hätte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die Identity and Access Management (IAM) Amazon Nimble Studio für den Zugriff auf Ihre Ressourcen gewährt. Wenn Sie beide Kontextschlüssel für globale Bedingungen verwenden, müssen der `aws:SourceAccount` Wert und das Konto im `aws:SourceArn` Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienerklärung verwendet werden.

Der Wert von `aws:SourceArn` muss der ARN des Studios sein und `aws:SourceAccount` muss Ihre Konto-ID sein. Sie werden nicht wissen, wie die Studio-ID lautet, bis das Studio erstellt wurde, da es von Nimble Studio generiert wurde. Sobald Ihr Studio erstellt ist, können Sie die Vertrauensrichtlinie so aktualisieren, dass die endgültige Studio-ID als festgelegt ist. `aws:SourceArn`

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit Platzhaltern (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:nimble::123456789012:*`.

Ihre Endbenutzer nehmen Ihre Studio-Rolle an, wenn sie sich beim Nimble Studio-Portal anmelden. Wenn Sie Ihr Studio erstellen, AWS konfiguriert es die Rolle und bewertet die Richtlinie. AWS bewertet die Richtlinie jedes Mal, wenn sich einer Ihrer Benutzer beim Nimble Studio-Portal anmeldet. Wenn Sie ein Studio erstellen, können Sie das nicht ändern. `aws:SourceArn` Nachdem Sie mit der Erstellung Ihres Studios fertig sind, können Sie Ihr StudioARN für die verwenden. `aws:SourceArn`

Das folgende Beispiel ist eine Richtlinie zur Übernahme einer Rolle, die zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Nimble Studio verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

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

Fehlerbehebung bei Identität und Zugriff auf Amazon Nimble Studio

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Nimble Studio und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Nimble Studio durchzuführen.
- Ich bin nicht berechtigt, iam: PassRole auszuführen.
- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen den Zugriff auf Nimble Studio ermöglichen.
- Ich möchte Personen außerhalb von mir den Zugriff auf meine Nimble AWS-Konto Studio-Ressourcen ermöglichen.

Ich bin nicht berechtigt, eine Aktion in Nimble Studio durchzuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `nimble:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `nimble:GetWidget`-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam: PassRole auszuführen.

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, wenden Sie sich an Ihren Administrator, um Unterstützung zu erhalten. Bitten Sie ihn, Ihre Richtlinien zu aktualisieren, damit Sie eine Rolle an Nimble Studio übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Dazu benötigen Sie Berechtigungen, um die Rolle an den Dienst zu übergeben.

Der folgende Beispielfehler tritt auf, wenn ein Benutzer mit dem Namen `johndoe` versucht, die Konsole zu verwenden, um eine Aktion in Nimble Studio auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Service-Rolle gewährt werden. John ist nicht berechtigt, die Rolle an den Dienst weiterzugeben.

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

In diesem Fall bittet John seinen Administrator, seine Richtlinien zu aktualisieren, um die Erlaubnis zur Durchführung der `iam:PassRole` Aktion zu erteilen.

Ich möchte meine Zugriffsschlüssel anzeigen

Amazon Nimble Studio stellt keine Zugriffsschlüssel zur Verfügung. Weitere Informationen zu geheimen Zugriffsschlüsseln finden Sie unter Verwaltung von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

> **Important**
>
> Geben Sie Ihre Zugangsschlüssel nicht an Dritte weiter, auch nicht, um Ihre kanonische Benutzer-ID zu finden. Wenn Sie dies tun, gewähren Sie anderen Personen möglicherweise den permanenten Zugriff auf Ihr Konto.

Wenn Sie ein Zugriffsschlüsselpaar erstellen, werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Ort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, fügen Sie Ihrem Benutzer neue Zugangsschlüssel hinzu. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei haben, löschen Sie ein key pair, bevor Sie ein neues erstellen. Anweisungen finden Sie unter Verwaltung von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen den Zugriff auf Nimble Studio ermöglichen.

Um anderen den Zugriff auf Nimble Studio zu ermöglichen, erstellen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Fügen Sie dann der Entität eine Richtlinie hinzu, die ihnen die richtigen Berechtigungen gewährt.

Nimble Studio bietet Ihnen das `AmazonNimbleStudio-StudioUser` in der AWS Management Console. Der IT-Administrator, der die Konsole verwaltet, verwendet diese Richtlinie, um anderen Benutzern Zugriff auf Studio zu gewähren.

