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。

目次

IAM のセットアップ

開始する前に、次の AWS Identity and Access Management (IAM) のドキュメントを確認してください。

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

AWS アカウントへのサインアップ

AWS アカウントがない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

1. https://portal.aws.amazon.com/billing/signup 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、電話のキーパッドを使用して検証コードを入力するように求められます。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーアクセスが必要なタスクを実行する場合にのみ、ルートユーザーを使用してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理ユーザーの作成

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

AWS アカウントのルートユーザーをセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。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、「AWS サインイン User Guide」の「Signing in as the root user」を参照してください。
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、「IAM ユーザーガイド」の「AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理ユーザーを作成する

1. IAM Identity Center を有効にする

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Center の有効化」を参照してください。
2. IAM アイデンティティセンターで、管理ユーザーに管理アクセス権を付与します。

   IAM アイデンティティセンターディレクトリをアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Centerユーザーガイド」の「デフォルトの IAM アイデンティティセンターディレクトリを使用したユーザーアクセスの設定」を参照してください。

管理ユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

IAM アイデンティティセンターのユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in to the AWS access portal」を参照してください。

関連リソース

- IAM での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。

Amazon Nimble Studio でのセキュリティ

AWS クラウドセキュリティは最優先事項です。 AWS お客様は、最もセキュリティに敏感な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の恩恵を受けることができます。

AWS セキュリティはお客様とお客様との間で共有される責任です。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して説明しています。

- クラウドのセキュリティ — AWS AWS AWS クラウドクラウド内でサービスを実行するインフラストラクチャを保護する責任があります。 AWS また、安全に使用できるサービスも提供します。第三者監査人は、AWS、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ています。Amazon Nimble Studio に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」「」を参照してください。
- クラウドにおけるセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。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**
>
> 「セキュリティピラー- AWS Well-Architected フレームワーク」を読んで理解することを強くお勧めします。この記事には、インフラストラクチャーを保護するための重要な原則が記載されています。 AWS

このドキュメントは、Nimble Studio を使用する際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。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Nimble Studio を設定する方法を示します。また、 AWS Nimble Studioリソースの監視と保護に役立つ他のサービスの使い方についても学びます。

詳細情報

- セキュリティピラー- AWS Well-Architected フレームワーク
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) のセキュリティ
- Amazon Virtual Private Cloud でのセキュリティ

- AWS セキュリティ認証情報
- セキュリティとコンプライアンスの目標を満たすように Amazon EC2 を設定し、Amazon EC2 リソースの保護に役立つ他の サービスの使用方法を学びます。
  - Linux
  - Windows

セキュリティの設定 AWS アカウント

このガイドでは、 AWS アカウント リソースが危険にさらされた場合に通知を受け取るように設定し、 AWS アカウント 特定のユーザーがアクセスできるようにする方法について説明します。 AWS アカウント リソースを保護して追跡するには、次の手順を実行してください。

コンテンツ

アカウントのアクセスキーを削除する

AWS Command Line Interface (AWS CLI) または AWS API を使用して、 AWS リソースへのプログラムによるアクセスを許可できます。ただし、root AWS アカウントに関連付けられたアクセスキーをプログラムによるアクセス用に作成したり使用したり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 API に必要なアクセス許可のみを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、「AWS 全般のリファレンス ユーザーガイド」の「AWS アカウントのアクセスキー管理」を参照してください。

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 の仕組みは次のとおりです。まず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を指定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取得することも、スマートフォンのアプリから取得することも可能です。

サポートされている MFA デバイスのリストから、使用する MFA デバイスのタイプを選択する必要があります。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、スマートフォンの紛失や破損の可能性について考慮します。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管することです。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ベートするか、仮想 MFA オプションを使用してデバイスキーを回復することです。

MFA の詳細については、「仮想多要素認証 (MFA) デバイスの有効化」を参照してください。

関連リソース

- 多要素認証を始める
- MFA AWS を使用する際のアクセスの保護

すべて有効にする CloudTrail AWS リージョン

を使用して、 AWS リソース内のすべてのアクティビティを追跡できますAWS CloudTrail。CloudTrail 今すぐオンにすることをおすすめします。これにより、 AWS Support AWS セキュリティや構成に関する問題を後でソリューションアーキテクトがトラブルシューティングする際に役立ちます。

CloudTrail 全員ログインを有効にするには AWS リージョン、「AWS CloudTrail 更新 — すべての地域で有効にする」と「複数のトレイルを使用する」を参照してください。

