管理者ガイド

Amazon Nimble Studio

Amazon Nimble Studio: 管理者ガイド

Table of Contents

Amazon Nimble Studio とは

Nimble Studio は、アーティストがクラウドでビジュアルエフェクト、アニメーション、ゲームコンテンツを制作するために使用できる一連のアプリケーションとサービスのインフラストラクチャと一元管理を提供します。

Nimble Studio では、ユーザーとグループの管理に欠かせないツールを手に入れることができます。また、AWS Thinkbox や Nimble Studio File Transfer などのアプリケーションを追加して管理することも可能です。

Nimble Studio は、スタジオのすべてのリソースを 1 か所にまとめる統合インターフェイスを備えています。ユーザーのオンボーディング、アプリケーションの割り当て、職務固有の権限の付与を行うことができます。Nimble Studio では、AWS の経験は必要ありません。約 5 分でセットアップが完了します。

目次

特徴と利点

Nimble Studio で使用できる特徴と利点の一部を以下に紹介します。

- Nimble Studio は無料で使用できます。お支払いいただくのは、アプリケーションが使用するスタジオリソースの分のみです。
- スタジオを一元管理し、ステータスを確認して、運営に関する概要レベルのインサイトを取得できます。
- Nimble Studio のアプリケーション、ユーザー、グループを追加および管理し、アクセス許可をアタッチします。
- AWS Identity and Access Management (IAM) ポリシーとロールを使用して、スタジオリソースへのアクセスを安全に管理します。
- スタジオユーザーと外部 ID プロバイダーのサインインセキュリティを AWS IAM Identity Center (IAM Identity Center) で管理します。

- スタジオリソースにタグを付けて整理し、簡単に検索できます。

関連アプリケーション

Nimble Studio は、デジタルコンテンツ制作者がクラウドベースのスタジオを運用してビジュアルエフェクト (VFX)、アニメーション、インタラクティブコンテンツを制作する際に必要となるアプリケーションを提供します。

これらのアプリケーションは、ローカルコンピュータにインストールすることも、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを使用してクラウドにインストールすることもできます。また、Amazon Simple Storage Service (Amazon S3) を使用して、デジタルメディアアセットを安全に転送して保存することもできます。つまり、Nimble Studio を使用すれば、物理インフラストラクチャ、機器、技術スタッフにかかるコストを削減できるということです。

Nimble Studio は現在、以下のアプリケーションを提供しています。

- AWS Thinkbox: Thinkbox ソフトウェアには、レンダーファームマネージャーの Thinkbox Deadline と 3D プラグインの Thinkbox Krakatoa が含まれています。Thinkbox ソフトウェアを使用すると、オンプレミス、Amazon EC2 のクラウド、あるいはその両方でスタジオのクリエイティブなアウトプットを増やすことができます。詳細については、「AWS Thinkbox 製品」を参照してください。
- Nimble Studio File Transfer: File Transfer によって、Amazon S3 との間のデジタルメディアアセットの送受信を高速化します。File Transfer はグラフィカルユーザーインターフェイスを備えているため、何千もの数にのぼるメディアファイルをすばやく移動できます。詳細については、「Nimble Studio File Transfer とは?」ページを参照してください。

Nimble Studio の料金

Nimble Studio を設定して、Studio のインフラストラクチャ、ユーザー、セキュリティ、サービスの管理に使用しても、料金はかかりません。

ただし、お使いのスタジオでサービスやアプリケーションを設定すると、ストレージやその他のスタジオリソースの料金が請求される場合があります。Nimble Studio アプリケーションの料金の詳細については、個々のアプリケーションの料金表を参照してください。

AWS の費用管理については、「AWS Cost Explorer Service」および「AWS Budgets」を参照してください。

Nimble Studio の使用を開始する方法

Nimble Studio のセットアップとデプロイには約 5 分かかります。

Nimble Studio の概念と用語について理解したら、「Amazon Nimble Studio の開始方法」を参照してください。Studio をデプロイするためのステップバイステップの手順が記載されています。

Amazon Nimble Studio の概念と用語

このガイドでは、Amazon Nimble Studio の仕組みを理解し使用を開始するために、主要な概念と用語を参照できます。

主な特徴

Amazon Nimble Studio

Amazon Nimble Studio は、ビジュアルエフェクト、アニメーション、インタラクティブコンテンツを、クリエイティブスタジオがストーリーボードのスケッチから最終的な成果物に至るまで、完全にクラウド内で作成することを可能にする AWS のサービス のサービスです。

Amazon Nimble Studio コンソール

Nimble Studio コンソールは、IT 部門の管理者であるお客様専用として、AWS Management Console の中に包含されています。このコンソールで、管理者はクラウドスタジオを作成し、多くの設定を管理します。例えば Studio マネージャーページでは、リソースの追加や削除、アプリケーションの追加、ユーザーおよびグループへのアクセス許可の付与を行うことができます。

Amazon Nimble Studio ポータル

Nimble Studio ポータルは、Nimble Studio のアプリケーションやサービスを日常的に操作するためのユーザーインターフェイスを提供します。ユーザーは、AWS Management Console とやり取りすることなく、ユーザー名とパスワードを使用してポータルに直接サインインします。

Nimble Studio File Transfer

File Transfer によって、Amazon Simple Storage Service (Amazon S3) との間のデジタルメディアアセットの送受信を高速化します。File Transfer はグラフィカルユーザーインターフェイスを備えているため、何千もの数にのぼるメディアファイルをすばやく移動できます。詳細については、「Nimble Studio File Transfer とは?」ページを参照してください。

AWS Thinkbox

Thinkbox ソフトウェアには、レンダーファームマネージャーの Thinkbox Deadline と、3D プラグインの Thinkbox Krakatoa が含まれています。Thinkbox ソフトウェアを使用すると、オンプレミス、Amazon EC2 のクラウド、あるいはその両方でスタジオのクリエイティブなアウトプットを増やすことができます。詳細については、「AWS Thinkbox 製品」を参照してください。

主要な概念と用語

AWS 管理ポリシー

AWS 管理ポリシーは、AWS が作成および管理するスタンドアロンポリシーです。スタンドアロンポリシーとは、ポリシー名を含む独自の Amazon リソースネーム (ARN) の付いたポリシーです。例えば、arn:aws:iam::aws:policy/IAMReadOnlyAccess は AWS 管理ポリシーの 1 つです。ARN の詳細については、「IAM ARN」(IAM の ARN) を参照してください。

AWS 管理ポリシーは、一般的なジョブ機能にアクセス許可を付与するために使用されます。ジョブ機能ポリシーは、新しいサービスや API オペレーションの導入時に、AWS によって保守および更新されます。たとえば、AdministratorAccess ジョブ関数は、AWS の各サービスおよびリソースへのフルアクセスを許可し、アクセス許可の委任が可能です。一方、AmazonMobileAnalyticsWriteOnlyAccess や AmazonEC2ReadOnlyAccess など、部分的なアクセス用の AWS 管理ポリシーでは、AWS のサービス への完全なアクセスではなく特定レベルのアクセスを許可します。アクセスポリシーの詳細については、ポリシー概要内のアクセスレベルの概要についてを参照してください。

AWS Management Console

AWS Management Console マネジメントコンソールは、AWS のサービス を管理するための広範なサービスコンソールコレクションへのアクセス権を提供するウェブアプリケーションです。

各サービスには独自のコンソールも含まれます。これらのコンソールは、クラウドコンピューティング用の各種ツールを提供します。さらに、請求とコスト管理に役立つサービスもあります。

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center は、複数の AWS アカウントとビジネスアプリケーションへのアクセスを簡単に一元管理できるようにする AWS のサービスです。IAM Identity Center を使用すると、割り当てられたすべてのアカウントとアプリケーションに 1 か所からアクセスするための、シングルサインオンアクセスをユーザーに提供できます。また、AWS Organizations のすべてのアカウントへのマルチアカウントアクセスとユーザーのアクセス許可を、一元的に管理することも可能です。詳細については、「AWS IAM Identity Center のよくある質問」を参照してください。

AWSPrivateLink

AWS PrivateLink により、トラフィックをパブリックインターネットに露出させることなく、VPC、AWS のサービス、およびオンプレミスネットワーク間でのプライベート接続が行えま

す。AWS PrivateLink では、異なるアカウントと VPC 間でのサービス接続が簡単になります。AWS PrivateLink は AWS アカウントに請求される月額料金の範囲でご利用いただけます。

デジタルコンテンツ作成 (DCC)

デジタルコンテンツ作成 (DCC) とは、Blender、Nuke、Maya、Houdini など、クリエイティブコンテンツの作成に使用されるアプリケーションのカテゴリを指します。

リージョン

Nimble Studio では、11 の AWS リージョンから選択してスタジオをデプロイできます。リージョンは、データやアプリケーションなど、必須のスタジオインフラストラクチャが存在する場所です。

リージョンはスタジオユーザーに最も近い場所に配置する必要があります。これにより遅延が減少し、データ転送速度が向上します。

スタジオ

スタジオは、他の Nimble Studio 関連リソースの最上位のコンテナです。クラウドスタジオは、Nimble Studio ウェブポータルを管理します。また VPC、ユーザーディレクトリ、ストレージ暗号化キーなど、AWS アカウント 内の重要なリソースへの接続の管理も行います。

スタジオのアプリケーション

スタジオコンポーネントは、お客様の Nimble Studio 内での設定であり、ファイルシステム、ライセンスサーバー、レンダーファームなど、AWS アカウント 内のリソースにアクセスする方法をサービスに対し指示します。

Nimble Studio には、共有ファイルシステム、コンピューティングファーム、アクティブディレクトリ、ライセンスコンポーネントなど、多数のスタジオコンポーネントのサブタイプが含まれています。これらのサブタイプは、スタジオで使用するリソースについて記述します。

スタジオリソース

スタジオリソースは、スタジオが日常業務に必要なものをカプセル化することを表す用語です。リソースをクラウドスタジオのインフラストラクチャに収める方法を記述する際、これらはスタジオコンポーネントとも呼ばれます。