Ein Tutorial zur Verwendung der Admin-Richtlinie finden Sie in der Einrichtung für Nimble Studio Anleitung. Informationen zum Anhängen vorhandener Richtlinien an Benutzer, z. B. Benutzer- und Startprofilrichtlinien, finden Sie unter IAM-Benutzer erstellen (Konsole).

Informationen zum Importieren von Richtlinien finden Sie im IAM-Benutzerhandbuch unter Erstellen Ihres ersten delegierten IAM-Benutzers und Ihrer ersten delegierten IAM-Gruppe.

Ich möchte Personen außerhalb von mir den Zugriff auf meine Nimble AWS-Konto Studio-Ressourcen ermöglichen.

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Nimble Studio diese Funktionen unterstützt, finden Sie unter. So funktioniert Amazon Nimble Studio mit IAM

- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Unterschiede zwischen IAM-Rollen und ressourcenbasierten Richtlinien.

Protokollierung und Überwachung von Sicherheitsereignissen mit Nimble Studio

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Nimble Studio und Ihren AWS Lösungen. Sammeln Sie Überwachungsdaten aus allen Teilen Ihrer AWS Lösung, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können.

AWS und Nimble Studio bieten Tools zur Überwachung Ihrer Ressourcen und zur Reaktion auf potenzielle Vorfälle, einschließlich eines BenutzerhandbuchsNimble Studio-Anrufe protokollieren mit AWS CloudTrail.AWS CloudFormation

Weitere Informationen zur Verwendung von Amazon Nimble Studio AWS CloudFormation, einschließlich Beispielen für JSON- und YAML-Vorlagen, finden Sie in der Ressourcen- und Eigenschaftsreferenz zu Amazon Nimble Studio im AWS CloudFormation Benutzerhandbuch. Informationen zur Verwendung von CloudFormation Vorlagen finden Sie unter Konzepte.AWS CloudFormation

Themen

- Nimble Studio-Anrufe protokollieren mit AWS CloudTrail

Nimble Studio-Anrufe protokollieren mit AWS CloudTrail

Amazon Nimble Studio ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Nimble Studio ausgeführten

Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für Nimble Studio als Ereignisse. Zu den erfassten Anrufen gehören Anrufe von der Nimble Studio-Konsole und Code-Aufrufe an die Amazon Nimble Studio-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Nimble Studio. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an Nimble Studio, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Informationen zu Nimble Studio in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Nimble Studio eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen im CloudTrail Event-Verlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für Nimble Studio, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren.

Weitere Informationen finden Sie hier:

Übersicht zum Erstellen eines Trails

CloudTrail unterstützte Dienste und Integrationen

Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

Empfangen von CloudTrail Protokolldateien aus mehreren Regionen

Empfangen von CloudTrail Protokolldateien von mehreren Konten

Nimble Studio-Aktionen werden von der Amazon Nimble Studio API-Referenz protokolliert CloudTrail und sind dort dokumentiert. Beispielsweise generieren Aufrufe von GetStudio und DeleteStudio Aktionen Einträge in den CloudTrail Protokolldateien. CreateStudio

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen -Service gesendet wurde

Weitere Informationen finden Sie unter dem Element CloudTrail Benutzeridentität.

Grundlegendes zu den Einträgen in Nimble Studio-Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail -Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Dieses JSON-Beispiel zeigt drei Aktionen:

- AKTION_1: CreateStudio
- AKTION_2: GetStudio
- AKTION_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"
}
```

In dem Beispiel werden Sie feststellen, dass die Ereignisse die Region, die IP-Adresse und andere „requestParameters“ wie "" und "userRoleArn" anzeigen, anhand derer Sie das Ereignis identifizieren können. adminRoleArn Sie können die Uhrzeit und das Datum im Feld „CreationDate“ sowie die Quelle sehen, von der die Anfrage stammt, die als „EventSource“ gekennzeichnet ist: „nimble.amazonaws.com“.

CloudTrail ist auf Ihrem aktiviert, wenn Sie das Konto erstellen. AWS-Konto Wenn eine Aktivität in IAM oder AWS STS auftritt, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto anzeigen, suchen und herunterladen.

AWS CloudTrail erfasst alle API-Aufrufe für IAM und AWS Security Token Service (AWS STS) als Ereignisse, einschließlich Aufrufe von der Konsole und API-Aufrufe. Weitere Informationen zur Verwendung CloudTrail mit IAM und AWS STS finden Sie unter Protokollieren von IAM- und AWS STS API-Aufrufen mit. AWS CloudTrail

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu anderen von Amazon angebotenen Überwachungsdiensten finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Konformitätsprüfung für Amazon Nimble Studio

Amazon Nimble Studio folgt dem Modell der geteilten Verantwortung, und die Einhaltung der Vorschriften erfolgt zwischen unseren Kunden AWS und unseren Kunden.

Um zu erfahren, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm AWS-Services unter und

wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu

überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Infrastruktursicherheit in Amazon Nimble Studio

Als verwalteter Service ist Amazon Nimble Studio durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Nimble Studio zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Bewährte Sicherheitsmethoden für Nimble Studio

Amazon Nimble Studio bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden

bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Überwachen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Nimble Studio und Ihren AWS Lösungen. Weitere Informationen zur Überwachung und Reaktion auf Ereignisse finden Sie unterProtokollierung und Überwachung von Sicherheitsereignissen mit Nimble Studio.

Datenschutz

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und individuelle Konten mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Nimble Studio oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Amazon Nimble Studio oder andere Dienste eingeben, werden möglicherweise zur Aufnahme in Diagnoseprotokolle aufgenommen. Wenn Sie eine URL für einen

externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Berechtigungen

Verwalten Sie den Zugriff auf AWS Ressourcen mithilfe von Benutzern und IAM-Rollen und indem Sie Benutzern die geringsten Rechte gewähren. Richten Sie Richtlinien und Verfahren zur Verwaltung von Anmeldeinformationen für die Erstellung, Verteilung, Rotation und den Widerruf AWS von Zugangsdaten ein. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Support für Nimble Studio

Dieser Abschnitt enthält Support-Optionen für Nimble Studio, z. B. wie Sie Hilfe bei der Bereitstellung oder Nutzung des Dienstes und der zugehörigen Anwendungen erhalten.

Inhalt

Das Nimble Studio-Forum

Wenn Sie Fragen zu Nimble Studio haben, können Sie das Nimble Studio-Forum besuchen. Dort erhalten Sie von der Community und den AWS Forum-Moderatoren Antworten zu den Funktionen von Nimble Studio, zu technischen Problemen und Hilfe bei der Fehlerbehebung.

Unterstützung für Anwendungen

Nimble Studio bietet zusätzliche Dokumentation für die folgenden Anwendungen.

AWSThinkboxDeadline

Wenn Sie Hilfe mit Ihrer Renderfarm benötigen oder erfahren möchten, wie Deadline funktioniert, siehe AWSThinkboxDeadline Dokumentation.

Nimble Studio File Transfer

Informationen zur Funktionsweise von File Transfer finden Sie im Nimble Studio File Transfer-Benutzerhandbuch.

Support Mitte

Das Support Center ist eine zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer Supportfälle. Es bietet Zugriff auf eine Vielzahl von Ressourcen, darunter Abrechnungs- und technische Lösungen,

ein Wissenszentrum, Videos und AWS Dokumentation im Wissenszentrum sowie Schulungen und Zertifizierungen.

Support Pläne

Support Pläne helfen Ihnen dabei, die Leistung zu optimieren, Sicherheit zu gewährleisten, Ausfallzeiten zu vermeiden und die Kosten zu kontrollieren. Weitere Informationen zu Support Plänen finden Sie unter Support Tarife vergleichen.

Weitere Informationen darüber, wie wir Sie unterstützen AWS können, finden Sie auf der Seite Kontakt.

Dokumentverlauf

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 2. Oktober 2024

In der folgenden Tabelle werden wichtige Änderungen in jeder Version des Nimble Studio Administrator Guide beschrieben.

Änderung	Beschreibung	
Hinweis zum Ende des Supports	Hinweis zum Ende des Supports: Am 22. Oktober 2024 AWS wird der Support für Amazon Nimble Studio eingestellt. Nach dem 22. Oktober 2024 können Sie nicht mehr auf die Nimble Studio-Konsole oder die Nimble Studio-Ressourcen zugreifen.	2. Oktober 2024
AWS verwaltete Richtlinienaktualisierungen	Die `AmazonNimbleStudio-StudioUser` `AmazonNimbleStudio-StudioAdmin` Richtlinien wurden aktualisiert, um die neueste Version des AWS IAM Identity Center Dienstes zu verwenden.	22. September 2023
Neuer Dienst mit dazugehörigem Handbuch	Dies ist die erste Version von Amazon Nimble Studio und das Amazon Nimble Studio Administrator Guide.	19. Juni 2023

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.