詳細については CloudTrail、「有効にする CloudTrail:API AWS アカウントアクティビティをあなたのログに記録する」を参照してください。Nimble Studio CloudTrail のモニタリング方法については、を参照してください。を使用して Nimble Studio の呼び出しを口ギングする AWS CloudTrail

Amazon GuardDuty と通知をセットアップする

Amazon GuardDuty は、以下を分析して処理する継続的なセキュリティ監視サービスです。

- 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、 AWS お客様の環境内で予期しない、または許可されていない可能性のある悪意のあるアクティビティを特定します。このアクティビティには、権限のエスカレートや、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、悪意のある IP GuardDuty アドレスやドメインのリストなどの脅威インテリジェンスフィードと機械学習を使用します。たとえば、 GuardDuty マルウェアを提供したり、ビットコインをマイニングしたりする、侵害された Amazon EC2 インスタンスを検出できます。

GuardDuty また、 AWS アカウント アクセス行動を監視して侵害の兆候がないか調べます。これには、にデプロイされたインスタンスが使用されたことがないなど、 AWS リージョン 許可されていないインフラストラクチャのデプロイメントが含まれます。また、パスワードの強度を低下させるパスワードポリシーの変更などの異常な API 呼び出しも含まれます。

GuardDuty セキュリティ結果を生成して、 AWS 環境の状態を通知します。 GuardDuty これらの結果はコンソールまたは Amazon CloudWatch イベントで確認できます。

Amazon SNS トピックおよびエンドポイントの設定

「Amazon SNS トピックおよびエンドポイントの設定」のチュートリアルの指示に従います。

EventBridge GuardDuty 調査結果のイベントを設定します。

EventBridge GuardDuty 生成されたすべての結果についてイベントを送信するルールを作成します。

EventBridge GuardDuty 調査結果の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:https://console.aws.amazon.com/events/
2. ナビゲーションペインで [Rules (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. AWS EventBridge イベントソースにはイベントまたはパートナーイベントを選択したままにします。
5. [イベントパターン] で、[イベントソース] に [AWS サービス] を選択します。次にGuardDuty、AWS サービスの場合は、[イベントタイプ] を、[GuardDuty 検索] を選択します。これは「Amazon SNS トピックおよびエンドポイントの設定」で作成したトピックです。

6. [次へ] を選択します。
7. [ターゲット 1] で [AWS サービス] を選択します。[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. [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) タグを使用してリソースを追跡する場合は、タグを追加します。 AWS
13. [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。

AWS アカウント セキュリティを設定したら、特定のユーザーにアクセス権を付与し、リソースが危険にさらされた場合に通知を受け取ることができます。

Amazon Nimble Studio でのデータ保護

AWS のデータ保護には、https://aws.amazon.com/compliance/shared-responsibility-model/、 (責任分担モデル) が適用されますAmazon Nimble Studio。このモデルで説明したように、 AWS は、

AWS クラウドすべてを稼働させ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。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に対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。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のよくある質問」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、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データ保護のため、 AWS アカウント 認証情報を保護し、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2、できれば TLS 1.3 が必要です。
- を使用して API とユーザーアクティビティのロギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- 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。
- コマンドラインインターフェイスまたは API AWS を介してアクセスするときに FIPS 140-2 で検証された暗号モジュールが必要な場合は、FIPS エンドポイントを使用してください。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) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや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。これには、コンソール、API、または SDK を操作する場合や、 AWS のサービス その他の方法でコンソール、API、Nimble Studioまたは SDK を使用する場合も含まれます。 AWS CLI AWS 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、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

AWS 責任分担モデルは Amazon Nimble Studio 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 クラウドお客様には、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を、適

切に制御する責任があります。このコンテンツには、 AWS のサービス 使用するのセキュリティ設定と管理タスクが含まれます。

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のよくある質問」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 では、AWS Key Management Service (AWS KMS) に保存されている暗号化キーを使用して、機密性の高いスタジオデータを保管時に暗号化し保護します。保存時の暗号化は、Nimble Studio AWS リージョン が利用可能なすべての場所で利用できます。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 AWS KMS が保管中のデータを暗号化する方法については、を参照してください。Amazon Nimble Studio のキー管理

キーでのグラントの使用 AWS KMS

グラントは、AWSAWS KMS プリンシパルが暗号操作でキーを使用できるようにするポリシー手段です。また、`DescribeKey` コマンドによる KMS キーの表示、権限の作成、管理を可能にします。