タグ

タグとは、AWS リソースに割り当てるラベルです。各タグは、お客様が定義するキーとオプション値で構成されています。

タグを使用すると、さまざまな方法で AWS リソースを分類できます。例えば、各インスタンスの所有者とスタックレベルを追跡しやすくするため、アカウントの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに対してタグセットを定義できます。また、タグを使用すると、組織の共有ファイルシステムおよびレンダーファームを Nimble Studio に統合して、ワークフローを中断させずにワークフォースをクラウドに移行することができます。

タグにより、目的、所有者、環境別に AWS リソースを分類できます。これは、同じ型のリソースが多い場合に役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別することができます。

Nimble Studio のセットアップ

このチュートリアルは、Amazon Nimble Studio をセットアップする管理者ユーザーを対象としています。

以下のセクションでは、Nimble Studio にスタジオをデプロイする前に完了する必要がある手順について説明します。

内容

セットアップ IAM

以下を確認する AWS Identity and Access Management （ IAM) ドキュメントをスタートする前に参照してください。

- IAM でのセキュリティのベストプラクティス
- にサインインする AWS アカウント 管理者ユーザーとして、残りのセットアップを完了します。

にサインアップする AWS アカウント

をお持ちでない場合 AWS アカウントで、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/サインアップ を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップするとき AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーはすべての にアクセスできます AWS のサービス アカウントの および リソース。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ に移動し、マイアカウント を選択すると、いつでも現在のアカウントアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップした後 AWS アカウント、 をセキュリティで保護する AWS アカウントのルートユーザー、有効化 AWS IAM Identity Center、および 管理ユーザーを作成して、日常的なタスクにルートユーザーを使用しないようにします。

のセキュリティ保護 AWS アカウントのルートユーザー

1. にサインインします。AWS Management Console ルートユーザーを選択し、 AWS アカウント E メールアドレス。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、「」の「ルートユーザーとしてサインインする」を参照してください。 AWS サインイン ユーザーガイド。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「 の仮想MFAデバイスの有効化」を参照してください。 AWS アカウントIAM ユーザーガイドのルートユーザー (コンソール) 。

管理アクセスを持つユーザーを作成する

1. IAM Identity Center を有効にします。

   手順については、「 の有効化」を参照してください。 AWS IAM Identity Center ()AWS IAM Identity Center ユーザーガイド。
2. IAM Identity Center で、ユーザーに管理アクセス権を付与します。

   の使用に関するチュートリアル IAM アイデンティティセンターディレクトリ ID ソースとして、「デフォルトを使用してユーザーアクセスを設定する」を参照してください。 IAM アイデンティティセンターディレクトリ ()AWS IAM Identity Center ユーザーガイド。

管理アクセス権を持つユーザーとしてサインインする

- IAM Identity Center ユーザーでサインインするには、IAMIdentity Center ユーザーの作成時に E メールアドレスにURL送信されたサインインを使用します。

IAM Identity Center ユーザーを使用してサインインする方法については、「 へのサインイン」を参照してください。 AWS の アクセスポータル AWS サインイン ユーザーガイド。

追加のユーザーにアクセス権を割り当てる

1. IAM Identity Center で、最小特権のアクセス許可を適用するベストプラクティスに従うアクセス許可セットを作成します。

   手順については、「」の「アクセス許可セットの作成」を参照してください。 AWS IAM Identity Center ユーザーガイド。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「」の「グループの追加」を参照してください。 AWS IAM Identity Center ユーザーガイド。

関連リソース

- IAM におけるセキュリティのベストプラクティス
- AWS のサービス クォータ - AWS 全般のリファレンス

Amazon Nimble Studio の開始方法

この章では、Nimble Studio コンソールを使用してスタジオのインフラストラクチャを作成する方法、AWS リージョンを確認する方法、およびスタジオを作成する方法について説明します。また、詳細設定を使用してセットアップをカスタマイズすることもできます。

AWS を初めてご利用のお客様は、「Nimble Studio のセットアップ」のチュートリアルを参照してください。

トピック

Nimble Studio のセットアップ

このガイドでは、インフラストラクチャの設定、設定の確認、スタジオの作成方法を説明します。また、「スタジオの詳細設定」を使用してスタジオをカスタマイズすることもできます。

ステップ 1: スタジオインフラストラクチャを設定する

スタジオのインフラストラクチャは、次のコンポーネントで構成されています。

- スタジオの表示名: スタジオの表示名は、スタジオを識別するために使用します (「AnyCompany Studio」など)。また、スタジオの名前によってスタジオポータルの URL も決まります。スタジオの表示名は、セットアップの完了後であればいつでも変更できます。
- スタジオポータルの URL: スタジオポータルの URL を使用してスタジオにアクセスできます。URL は、スタジオの表示名が基になります (例: https://anycompanystudio.awsapps.com)。スタジオポータルの URL は、セットアップの完了後であればいつでも変更できます。
- AWS リージョン: AWS リージョンは、AWS データセンターが集まる物理的な場所です。スタジオをセットアップすると、リージョンはデフォルトで最も近い場所に設定されます。リージョンはユーザーに最も近い場所になるように変更する必要があります。これにより遅延が減少し、データ転送速度が向上します。

> **Important**
>
> リージョンは、Nimble Studio のセットアップが完了すると変更できなくなります。

スタジオのインフラストラクチャを設定するには、このセクションのタスクを完了します。

スタジオのインフラストラクチャを設定するには

1. AWS Management Console にサインインし Nimble Studio コンソールを開きます。
2. [Nimble Studio のセットアップ] を選択し、[次へ] を選びます。
3. スタジオの表示名 (例: **AnyCompany Studio**) を入力します。
4. (オプション) スタジオポータル名を変更するには、[URL を編集] を選択します。
5. (オプション) スタジオユーザーに最も近い場所になるように AWS リージョンを変更するには、[リージョンを変更] を選択します。
   a. ユーザーに最も近いリージョンを選択します。
   b. [リージョンを適用] を選択します。
6. (オプション) スタジオのセットアップをさらにカスタマイズするには、[スタジオの詳細設定] を選択します。
7. スタジオの作成を開始する前に設定を確認するには、[次へ] を選択します。

ステップ 2: スタジオを確認して作成する

スタジオのインフラストラクチャを設定したら、スタジオを確認、変更、作成できます。

スタジオを確認して作成するには

1. [確認と作成] ページで、[スタジオのインフラストラクチャ] を確認します。
2. AWS リージョンがスタジオユーザーに最も近いことを確認します。
3. (オプション) スタジオのセットアップを変更するには、[編集] を選択します。
4. 準備が完了したら、[スタジオを作成] を選択します。

スタジオの詳細設定

Nimble Studio のセットアップには、スタジオの詳細設定が含まれます。これらの設定により、Nimble Studio のセットアップで AWS アカウントに対して行った変更をすべて表示したり、スタジオユーザーロールを設定したり、暗号化キータイプを変更したりできます。スタジオリソースにオプションのタグを追加することもできます。

スタジオユーザーロールを設定する

AWS のサービスでは、お客様に代わってアクションを実行するサービスロールを割り当てることができます。Nimble Studio には、サービスでスタジオ内のリソースに対するアクセス許可をユーザーに付与するためのスタジオユーザーロールが必要です。

スタジオユーザーロールには AWS Identity and Access Management (IAM) 管理ポリシーをアタッチできます。このポリシーにより、ユーザーは特定の Nimble Studio アプリケーションでのジョブの作成など、特定のアクションを実行できます。アプリケーションは管理ポリシーの特定の条件に依存するため、管理ポリシーを使用しないと、アプリケーションが期待どおりに動作しない可能性があります。

スタジオユーザーロールは、セットアップの完了後であればいつでも変更できます。ユーザーロールの詳細については、「IAM ロール」を参照してください。

以下のタブには、2 つの異なるユースケースの説明が含まれています。新しいサービスロールを作成して使用するには、[新しいサービスロール] タブを選択します。既存のサービスロールを使用するには、[既存のサービスロール] タブを選択します。

New service role

新しいサービスロールを作成して使用するには

1. [新しいサービスロールを作成し使用する] を選択します。
2. (オプション) サービスユーザーロール名を入力します。
3. ロールの詳細については、[許可の詳細を表示] を選択します。

Existing service role

既存のサービスロールを使用するには

1. [既存のサービスロールを使用する] を選択します。
2. ドロップダウンリストを開いて既存のサービスロールを選択します。
3. (オプション) ロールの詳細については、[IAM コンソールで表示] を選択してください。

AWS IAM Identity Center

AWS IAM Identity Center は、ユーザーとグループを管理するための、クラウドベースのシングルサインオンサービスです。IAM Identity Center をエンタープライズシングルサインオン (SSO) プロバイダーと統合して、ユーザーが会社のアカウントでサインインできるようにすることも可能です。

Nimble Studio では IAM Identity Center がデフォルトで有効になっており、Nimble Studio をセットアップして使用する際に必要となります。詳細については、「AWS IAM Identity Center とは」を参照してください。

AWS KMS 暗号化キーを設定する

AWS Key Management Service (AWS KMS) キーは、データの暗号化、復号化、再暗号化に使用できる KMS キーの主要なタイプです。

Nimble Studio には以下のタイプの AWS KMS 暗号化キーが含まれています。

- AWS 所有キー - AWS 所有キーは、複数の AWS アカウントで使用するために AWS のサービスが所有および管理する KMS キーです。AWS 所有キーは AWS アカウント内にはありませんが、Nimble Studio は AWS 所有キーを使用してアカウント内のリソースを保護できます。

  AWS KMS を使用するために、キーやそのキーポリシーを作成または管理する必要はありません。AWS 所有キーの使用に費用はかかりません。また、所有キーは AWS アカウントの AWS KMS クォータにはカウントされません。
- カスタマーマネージド AWS KMS キー - カスタマーマネージドキーは、ユーザーが作成、所有、管理する AWS アカウント内の KMS キーです。

  ユーザーは、この KMS キーに関する完全なコントロール権を持ちます。カスタマーマネージドキーには、月額料金が発生します。また、無料利用枠を超える AWS KMS には、API リクエストごとに料金がかかります。AWS KMSの料金の詳細については、「AWS Key Management Service 料金表」を参照してください。

暗号化キータイプは、セットアップ完了後は変更できません。AWS KMS および暗号化キータイプの詳細については、AWS KMS のドキュメントを参照してください。

別の暗号化キータイプを選択するには

1. [異なる AWS KMS キーを選択 (高度)] を選択します。
2. AWS KMS キーを選択するか、Amazon リソース番号 (ARN) を入力します。

3. [AWS KMS キーの作成] を選択します。

タグを設定する

タグは Nimble Studio リソースを整理するためのラベルとして機能します。タグは最大 50 個まで追加でき、リソースの識別、整理、検索、フィルタリングに役立ちます。

各タグは 2 つの部分で構成されます。1 つは Key というタグで、もう 1 つはオプションの Value タグです (例: key: `domain` と value: `anycompanystudio.com`)。

タグは、セットアップの完了後であればいつでも追加または削除できます。タグの詳細については、「AWS リソースにタグを付ける」を参照してください。

スタジオリソースにタグを追加するには

1. 新しいタグを追加を選択します。
2. タグキーを入力します。
3. (オプション) Value タグを入力します。

スタジオを削除する

スタジオが不要になった場合は、削除することができます。スタジオを削除すると、スタジオのインフラストラクチャのみが削除されます。ユーザーロール、ポリシー、アプリケーションデータなど、その他の AWS リソースはそのまま残ります。

> **Important**
>
> スタジオは、削除後に回復することはできません。

スタジオを削除するには

1. AWS Management Console にサインインし Nimble Studio コンソールを開きます。
2. [Studio 概要] を選択します。
3. [アクション] を選択して、[スタジオを削除] を選びます。
4. 「**delete**」と入力し、[削除] を選択します。

セキュリティ Amazon Nimble Studio

でのクラウドセキュリティ AWS が最優先事項です。として AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 間で共有される責任です。 AWS とユーザー。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 が実行するインフラストラクチャを保護する責任を負います。 AWS の サービス AWS クラウド. AWS は、安全に使用できる サービスも提供します。サードパーティーの監査者は、 の一環として、当社のセキュリティの有効性を定期的にテストおよび検証します。 AWS コンプライアンスプログラム。に適用されるコンプライアンスプログラムについて学ぶには Amazon Nimble Studio、「」を参照してください。 AWS コンプライアンスプログラムによる対象範囲内のサービス。
- クラウド内のセキュリティ — お客様の責任は によって決まります。 AWS 使用する サービス。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

> **Important**
>
> セキュリティの柱 - を読み、理解しておくことを強くお勧めします。 AWS Well-Architected フレームワーク 。この記事には、 のセキュリティを保護するための主要な原則が含まれています。 AWS インフラストラクチャ。

このドキュメントは、 の使用時に責任共有モデルを適用する方法を理解するのに役立ちます。Nimble Studio。 以下のトピックでは、 を設定する方法を示します。Nimble Studio セキュリティとコンプライアンスの目標を達成するための 。また、他の の使用方法についても説明します。AWS のモニタリングと保護に役立つ のサービス Nimble Studio リソースの使用料金を見積もることができます。

詳細情報

- セキュリティの柱 - AWS Well-Architected フレームワーク
- のセキュリティ AWS Cloud Development Kit (AWS CDK) (AWS CDK)

- Amazon Virtual Private Cloud でのセキュリティ
- AWS セキュリティ認証情報
- Amazon のセキュリティ EC2
  - Linux
  - Windows

セットアップする AWS アカウント セキュリティ

このガイドでは、 AWS アカウント リソースが侵害されたときに通知を受信し、特定の AWS アカウント ユーザーがアクセスします。を保護するには AWS アカウント リソースを追跡するには、次のステップを実行します。

内容

- アカウントのアクセスキーを削除する
- Multi-Factor·Authentication を有効にする
- すべての CloudTrail で を有効にする AWS リージョン
- Amazon GuardDuty および 通知を設定する

アカウントのアクセスキーを削除する

へのプログラムによるアクセスを許可できます。 AWS からの リソース AWS Command Line Interface (AWS CLI) または と AWS APIs。ただし、 AWS では、プログラムによるアクセスのためにルートアカウントに関連付けられたアクセスキーを作成または使用しないことをお勧めします。

アクセスキーがまだ残っている場合は、それらを削除してユーザーを作成することをお勧めします。次に、呼び出す予定の に必要なアクセス許可のみをAPIsそのユーザーに付与します。そのユーザーを使ってアクセスキーを発行できます。

詳細については、「 のアクセスキーの管理」を参照してください。 AWS アカウント ()AWS 全般のリファレンス ガイド 。

Multi-Factor·Authentication を有効にする

多要素認証 (MFA) は、ユーザー名とパスワードに加えて認証レイヤーを提供するセキュリティ機能です。

MFA は次のように動作します。ユーザー名とパスワードでサインインしたら、自分だけが物理的にアクセスできる追加の情報も提供する必要があります。この情報は、専用のMFAハードウェアデバイスから、または電話のアプリから取得できます。

サポートされているMFAデバイスのリストから、使用するデバイスのタイプを選択する必要があります。 MFA ハードウェアデバイスの場合は、MFAデバイスを安全な場所に保管してください。

仮想MFAデバイス (電話アプリなど) を使用する場合は、電話が紛失したり破損したりした場合に何が起こるかを検討してください。1 つの方法は、使用する仮想MFAデバイスを安全な場所に保持することです。もう 1 つのオプションは、複数のデバイスを同時にアクティブ化するか、デバイスキーの復旧に仮想MFAオプションを使用することです。

の詳細についてはMFA、「Virtual Multi-Factor Authentication (MFA) Device の有効化」を参照してください。

関連リソース

- 多要素認証を始める
- へのアクセスの保護 AWS の使用 MFA

すべての CloudTrail で を有効にする AWS リージョン

のすべてのアクティビティを追跡できます。 AWS を使用した リソース AWS CloudTrail。 ここでを有効にすることをお勧めします CloudTrail 。これは、 AWS Support と AWS ソリューションアーキテクトは、後でセキュリティまたは設定の問題をトラブルシューティングします。

すべての で CloudTrail ログインを有効にするには AWS リージョン、「」を参照してください。 AWS CloudTrail 更新 — すべてのリージョンで を有効にし、複数の証跡を使用します。

の詳細については CloudTrail、「 をオンにする CloudTrail: でAPIアクティビティを ログに記録する」を参照してください。 AWS アカウント。 が Nimble Studio をモニタリングする CloudTrail 方法については、「」を参照してください を使用した Nimble Studio 呼び出しの ログ記録 AWS CloudTrail。

Amazon GuardDuty および 通知を設定する

Amazon GuardDuty は、以下を分析して処理する継続的なセキュリティモニタリングサービスです。

- データソース
- Amazon VPC フローログ
- AWS CloudTrail 管理イベントログ
- CloudTrail S3 データイベントログ
- DNS ログ

Amazon GuardDuty は、 内の予期しないアクティビティ、潜在的に不正なアクティビティ、悪意のあるアクティビティを特定します。 AWS 環境。このアクティビティには、権限の工スカレートや、公開されている認証情報の使用、悪意のある IP アドレスまたはドメインでの通信も含まれます。これらのアクティビティを特定するために、 は悪意のある IP アドレスやドメインのリスト、機械学習などの脅威インテリジェンスフィード GuardDuty を使用します。例えば、マルウェアやマイニングビットコインを処理する侵害された Amazon EC2インスタンスを検出 GuardDuty できます。

GuardDuty また、 は をモニタリングします。 AWS アカウント 侵害の兆候に対する アクセス動作。これには、 にデプロイされたインスタンスなど、不正なインフラストラクチャのデプロイが含まれます。 AWS リージョン 一度も使用したことがない 。また、パスワードの強度を低下させるためのパスワードポリシーの変更など、異常なAPI呼び出しも含まれます。

GuardDuty は、 のステータスを通知します。 AWS セキュリティ検出結果 を生成するための 環境。これらの検出結果は、 GuardDuty コンソールまたは Amazon CloudWatch イベント を通じて表示できます。

Amazon SNSトピックとエンドポイントを設定する

「Amazon SNSトピックとエンドポイントのセットアップ」チュートリアルの手順に従います。

GuardDuty 検出結果の EventBridge イベントを設定する

が GuardDuty 生成 EventBridge するすべての検出結果のイベントを送信する のルールを作成します。

GuardDuty 検出結果の EventBridge イベントを作成するには

1. Amazon EventBridge コンソールにサインインします。 https://console.aws.amazon.com/events/
2. ナビゲーションペインで ルール] を選択します。次に、[Create rule (ルールを作成)] を選択します。
3. 新しいルールの [名前] と [説明] を入力します。次いで、[次へ] を選択します。

4. 退出 AWS イベントソース に選択された イベントまたは EventBridge パートナーイベント。
5. イベントパターン で、 を選択します。 AWS イベントソース の サービス。次にGuardDuty、AWS サービス、およびイベントタイプ GuardDuty の検出結果。これは「Amazon SNSトピックとエンドポイントを設定する」で作成したトピックです。
6. [Next (次へ)] を選択します。
7. ターゲット 1 で、 を選択します。 AWS サービス 。ターゲットの選択ドロップダウンでSNSトピックを選択します。次に、GuardDuty_to_Email トピックを選択します。
8. [追加設定] セクションでは、[ターゲット入力の設定] ドロップダウンを使用して [入力トランスフォーマー] を選択します。[入力トランスフォーマーを設定] を選択します。
9. [ターゲット入力トランスフォーマー] セクションの [入力パス] フィールドに、以下のコードを入力します。

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

10. E メールの形式を設定するには、[テンプレート] フィールドに以下のコードを入力します。

```
"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. [Create] (作成) を選択します。次いで、[次へ] を選択します。
12. (オプション) タグを使用して を追跡する場合は、タグを追加します。 AWS リソースの使用料金を見積もることができます。
13. [Next (次へ)] を選択します。
14. ルールを確認します。次に、[Create rule (ルールを作成)] を選択します。

これで、 AWS アカウント セキュリティでは、特定のユーザーにアクセス権を付与し、リソースが侵害されたときに通知を受け取ることができます。

でのデータ保護 Amazon Nimble Studio

- AWS 責任共有モデル 、 でのデータ保護に適用されます。Amazon Nimble Studio。 このモデルで説明されているように、 AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウド。 お客様は、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。 AWS のサービス 使用する 。データプライバシーの詳細については、「データプライバシーFAQ」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。 AWS の責任共有モデルとGDPRブログ記事 AWS セキュリティブログ 。

データ保護の目的で、 を保護することをお勧めします。 AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management （ IAM ）。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が必要で、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティの口グ記録を設定する AWS CloudTrail。 CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。 AWS アクティビティ、「」の「証 CloudTrail 跡の使用」を参照してください。 AWS CloudTrail ユーザーガイド 。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス.
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。利用可能なFIPSエンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、 を使用する場合も含まれます。Nimble Studio またはその他の AWS のサービス コンソール、API、 AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断口グに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

- AWS の責任共有モデルは、Amazon Nimble Studio でのデータ保護に適用されます。このモデルで説明されているように、 AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウド。 このインフラストラクチャでホストされているコンテンツの制御を維持するのはお客様の責任です。このコンテンツには、 のセキュリティ設定および管理タスクが含まれます。 AWS のサービス 使用する 。

データプライバシーの詳細については、「データプライバシーFAQ」を参照してください。欧州連合におけるデータ保護の詳細については、 GDPRセンターを参照してください。

保管中の暗号化

Nimble Studio は、 に保存されている暗号化キーを使用して保管時に暗号化することで、機密性の高いスタジオデータを保護します。 AWS Key Management Service (AWS KMS) 。 保管時の暗号化はすべての で使用できます。 AWS リージョン Nimble Studio が利用可能な 。暗号化するスタジオデータには、すべてのリソースタイプの名前と説明、スタジオコンポーネントのスクリプト、スクリプトパラメータ、マウントポイント、共有名、その他のデータが含まれます。

データを暗号化することで、ディスクに保存された機密データを、有効なキーを持たないユーザーやアプリケーションが読み取ることを防ぎます。暗号化されたデータは安全に保存され、マネージドキーへのアクセス権を認可された当事者のみによって、復号することができます。

Nimble Studio が を使用する方法の詳細については、「」を参照してください。 AWS KMS 保管中のデータの暗号化については、「」を参照してくださいAmazon Nimble Studio のキー管理。

での許可の使用 AWS KMS キー

許可は、 を許可するポリシーインストルメントです。 AWS 使用するプリンシパル AWS KMS 暗号化オペレーションの キー。また、コマンド を使用してKMSキーを表示しDescribeKey、権限を作成および管理することもできます。

グラントは によって一般的に使用されます AWS のサービス と統合する AWS KMS は、保管中のデータを暗号化します。サービスは、アカウント内のユーザーの代わりにグラントを作成し、そのアクセス許可を使用して、タスクが完了するとすぐにグラント廃止にします。

Nimble Studio がスタジオを作成する際、Nimble Studio ポータルユーザーに、ユーザーロールと管理者ロールの 2 つのロールを提供します。Nimble Studio は、これらのロールのカスタマーマネージドキーに対する権限を作成し、スタジオの暗号化されたデータへのアクセスを許可します。

> **Important**
>
> 権限を削除すると、管理者が新しい権限を作成するまでユーザーは Nimble Studio ポータルを使用できなくなります。

方法の詳細については、 AWS のサービス 許可の使用については、「方法」を参照してください。AWS のサービス use AWS KMS または、サービスのユーザーガイドまたはデベロッパーガイドの保管時の暗号化に関するトピック。

転送中の暗号化

次のテーブルに、転送中のデータの暗号化方法に関する情報を示します。該当する場合は、Nimble Studio の他のデータ保護方法も一覧表示されます。

[データ]	ネットワークパス	保護
イメージや JavaScript ファイルなどのウェブアセット	ネットワークパスは Nimble Studio ユーザーと Nimble Studio の間にあります。	データ暗号化は TLS 1.2 以降を使用します。
ピクセルおよび関連するストリーミングトラフィック	ネットワークパスは Nimble Studio ユーザーと Nimble Studio の間にあります。	256 ビット Advanced Encryption Standard (AES-256) を使用して暗号化され、1.2 TLS 以降を使用して転送されます。
API トラフィック	パスは Nimble Studio ユーザーと Nimble Studio の間にあります。	1.2 TLS 以降を使用して暗号化されます。接続を作成するリクエストは、SigV4 を使用して署名されます。

Amazon Nimble Studio のキー管理

新しいスタジオを作成する場合、以下のいずれかのキーを選択してスタジオデータを暗号化できます。

- AWS 所有KMSキー – デフォルトの暗号化タイプ。キーは Nimble Studio により所有されます (追加料金なし)。
- カスタマーマネージドKMSキー – キーはアカウントに保存され、ユーザーが作成、所有、管理します。ユーザーは、キーに関する完全なコントロール権を持ちます。 AWS KMS 料金が適用されます。

でのカスタマーマネージドKMSキーの削除 AWS Key Management Service (AWS KMS) は破壊的であり、潜在的に危険です。これにより、キーマテリアルとキーに関連付けられているすべてのメタデータが削除され、元に戻すことはできません。カスタマーマネージドKMSキーが削除されると、そのキーによって暗号化されたデータを復号できなくなります。これは、データが回復不能になることを意味します。

これが AWS KMS は、キーを削除する前に、最大 30 日間の待機期間をお客様に付与します。デフォルトの待機時間は、30 日です。

待機期間について

カスタマーマネージドKMSキーの削除は破壊的で潜在的に危険であるため、7 ~ 30 日間の待機期間を設定する必要があります。デフォルトの待機時間は、30 日です。

ただし、実際の待機期間は、スケジュールした待機期間よりも最大 24 時間長くなる場合があります。キーが削除される実際の日時を取得するには、 DescribeKeyオペレーションを使用します。また、 でキーの削除予定日を確認することもできます。 AWS KMS「 全般の設定」セクションのキーの詳細ページの コンソール。タイムゾーンに注意してください。

削除の待機期間中は、カスタマーマネージドキーのステータスおよびキーの状態が削除保留中になります。

- 削除保留中のカスタマーマネージドKMSキーは、暗号化オペレーション では使用できません。
- AWS KMS はカスタマー管理のバッキングキーをローテーションしない AWS KMS 削除保留中のキー。

カスタマー管理の削除の詳細については、 AWS KMS key「カスタマーマスターキーの削除」を参照してください。

データセキュリティ対策

データ保護の目的で、 を保護することをお勧めします。 AWS アカウント 認証情報と を使用して個々のアカウントをセットアップする AWS Identity and Access Management （ IAM ）。この方法に

より、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1.2 TLS 以降をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定する AWS CloudTrail.
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス.
- アクセス時に FIPS 140-2 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。使用可能なFIPSエンドポイントの詳細については、「連邦情報処理標準 (FIPS) 140-2」を参照してください。

顧客のアカウント番号などの機密の識別情報は、[Name] (名前) フィールドなどの自由形式のフィールドに入力しないことを強くお勧めします。これは、Amazon Nimble Studio またはその他の を使用する場合も同様です。 AWS のサービス コンソール、API、 AWS CLI、または AWS SDKs。Amazon Nimble Studio またはその他のサービスに入力したデータはいずれも、診断ログへ含めるために取得される可能性があります。URL を外部サーバーに提供する場合、そのサーバーへのリクエストを検証URLするために認証情報を に含めないでください。

診断データとメトリクス

のデプロイと削除中 StudioBuilder、Amazon Nimble Studio は、問題を診断し、Nimble Studio の機能やユーザーエクスペリエンスを向上させるために使用する特定のメトリクスを収集します。

収集されるメトリクスのタイプ

- 使用状況の情報 - 実行される汎用コマンドとサブコマンド。
- エラーと診断情報 - 終了コード、内部例外名、障害など、実行されるコマンドのステータスと継続時間です。
- システムおよび環境情報 — Python バージョン、オペレーティングシステム (Windows, Linux、または macOS) 、および StudioBuilder が実行される環境。

Amazon Nimble Studio 向けの Identity and Access Management

AWS Identity and Access Management （ IAM) は AWS のサービス 管理者は へのアクセスを安全に制御できます。 AWS リソースの使用料金を見積もることができます。管理者は、(サインインを) 認証された、および Amazon Nimble Studio リソースの使用を認可された (アクセス許可を持つ) ユーザーを制御します。IAM は AWS のサービス 追加料金なしで使用できます。

トピック

対象者

の使用方法 AWS Identity and Access Management （ IAM) は、Nimble Studio で行う作業によって異なります。

サービスユーザー — Nimble Studio サービスを使用してジョブを実行する場合は、サービスユーザーになります。この場合、割り当てられたリソースにアクセスするために必要な認証情報とアクセス許可を、管理者が用意します。作業を行うためにさらに多くの Nimble Studio の機能を使用する際は、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Nimble Studio の機能にアクセスできない場合は、「Amazon Nimble Studio のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Nimble Studio リソースを担当している場合は、通常、Nimble Studio へのフルアクセス許可が付与されます。従業員がアクセスする必要のある Nimble Studio の機能とリソースを決定することは、管理者のジョブです。その後、サービスユーザーのアクセス許可を変更するリクエストを管理者に送信します。このページの情報を確認して、 の基本概念を理解してください IAM。会社で Nimble Studio IAMを使用する方法の詳細については、「」を参照してくださいAmazon Nimble Studio と の連携方法 IAM。

アイデンティティを使用した認証

認証は、 にサインインする方法です。 AWS ID 認証情報を使用する。を使用したサインインの詳細については、「」を参照してください。 AWS Management Console、「 へのサインイン」を参照してください。 AWS Management Console ユーザーガイドの IAM ユーザーまたはルートユーザーIAMとして。

認証される必要があります (にサインインします AWSとしての) AWS アカウント ルートユーザー、 ユーザー、または IAMロールを引き受ける 。会社のシングルサインオン認証を使用することも、Google や Facebook のサインインを使用することもできます。このような場合、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。にアクセスする場合 AWS 別の会社の認証情報を使用して、間接的にロールを引き受けることになります。

に直接サインインするには AWS Management Console、ルートユーザーの E メールアドレスまたはユーザー名でパスワードを使用します。にアクセスできます AWS ルートユーザーまたはユーザーアクセスキーをプログラムで使用します。

AWS には、 認証情報を使用してリクエストに暗号で署名するための SDKおよび コマンドラインツールが用意されています。を使用しない場合 AWS ツールの場合は、リクエストに自分で署名します。これを行うには、署名バージョン 4 を使用します。これは、インバウンドAPIリクエストを認証するためのプロトコルです。リクエストの認証の詳細については、「」の「署名バージョン 4 の署名プロセス」を参照してください。 AWS 全般のリファレンス .

使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。例えば、などです AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「 での多要素認証 (MFA) の使用」を参照してください。 AWS IAMユーザーガイドの 。

AWS アカウント ルートユーザー

を初めて作成するとき AWS アカウントでは、すべての への完全なアクセス権を持つ単一のサインインアイデンティティから始めます。 AWS のサービス アカウントの および リソース。この ID はと呼ばれます。 AWS アカウント root ユーザー と には、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。ただし、日常的なタスクには、それが管理的なタスクであっても、ルートユーザーを使用しないことを強くお勧めします。代わりに、最初のユーザー の作成にのみルートIAMユーザーを使用するというベストプラクティスに従ってください。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

ユーザーとグループ

ユーザーは 内のアイデンティティです。 AWS アカウント 1 人のユーザーまたはアプリケーションに対して特定のアクセス許可を持つ 。ユーザーは、長期的な認証情報またはアクセスキーのセットを持つことができます。アクセスキーを生成する方法については、 ユーザーガイドのIAM「ユーザーのアクセスキーの管理」を参照してください。 IAMユーザーにアクセスキーを生成する際は、キーペアを表示して安全に保存してください。後で、シークレットアクセスキーを復元することはできません。新しいアクセスキーペアを生成します。

IAM グループは、ユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、 という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」の「 (ロールではなく) ユーザーを作成するタイミングIAM」を参照してください。

IAM ロール

IAM ロールは 内のアイデンティティです。 AWS アカウント 特定のアクセス許可を持つ 。これはユーザーに似ていますが、特定のユーザーには関連付けられていません。で一時的に IAMロールを引き受けることができます。 AWS Management Console ロールを切り替えます。を呼び出すことでロールを引き受けることができます。 AWS CLI または AWS API オペレーション、またはカスタムの使用URL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- 一時的なユーザーアクセス許可 – ユーザーは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- フェデレーティッドユーザーアクセス — ユーザーを作成する代わりに、 から既存の ID を使用できます。 AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブ ID プロバイダー。このようなユーザーはフェデレーションユーザーと呼ばれます。 AWS は、ID プロバイダー を介してアクセスがリクエストされたときに、フェデレーティッドユーザーにロールを割

り当てます。フェデレーティッドユーザーの詳細については、「 IAMユーザーガイド」の「フェデレーティッドユーザーとロール」を参照してください。

- メンバーシップ – Nimble Studio は「メンバーシップ」と呼ばれる概念を使用して、特定の起動プロファイルへのユーザーアクセスを許可します。メンバーシップを使用すると、スタジオ管理者はIAMポリシーを記述したり理解したりすることなく、リソースへのアクセスをユーザーに委任できます。Nimble Studio 管理者が起動プロファイルでユーザーのメンバーシップを作成すると、ユーザーは、そのプロパティの表示や、その起動プロファイルを使用したストリーミングセッションの開始など、起動プロファイルの使用に必要なIAMアクションを実行する権限が与えられます。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。サービスロールは、ご使用のアカウント内のみでアクセス権の付与を行います。他のアカウント内にあるサービスに、アクセス権を付与することはできません。管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 にアクセス許可を委任するロールの作成」を参照してください。 AWS のサービス IAM ユーザーガイドの 。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。 AWS のサービス。 このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。Nimble Studio は、サービスにリンクされたロールをサポートしていません。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 を作成しているアプリケーションの一時的な認証情報を管理できます。 AWS CLI または AWS API リクエスト。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。を割り当てるには AWS EC2 インスタンスにロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」を参照してください。

IAM ロールとユーザーのどちらを使用するかについては、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成するタイミングIAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスをコントロールする AWS ポリシーを作成して ID IAM または にアタッチする AWS リソースの使用料金を見積もることができます。ポリシーは のオブジェクトです。 AWS ID またはリ

ソースに関連付けられている場合、そのアクセス許可を定義します。ルートユーザーまたはユーザーとしてサインインすることも、 IAMロールを引き受けることもできます。その後、リクエストを行うと、 AWS は、関連するアイデンティティベースまたはリソースベースのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは に保存されます。 AWS JSON ドキュメントとして。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者は を使用できます AWS JSON ポリシー。誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

すべてのIAMエンティティ (ユーザーまたはロール) は、アクセス許可なしで始まります。言い換えると、デフォルト設定では、ユーザーは何もできず、自分のパスワードを変更することすらできません。何かを実行する許可をユーザーに付与するには、管理者がユーザーに許可ポリシーをアタッチする必要があります。また、管理者は、必要な許可があるグループにユーザーを追加できます。管理者がグループに許可を付与すると、そのグループ内のすべてのユーザーにこれらの許可が付与されます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 からロール情報を取得できます。 AWS Management Console、 AWS CLI、または AWS API.

アイデンティティベースのポリシー

ID ベースのポリシーは、ユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント。 管理ポリシーには以下が含まれます。 AWS 管理ポリシーとカスタマー管理ポリシー。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「 IAMユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定します。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービス.

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。は使用できません AWS リソースベースのポリシーIAMの からの マネージドポリシー。

Nimble Studio のアクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、 AWS WAF、、および Amazon VPCは、 をサポートする のサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (ユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる許可は、エンティティのアイデンティティベースポリシーとその許可の境界にある共通部分です。`Principal`フィールドでユーザーまたはロールを指定するリソースベースのポリシーは、許可の境界では制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」のIAM「エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、Organizations の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです。Organizations は、複数の をグループ化

して一元管理するためのサービスです。 AWS アカウント お客様のビジネスが所有する 。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します。 AWS アカウント ルートユーザー。Organizations と の詳細についてはSCPs、「」の「 のSCPs仕組み」を参照してください。 AWS Organizations ユーザーガイド。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として得られるセッションの許可は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分です。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。方法を学ぶには AWS は、複数のポリシータイプが関与する場合にリクエストを許可するかどうかを決定します。「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

Amazon Nimble Studio と の連携方法 IAM

IAM を使用して Nimble Studio へのアクセスを管理する前に、Nimble Studio で使用できるIAM機能を確認してください。

IAM Amazon Nimble Studio で使用できる の機能

IAM 機能	Nimble Studio Support
Nimble Studio のポリシーアクション	あり
Nimble Studio のポリシーリソース	はい
Nimble Studio のポリシー条件キー	はい
Nimble Studio のアクセスコントロールリスト (ACLs)	いいえ
Nimble Studio での属性ベースのアクセスコントロール (ABAC)	はい

IAM 機能	Nimble Studio Support
Nimble Studio での一時的な認証情報の使用	はい
Nimble Studio のクロスサービスプリンシパル許可	はい
Nimble Studio のサービスロール	はい
Nimble Studio のサービスにリンクされたロール	なし

Nimble Studio とその他の の概要を把握するには AWS のサービス ほとんどのIAM機能を操作するには、「」を参照してください。 AWS のサービス ユーザーガイドIAMの で動作する IAM 。

Nimble Studio のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	あり

ID ベースのポリシーは、ユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件を制御します。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルはアタッチされているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」を参照してください。

Amazon Nimble Studio のアイデンティティベースのポリシー例

Nimble Studio でのアイデンティティベースのポリシーの例については、「Amazon Nimble Studio のアイデンティティベースのポリシー例」を参照してください。

Nimble Studio 内のリソースベースのポリシー

リソースベースのポリシーのサポート	なし

Nimble Studio では、リソースベースのポリシーとクロスアカウントでのアクセスはサポートされません。リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定します。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービス.

Nimble Studio のポリシーアクション

ポリシーアクションのサポート	あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションは通常、関連付けられている と同じ名前です。 AWS API オペレーション。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Nimble Studio アクションのリストは、「サービス認証リファレンス」の「Amazon Nimble Studio のアクション、リソース、条件キー」を参照してください。

Nimble Studio のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

```
nimble
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

Nimble Studio でのアイデンティティベースのポリシーの例については、「Amazon Nimble Studio のアイデンティティベースのポリシー例」を参照してください。

Nimble Studio のポリシーリソース

ポリシーリソースに対するサポート	あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを表示するワイルドカード (*) を使用します。

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

Nimble Studio でのアイデンティティベースのポリシーの例については、「Amazon Nimble Studio のアイデンティティベースのポリシー例」を参照してください。

Nimble Studio のポリシー条件キー

ポリシー条件キーに対するサポート	あり

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition block) を使用すると、ステートメントが有効になる条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

ステートメントで複数のCondition要素を指定するか、単一のCondition要素で複数のキーを指定する場合は、 AWS は論理ANDオペレーションを使用してそれらを評価します。1 つの条件キーに複数の値を指定する場合は、 AWS は論理ORオペレーションを使用して条件を評価します。ステートメントのアクセス許可が付与される前に、すべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、ユーザー名でタグ付けされている場合のみ、リソースにアクセスするユーザーアクセス許可を付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべてを表示するには AWS グローバル条件キー、「」を参照してください。 AWSIAM ユーザーガイドの グローバル条件コンテキストキー。

Nimble Studio でのアイデンティティベースのポリシーの例については、「Amazon Nimble Studio のアイデンティティベースのポリシー例」を参照してください。

Nimble Studio のアクセスコントロールリスト (ACLs)

サポート ACLs	なし

Nimble Studio はアクセスコントロールリスト () をサポートしていませんACLs。ACLs は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Nimble Studio での属性ベースのアクセスコントロール (ABAC)

サポート ABAC (ポリシー内のタグ)	あり

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。In AWSでは、これらの属性はタグ と呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くの にタグをアタッチできます。 AWS リソースの使用料金を見積もることができます。エンティティとリソースのタグ付けは、 の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの 条件要素でタグ情報を提供します。

の詳細についてはABAC、 ユーザーガイドの「 とはABACIAM」を参照してください。の設定手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

Nimble Studio での一時的な認証情報の使用

一時的な認証情報のサポート	あり

ある程度 AWS のサービス 一時的な認証情報を使用してサインインすると、 は機能しません。以下を含む追加情報 AWS のサービス 一時的な認証情報の使用については、「」を参照してください。AWS のサービス ユーザーガイドの IAMで動作する IAM 。

にサインインする場合、一時的な認証情報を使用している AWS Management Console ユーザー名とパスワード以外の方法を使用する。例えば、 にアクセスする場合 AWS 会社のシングルサインオン (SSO) リンクを使用すると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

を使用して、一時的な認証情報を手動で作成できます。 AWS CLI または AWS API。その後、これらの一時的な認証情報を使用して にアクセスできます。 AWS. AWS では、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

Nimble Studio のクロスサービスプリンシパル許可

プリンシパル権限のサポート	あり

Nimble Studio のサービスロール

サービスロールのサポート	あり

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。サービスロールは、ご使用のアカウント内のみでアクセス権の付与を行います。他のアカウント内にあるサービスに、アクセス権を付与することはできません。管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 にアクセス許可を委任するロールの作成」を参照してください。 AWS のサービス IAMユーザーガイドの 。

> **Warning**
>
> サービスロールの許可を変更すると、Nimble Studio の機能が破損する可能性があります。Nimble Studio が指示した場合にのみ、サービスロールを編集してください。

Nimble Studio のサービスにリンクされたロール

サービスにリンクされたロールのサポート	なし

Nimble Studio は、サービスにリンクされたロールをサポートしていません。サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。 AWS のサービス。 このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールはIAMアカウントに表示され、サービスによって所有されます。 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「」を参照してください。 AWS のサービス で動作する IAM。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

Amazon Nimble Studio のアイデンティティベースのポリシー例

デフォルトでは、ユーザーおよびロールには、Nimble Studio リソースを作成または変更するアクセス許可はありません。また、 を使用してタスクを実行することはできません。 AWS Management

Console, AWS CLI、または AWS API。管理者は、必要なリソースに対してアクションを実行するアクセス許可をユーザーとロールに付与するIAMポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のJSON「 タブでのポリシーの作成IAM」を参照してください。

トピック

- ポリシーのベストプラクティス

ポリシーのベストプラクティス

アイデンティティベースのポリシーは非常に強力です。アカウント内でユーザーが Nimble Studio リソースを作成、アクセス、削除できるかどうかを決定します。これらのアクションでは、 のコストが発生する可能性があります。 AWS アカウント。 アイデンティティベースのポリシーを作成または編集するときは、以下のガイドラインと推奨事項に従ってください。

- の使用を開始する AWS マネージドポリシー – Nimble Studio の使用をすばやく開始するには、 を使用します。 AWS 従業員が必要とするアクセス許可を付与するための マネージドポリシー。これらのポリシーはアカウントで既に利用可能であり、 によって管理および更新されます。 AWS。詳細については、「 でアクセス許可の使用を開始する」を参照してください。 AWS IAM ユーザーガイドの マネージドポリシー。
- 最小特権を付与する - カスタムポリシーを作成するときは、タスクの実行に必要な許可のみを付与します。最小限の許可からスタートし、必要に応じて追加の許可を付与します。この方法は、寛容過ぎる許可から始めて、後から厳しくしようとするよりも安全です。詳細については、「 ユーザーガイド」の「最小特権を付与するIAM」を参照してください。
- 機密性の高いオペレーションMFAを有効にする – セキュリティを強化するには、機密性の高いリソースまたはAPIオペレーションにアクセスするために多要素認証 (MFA) の使用をユーザーに要求します。詳細については、「 での多要素認証 (MFA) の使用」を参照してください。 AWS IAM ユーザーガイドの 。
- 追加のセキュリティとしてポリシー条件を使用する – 実行可能な範囲内で、アイデンティティベースのポリシーでリソースへのアクセスを許可する条件を定義します。例えば、あるリクエストの送信が許可される IP アドレスの範囲を指定するための条件を記述できます。また、指定した日付または時間範囲内のリクエストのみを許可する条件を記述したり、 SSL または の使用を要求したりすることもできますMFA。詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」を参照してください。

AWS Amazon Nimble Studio の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、 を使用する方が簡単です。 AWS 自分でポリシーを記述するよりも マネージドポリシー。必要なアクセス許可のみをチームに提供するIAMカスタマー管理ポリシーを作成するには、時間と専門知識が必要です。すぐに使用を開始するには、 AWS マネージドポリシー。これらのポリシーは一般的なユースケースを対象としており、で利用できます。 AWS アカウント。 の詳細については、「」を参照してください。 AWS 管理ポリシー、「」を参照してください。 AWSIAM ユーザーガイドの マネージドポリシー。

AWS サービスによるメンテナンスと更新 AWS マネージドポリシー。のアクセス許可は変更できません AWS マネージドポリシー。サービスが にアクセス許可を追加することがある AWS 新機能をサポートする マネージドポリシー。この種の更新は、ポリシーがアタッチされているすべてのアイデンティティ (ユーザー、グループ、ロール) に影響を与えます。サービスは を更新する可能性が最も高い AWS 新しい機能が起動されたとき、または新しいオペレーションが利用可能になったときのマネージドポリシー。サービスは からアクセス許可を削除しません AWS マネージドポリシー。ポリシーの更新によって既存のアクセス許可が損なわれることはありません。

さらに、 AWS は、複数の サービスにまたがる職務機能の マネージドポリシーをサポートします。例えば、 ReadOnlyAccess AWS 管理ポリシーは、すべての への読み取り専用アクセスを提供します。 AWS サービスとリソース。サービスが新機能を起動すると、 AWS は、新しいオペレーションとリソースの読み取り専用アクセス許可を追加します。職務機能ポリシーのリストと説明については、「」を参照してください。 AWS ユーザーガイドの ジョブ機能の IAM マネージドポリシー。

エンドユーザーは主に Nimble Studio ポータルを使用して、Amazon Nimble Studio にアクセスします。 StudioBuilder または Nimble Studio コンソールを使用してスタジオを作成すると、スタジオ管理者とスタジオユーザーという 1 つのIAMロールがスタジオペルソナごとに作成されます。各 には、それぞれのIAM管理ポリシーがアタッチされています。Nimble Studio ポータルからユーザーに提供されるエクスペリエンスでは、アクセス許可を持つリソースのみを一覧表示して使用することができます。

Nimble Studio ポータルのエクスペリエンスでは、ユーザーはアクセス権を付与されたリソースのみを一覧表示し使用できます。また、このポータルは、適切な動作を行うために関係するポリシーの内容に依存します。Nimble Studio のエンドユーザーは、ポータルを使用してクラウドスタジオにアクセスします。したがって、管理者が を使用してスタジオを作成すると StudioBuilder、スタジオにアクセスする必要があるユーザーごとに 1 つのIAMロールが作成されます。これには、スタジオ管理者とスタジオユーザーが含まれ、それぞれにそれぞれのIAM管理ポリシーがアタッチされています。

職務機能ポリシーのリストと説明については、「」を参照してください。 AWS IAM ユーザーガイドの ジョブ機能の マネージドポリシー。

AWS マネージドポリシー: **AmazonNimbleStudio-LaunchProfileWorker**

IAM ID にAmazonNimbleStudio-LaunchProfileWorkerポリシーをアタッチできます。

このポリシーを Nimble Studio Builder によって作成されたEC2インスタンスにアタッチして、Nimble Studio 起動プロファイルワーカーが必要とするリソースへのアクセスを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ds - LaunchProfile ワーカーが に関する接続情報を検出できるようにします AWS Managed Microsoft AD に関連付けられた LaunchProfile。
- ec2 - LaunchProfile ワーカーが に接続するためのセキュリティグループとサブネット情報を検出できるようにします LaunchProfile。
- fsx - LaunchProfile ワーカーが に関連付けられた Amazon FSxボリュームへの接続情報を検出できるようにします LaunchProfile。

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

AWS マネージドポリシー: **AmazonNimbleStudio-StudioAdmin**

IAM ID にAmazonNimbleStudio-StudioAdminポリシーをアタッチできます。

このポリシーを、スタジオに関連付けられた管理者ロールにアタッチして、スタジオ管理者に関連付けられた Amazon Nimble Studio リソースおよびその他のサービスの関連するスタジオリソースへのアクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- nimble - Studio ユーザーが によって委任された Nimble リソースにアクセスできるようにします StudioAdmins。
- sso - スタジオユーザーに、スタジオ内の他のユーザー名の表示を許可します。
- identitystore - スタジオユーザーに、スタジオ内の他のユーザー名の表示を許可します。
- ds - Nimble Studio が仮想ワークステーションを に追加できるようにします AWS Managed Microsoft AD スタジオに関連付けられた 。
- ec2 - Nimble Studio が仮想ワークステーションを設定済みの にアタッチできるようにします VPC。
- fsx - Nimble Studio が仮想ワークステーションを設定済みの Amazon FSxボリュームに接続できるようにします。
- cloudwatch - Nimble Studio が CloudWatch メトリクスを取得できるようにします。

```
{
  "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 マネージドポリシー: **AmazonNimbleStudio-StudioUser**

IAM ID に[AmazonNimbleStudio-StudioUser](#)ポリシーをアタッチできます。

このポリシーをスタジオに関連付けられたユーザーロールにアタッチして、スタジオユーザーに関連付けられた Amazon Nimble Studio リソースおよびその他のサービスの関連するスタジオリソースへのアクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- nimble - Studio ユーザーが によって委任された Nimble リソースにアクセスできるようにします StudioAdmins。
- sso - スタジオユーザーに、スタジオ内の他のユーザー名の表示を許可します。

- identitystore - スタジオユーザーに、スタジオ内の他のユーザー名の表示を許可します。
- ds - Nimble Studio が仮想ワークステーションを に追加できるようにします AWS Managed Microsoft AD スタジオに関連付けられた 。
- ec2 - Nimble Studio が仮想ワークステーションを設定済みの にアタッチできるようにします VPC。
- fsx - Nimble Studio が仮想ワークステーションを設定済みの Amazon FSxボリュームに接続できるようにします。

```
{
  "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 の への更新 AWS 管理ポリシー

の更新に関する詳細を表示する AWS Amazon Nimble Studio の マネージドポリシーは、このサービスがこれらの変更の追跡を開始してからです。

変更	説明	日付
AWS マネージドポリシー: AmazonNimbleStudio-StudioUser – Updated policy	Amazon Nimble Studio は、ID Store サービスの最新バージョンを使用するようにポリシーを更新しました。	2023 年 9 月 22 日
AWS マネージドポリシー: AmazonNimbleStudio-StudioAdmin – Updated policy	Amazon Nimble Studio は、ID Store サービスの最新バージョンを使用するようにポリシーを更新しました。	2023 年 9 月 22 日
AWS マネージドポリシー: AmazonNimbleStudio-StudioUser – Updated policy	Amazon Nimble Studio は、スタジオユーザーがワークステーションのバックアップを表示できるようにポリシーを更新しました。	2022 年 12 月 20 日
AWS マネージドポリシー: AmazonNimbleStudio-StudioAdmin – Updated policy	Amazon Nimble Studio は、スタジオ管理者がワークステーションのバックアップを表示できるようにポリシーを更新しました。	2022 年 12 月 20 日
AWS マネージドポリシー: AmazonNimbleStudio	Amazon Nimble Studio は、スタジオ管理者がメトリクスを	2021 年 11 月 11 日

変更	説明	日付
-StudioUser – Updated policy	取得 CloudWatchできるようにポリシーを更新しました。	
AWS マネージドポリシー: AmazonNimbleStudio -StudioUser – Updated policy	Amazon Nimble Studio は、スタジオユーザーがワークステーションを起動および停止できるようにポリシーを更新しました。	2021 年 11 月 1 日
AWS マネージドポリシー: AmazonNimbleStudio-StudioAdmin – Updated policy	Amazon Nimble Studio は、スタジオ管理者がワークステーションを起動および停止できるようにポリシーを更新しました。	2021 年 11 月 1 日
AWS マネージドポリシー: AmazonNimbleStudio -StudioUser – Updated policy	Amazon Nimble Studio は、`nimble:createdBy` の代わりに `nimble:ownedBy` に基づいて、ストリーミングセッションリソースへのアクセスを条件付きで許可するようにポリシーを更新しました。	2021 年 8 月 16 日
AWS マネージドポリシー: AmazonNimbleStudio-StudioUser - 新しいポリシー	Amazon Nimble Studio は、スタジオユーザーに関連付けられたリソースと、他のサービスの関連するスタジオリソースへのアクセスを許可する新しいポリシーを追加しました。	2021 年 4 月 28 日

変更	説明	日付
AWS マネージドポリシー: AmazonNimbleStudio-StudioAdmin – 新しいポリシー	Amazon Nimble Studio は、他のサービスのスタジオ管理者に関連付けられたリソースと、他のリソースの関連付けられたリソースへのアクセスを許可する新しいポリシーを追加しました。	2021 年 4 月 28 日
AWS マネージドポリシー: AmazonNimbleStudio-LaunchProfileWorker - 新しいポリシー	Amazon Nimble Studio は、Nimble Studio 起動プロファイルワーカーが必要とするリソースへのアクセスを許可する新しいポリシーを追加しました。	2021 年 4 月 28 日
Amazon Nimble Studio が変更の追跡を開始	Amazon Nimble Studio が の変更の追跡を開始しました AWS マネージドポリシー。	2021 年 4 月 28 日

サービス間の混乱した代理の防止

混乱した代理問題とは、あるアクションを実行する許可を持たないエンティティが、より多くの特権を持つエンティティにアクションの実行を強制できることで生じるセキュリティ上の問題です。In AWS、サービス間のなりすましは、混乱した代理問題を引き起こす可能性があります。サービス間でのなりすましは、あるサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスが操作され、それ自体のアクセス許可を通じて、別の顧客のリソースに対して本来アクセス許可が付与されるべきではない形で働きかけが行われることがあります。これを防ぐには、 AWS は、アカウント内のリソースへのアクセスが許可されているサービスプリンシパルを使用して、すべてのサービスのデータを保護するのに役立つツールを提供します。

Identity `aws:SourceArn` and Access Management (IAM) が Amazon Nimble Studio にリソースへのアクセスを許可するアクセス許可を制限するには、リソースポリシーで および `aws:SourceAccount` グローバル条件コンテキストキーを使用することをお勧めします。両方のグローバル条件コンテキストキーを同じポリシーステートメントで使用する場

合、aws:SourceAccount 値、および aws:SourceArn 値の中のアカウントで、同じアカウント ID を使用する必要があります。

の値はaws:SourceArnスタジオの ARNで、 アカウント ID aws:SourceAccountである必要があります。スタジオは Nimble Studio によって生成されるため、スタジオが作成されるまでは、スタジオ ID が何であるかを知ることはできません。スタジオを作成したら、最終的なスタジオ ID を aws:SourceArn として設定し、信頼ポリシーを更新できます。

混乱した代理問題から保護する最も効果的な方法は、リソースARNがいっぱいになった aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースARNの全体がわからない場合、または複数のリソースを指定する場合は、 の不明な部分にワイルドカード (*) が付いたaws:SourceArnグローバルコンテキスト条件キーを使用しますARN。例えば、arn:aws:nimble::123456789012:* と指定します。

エンドユーザーは、Nimble Studio ポータルへのサインイン時にスタジオのロールを引き受けます。スタジオを作成すると、 AWS はロールを設定し、ポリシーを評価します。 AWS は、ユーザーが Nimble Studio ポータルにログインするたびにポリシーを評価します。スタジオ作成時に aws:SourceArn を変更することはできません。スタジオの作成が完了したら、 studioArn に を使用できますaws:SourceArn。

次のロールポリシー引き受けの例は、aws:SourceArn および aws:SourceAccount のグローバル条件コンテキストキーを Nimble Studio で使用して、混乱した代理問題を防止する方法を示しています。

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

Amazon Nimble Studio のアイデンティティとアクセスのトラブルシューティング

以下の情報は、Nimble Studio と の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

トピック

- Nimble Studio でアクションを実行する権限がない。
- iam を実行する権限がありませんPassRole。
- アクセスキーを表示する場合
- 管理者として Nimble Studio へのアクセスを他のユーザーに許可したい。
- 自分の 以外のユーザーに許可したい AWS アカウント Nimble Studio リソースにアクセスする場合。

Nimble Studio でアクションを実行する権限がない。

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のnimble:*GetWidget*アクセス許可がない場合に発生します。

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

この場合、nimble:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 にお問い合わせください。 AWS 管理者。サインイン認証情報を提供した担当者が管理者です。

iam を実行する権限がありませんPassRole。

[iam:PassRole] アクションを実行する権限がないというエラーが表示された場合は、管理者に問い合わせてサポートを依頼してください。ポリシーを更新して、Nimble Studio にロールを渡すことができるように管理者に依頼します。

ある程度 AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す許可が必要です。

以下は、johndoe という名前のユーザーがコンソールを使用して、Nimble Studio でアクションを実行した場合に発生したエラーの例です。ただし、アクションには、サービスロールによってサービスに許可が付与されている必要があります。John には、ロールをサービスに渡すアクセス許可がありません。

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

この場合 John は、ポリシーを更新して iam:PassRole アクションを実行するための許可を付与するように、管理者に依頼します。

アクセスキーを表示する場合

Amazon Nimble Studio では、アクセスキーを提供しません。シークレットアクセスキーの詳細については、「 ユーザーガイド」の「アクセスキーの管理IAM」を参照してください。

> **Important**
>
> 正規ユーザー ID を確認するためであっても、ご自身のアクセスキーはサードパーティーに提供しないでください。提供すると、第三者がアカウントへの永続的なアクセスを取得する場合があります。

アクセスキーペアを作成する際は、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合、新しいアクセスキーをユーザーに追加します。アクセスキーは最大 2 つまで持つことができます。既に 2 つある場合は、新しいキーペアを作成する前に、いずれかを削除します。手順を確認するには、「 ユーザーガイド」の「アクセスキーの管理IAM」を参照してください。

管理者として Nimble Studio へのアクセスを他のユーザーに許可したい。

Nimble Studio へのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションのIAMエンティティ (ユーザーまたはロール) を作成します。そのエンティティの認証情報を使用して にアクセスします。 AWS。 次に、適切なアクセス許可を付与するポリシーをエンティティにアタッチします。

Nimble Studio は、 の `AmazonNimbleStudio-StudioUser`を提供します。 AWS Management Console。 コンソールを管理する IT 管理者は、このポリシーを使用して、他のユーザーにスタジオへのアクセスを許可します。

管理者ポリシーの使用に関するチュートリアルについては、「Nimble Studio のセットアップ ガイド」を参照してください。ユーザーポリシーや起動プロファイルポリシーなど、既存のポリシーをユーザーにアタッチする方法については、IAM「ユーザーの作成 (コンソール) 」を参照してください。

ポリシーのインポートの詳細については、「 IAMユーザーガイド」の「最初のIAM委任されたユーザーとグループの作成」を参照してください。

自分の 以外のユーザーに許可したい AWS アカウント Nimble Studio リソースにアクセスする場合。

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- Nimble Studio がこれらの機能をサポートしているかどうかを確認するには、「Amazon Nimble Studio と の連携方法 IAM」を参照してください。
- 全体で リソースへのアクセスを提供する方法を学ぶには AWS アカウント 所有している 。「別のIAMユーザーにアクセス権を付与する」を参照してください。 AWS アカウント ユーザーガイドで所有している IAM 。
- リソースへのアクセスをサードパーティーに提供する方法を学ぶには AWS アカウント、「 へのアクセスの提供」を参照してください。 AWS アカウント IAM ユーザーガイドのサードパーティーが所有しています。
- ID フェデレーションを通じてアクセスを提供する方法については、 IAMユーザーガイドの「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) 」を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、「 IAMユーザーガイド」のIAM「ロールとリソースベースのポリシーの違い」を参照してください。

Nimble Studio によるセキュリティイベントのロギングとモニタリング

モニタリングは、Amazon Nimble Studio と の信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS ソリューション。のすべての部分からモニタリングデータを収集する AWS マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできる ソリューション。

AWS と Nimble Studio には、 リソースをモニタリングし、 や などの潜在的なインシデントに対応するためのツールを使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrailが用意されています。 AWS CloudFormation ユーザーガイド 。

Amazon Nimble Studio と の連携方法の詳細については、「」を参照してください。 AWS CloudFormationおよび JSON YAML テンプレートの例を含む については、「」の「Amazon Nimble Studio リソースとプロパティのリファレンス」を参照してください。 AWS CloudFormation ユーザーガイド。テンプレートの使用方法 CloudFormationについては、「」を参照してください。 AWS CloudFormation の概念。

トピック

- を使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrail

を使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrail

Amazon Nimble Studio は と統合されています AWS CloudTrail、ユーザー、ロール、または によって実行されたアクションを記録するサービス AWS のサービス Nimble Studio. の は、Nimble Studio のすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされるコールには、Nimble Studio コンソールからのコールと、Amazon Nimble Studio オペレーションへのコードコールが含まれます。

証跡を作成する場合は、Nimble Studio の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。で収集された情報を使用して CloudTrail、Nimble Studio に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の Nimble Studio 情報 CloudTrail

CloudTrail が で有効になっている AWS アカウント アカウントを作成するとき。Nimble Studio でアクティビティが発生すると、そのアクティビティは他の とともに CloudTrail イベントに記録されます。 AWS のサービス イベント履歴 の イベント。で最近のイベントを表示、検索、ダウンロードできます。 AWS アカウント。 詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

のイベントを継続的に記録するには AWS アカウント Nimble Studio のイベントを含む は、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての に適用されます。 AWS リージョン。 証跡は、 内のすべてのリージョンからのイベントをログに記録します。 AWS パーティション 分割し、指定した Amazon S3 バケットにログファイルを配信します。さらに、他の AWS のサービス CloudTrail ログで収集されたイベントデータをさらに分析し、それに基づく対応を行います。

詳細については、次を参照してください:

追跡を作成するための概要

CloudTrail がサポートするサービスと統合

の Amazon SNS通知の設定 CloudTrail

複数のリージョンからの CloudTrail ログファイルの受信

複数のアカウントからの CloudTrail ログファイルの受信

Nimble Studio アクションは によってログに記録 CloudTrail され、Amazon Nimble Studio APIリファレンス に記載されています。例えば、、、および DeleteStudio アクションを呼び出す GetStudio と CreateStudio、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが root または で行われたかどうか AWS Identity and Access Management （ IAM) ユーザー認証情報。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の サービスによって行われたかどうか。

詳細については、CloudTrail 「ユーザー ID 要素」を参照してください。

Nimble Studio ログファイルエントリの概要

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。 CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

このJSON例は、次の 3 つのアクションを示しています。

- ACTION_1: CreateStudio
- ACTION_2: GetStudio
- ACTION_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"
}
```


この例では、イベントにリージョン、IP アドレス、およびイベントの特定に役立つ「」や requestParameters「」などのその他の「」が表示されuserRoleArnadminRoleArnていることに気付くでしょう。creationDate「」の日時と、「」としてマークされたリクエストの発信元のソースを確認できますeventSource。nimble.amazonaws.com」。

CloudTrail が で有効になっている AWS アカウント アカウントを作成するとき。アクティビティが IAMまたは で発生した場合 AWS STS、そのアクティビティは他の とともに CloudTrail イベントに

記録されます。 AWS のサービス イベント履歴の イベント。で最近のイベントを表示、検索、ダウンロードできます。 AWS アカウント.

AWS CloudTrail は、 IAMと のすべてのAPI呼び出しをキャプチャします。 AWS Security Token Service (AWS STS) コンソールからの呼び出しや API 呼び出しを含む、イベントとしての 。と CloudTrail での の使用の詳細については、IAM「」を参照してください。 AWS STS、「ログ記録 IAM」および「」を参照してください。 AWS STS API を使用した 呼び出し AWS CloudTrail.

の詳細については、 CloudTrail「」を参照してください。 AWS CloudTrail ユーザーガイド 。

Amazon が提供する他のモニタリングサービスの詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

Amazon Nimble Studio のコンプライアンス検証

Amazon Nimble Studio は責任共有モデル に従い、コンプライアンスは 間で共有されます。 AWS と当社のお客様。

が AWS のサービス は特定のコンプライアンスプログラムの範囲内にあります。「」を参照してください。 AWS のサービス コンプライアンスプログラムによる対象範囲内による対象範囲内で、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、「」を参照してください。 AWS コンプライアンスプログラム。

サードパーティーの監査レポートは、 を使用してダウンロードできます。 AWS Artifact。 詳細については、「 でのレポートのダウンロード」を参照してください。 AWS Artifact.

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、データの機密性、企業のコンプライアンス目的、適用可能な法律および規制によって決まります。 AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、 にベースライン環境をデプロイする手順について説明します。 AWS セキュリティとコンプライアンスに重点を置いた 。
- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が を使用する方法について説明します。 AWS は、HIPAA対象アプリケーションを作成します。

> **Note**
>
> すべてではない AWS のサービス がHIPAA対象です。詳細については、HIPAA「対象サービスリファレンス」を参照してください。

- AWS コンプライアンスリソース — このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、 を保護するためのベストプラクティスをまとめています。 AWS のサービス と は、ガイダンスを複数のフレームワーク (米国国立標準技術研究所 (NIST) 、Payment Card Industry Security Standards Council (PCI) 、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングします。
- のルールによるリソースの評価 AWS Config デベロッパーガイド – AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub – これは AWS のサービス は、 内のセキュリティ状態を包括的に表示します。 AWS。 Security Hub は、セキュリティコントロールを使用して を評価します。 AWS リソースとを使用して、セキュリティ業界標準とベストプラクティスに照らしてコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これは AWS のサービス が に対する潜在的な脅威を検出する AWS アカウント、ワークロード、コンテナ、およびデータをモニタリングして、疑わしいアクティビティや悪意のあるアクティビティがないかを確認します。 PCI GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことでDSS、 などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- AWS Audit Manager – これは AWS のサービス は、 の継続的な監査に役立ちます。 AWS を使用して、リスクの管理方法と規制や業界標準への準拠を簡素化します。

Amazon Nimble Studio でのインフラストラクチャセキュリティ

マネージドサービスである Amazon Nimble Studio は によって保護されています。 AWS グローバルネットワークセキュリティ。参考情報 AWS セキュリティサービスとその方法 AWS インフラストラクチャを保護するには、「」を参照してください。 AWS クラウドセキュリティ 。を設計するには AWS インフラストラクチャセキュリティのベストプラクティスを使用する 環境、「セキュリティの

柱」の「インフラストラクチャの保護」を参照してください。 AWS Well-Architected フレームワーク 。

を使用する AWS は、ネットワーク経由で Nimble Studio にアクセスするためのAPI呼び出しを発行しました。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS) 。1TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。または、 AWS Security Token Service (AWS STS) リクエストに署名するための一時的なセキュリティ認証情報を生成します。

Nimble Studio のセキュリティのベストプラクティス

Amazon Nimble Studio には、独自のセキュリティポリシーを策定および実装する際に検討するべき、さまざまなセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

モニタリング

モニタリングは、Nimble Studio と の信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS ソリューション。イベントのモニタリングと応答の詳細については、「Nimble Studio によるセキュリティイベントのロギングとモニタリング」を参照してください。

データ保護

データ保護の目的で、 を保護することをお勧めします。 AWS アカウント 認証情報と を使用して個々のアカウントをセットアップする AWS Identity and Access Management （ IAM ）。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。

- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1.2 TLS 以降をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定する AWS CloudTrail.
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス.
- Amazon Macie などのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3 に保存されている個人データの検出と保護を支援します。
- アクセス時に FIPS 140-2 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。利用可能なFIPSエンドポイントの詳細については、「連邦情報処理標準 (FIPS) 140-2」を参照してください。

顧客のアカウント番号などの機密の識別情報は、[名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、Amazon Nimble Studio またはその他の を使用する場合も同様です。 AWS のサービス コンソール、API、 AWS CLI、または AWS SDKs。Amazon Nimble Studio またはその他のサービスに入力したデータはいずれも、診断ログへ含めるために取得される可能性があります。URL を外部サーバーに提供する場合、そのサーバーへのリクエストを検証URLするために認証情報を に含めないでください。

アクセス許可

へのアクセスを管理する AWS ユーザー、IAMロールを使用する リソース、およびユーザーに最小特権を付与する リソース。認証情報管理ポリシーと、作成、配布、ローテーション、取り消しの手順を確立する AWS アクセス認証情報。詳細については、「 ユーザーガイド」のIAM「ベストプラクティスIAM」を参照してください。

Nimble Studio のサポート

このセクションでは、サービスや関連アプリケーションをデプロイまたは使用する際にサポートを受ける方法など、Nimble Studio のさまざまなサポートオプションについて説明します。

目次

Nimble Studio フォーラム

Nimble Studio について質問がある場合は、Nimble Studio フォーラムにアクセスしてください。フォーラムでは、Nimble Studio の機能、技術的な問題、トラブルシューティングに関するヘルプについて、コミュニティや AWS フォーラムのモデレーターから回答を得ることができます。

アプリケーションのサポート

Nimble Studio では、以下のアプリケーションに関する追加ドキュメントを用意しています。

AWSThinkboxDeadline

レンダーファームのヘルプや Deadline の仕組みについては、AWSThinkboxDeadline のドキュメントを参照してください。

Nimble Studio File Transfer

File Transfer の仕組みについては、「Nimble Studio File Transfer ユーザーガイド」を参照してください。

AWS Support センター

AWS Support Center は、サポートケースを作成して管理するためのハブです。請求と技術ソリューション、ナレッジセンター、ナレッジセンターのビデオ、AWS のドキュメント、トレーニングと認定など、さまざまなリソースにアクセスできます。

AWS Support プラン

AWS Support プランは、パフォーマンスの最適化、セキュリティの維持、ダウンタイムの回避、コストの管理に役立ちます。AWS Support プランの詳細については、「AWS Support のプラン比較」を参照してください。

AWS のお客様サポートの詳細については、「お問い合わせ」ページを参照してください。

ドキュメント履歴

- API バージョン: 最新
- ドキュメント最終更新日: 2023 年 9 月 22 日

次の表に、「Nimble Studio 管理者ガイド」のリリース別の重要な変更点を示します。

変更	説明	
新しいサービスとガイド	これは Amazon Nimble Studio と「Amazon Nimble Studio 管理者ガイド」の初版リリースです。	2023 年 6 月 19 日
AWSマネージドポリシーの更新	`AmazonNimbleStudio-StudioUser` および `AmazonNimbleStudio-StudioAdmin` ポリシーを、AWS IAM Identity Center サービスの最新バージョンを使用するように更新しました。	2023 年 9 月 22 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。