グラントは、 AWS のサービス AWS KMS と連動して保存されているデータを暗号化するために一般的に使用されます。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。

AWS のサービス 権限の使用方法の詳細については、AWS KMS サービスのユーザーガイドまたは開発者ガイドの「 AWS のサービス 使用方法」または「保存時の暗号化」トピックを参照してください。

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
JavaScript 画像やファイルなどの Web 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。	データ暗号化では、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 ビットのAdvanced Encryption Standard (AES-256) を使用して暗号化され、TLS 1.2 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。	TLS 1.2 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キー – キーはアカウントに保存され、ユーザーによって作成、所有、管理されます。キーは自由に制御できます。 AWS KMS 料金がかかります。

AWS Key Management Service (AWS KMS) 内の顧客管理の KMS キーを削除すると破壊的であり、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 キーを削除すると、そのキーで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。

そのため、 AWS KMS お客様にはキーを削除するまでに最大 30 日間の待機期間を設ける必要があります。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、破壊的で危険な場合があるため、7～30 日の待期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付と時刻を取得するには、DescribeKeyオペレーションを使用してください。また、[General configuration] (一般的な設定) セクションのキーの詳細ページにある AWS KMS コンソールでは、削除のためにスケジュールされた日付を確認することが可能です。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に使用することはできません。
- AWS KMS AWS KMS 削除待ちの顧客管理キーのバッキングキーはローテーションしません。

AWS KMS カスタマー管理キーの削除について詳しくは、「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

データ保護のため、 AWS アカウント 認証情報を保護し、 AWS Identity and Access Management (IAM) で個別のアカウントを設定することをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2 以降が推奨されます。

- を使用して API とユーザーアクティビティのロギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- コマンドラインインターフェイスまたは API により AWS にアクセスするときに FIPS 140-2 検証済み暗号化モジュールが必要な場合は、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) 140-2」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。これには、コンソール、API AWS CLI、または AWS SDK AWS のサービス を使用して Amazon Nimble Studio やその他のツールを操作する場合も含まれます。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。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

診断データとメトリクス

Amazon Nimble Studio は StudioBuilder、のデプロイと削除の際に、問題の診断と Nimble Studio の機能とユーザーエクスペリエンスの向上の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 のバージョンWindows、オペレーティングシステム (Linux、またはmacOS)、および実行環境。 StudioBuilder

Amazon Nimble Studio 向けの Identity and Access Management

AWS Identity and Access Management (IAM) は、 AWS のサービス AWS 管理者がリソースへのアクセスを安全に制御できるようにするためのものです。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 AWS のサービス は追加料金なしで使用できるアプリです。

トピック

- 対象者

- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon Nimble Studio で IAM を使用する方法
- Amazon Nimble Studio のアイデンティティベースのポリシー例
- AWS Amazon Nimble Studio の管理ポリシー
- サービス間の混乱した代理の防止
- 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

対象者

AWS Identity and Access Management (IAM) の使用方法は、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、IAM の基本概念を理解してください。企業における Nimble Studio での IAM の使用方法については、「Amazon Nimble Studio で IAM を使用する方法」を参照してください。

アイデンティティを使用した認証

認証とは、ID AWS 認証情報を使用してサインインする方法です。を使用してサインインする方法の詳細については AWS Management Console、『IAM ユーザーガイド』の「IAM ユーザーまたは root AWS Management Console ユーザーとしてにサインイン」を参照してください。

AWS アカウント root ユーザーまたはユーザーとして認証 (サインイン AWS) されるか、IAM ロールを引き受ける必要があります。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、管理者が事前に IAM ロールを

使用して ID フェデレーションを設定している必要があります。 AWS 他社の認証情報を使用してアクセスすると、間接的にロールを引き継ぐことになります。

AWS Management Console に直接サインインするには、パスワードとルートユーザーの E メールまたはユーザーのユーザー名を使用します。自分のルートユーザーまたはユーザーのアクセスキーを使用すると、 AWS へのプログラム的なアクセスが可能です。

AWS には、認証情報を使用してリクエストに暗号的に署名するための SDK ツールとコマンドラインツールが用意されています。 AWS ツールを使用しない場合は、自分でリクエストに署名してください。これには、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ある署名バージョン 4 を使用します。リクエストの認証の詳細については、「 AWS 全般のリファレンス 」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。

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。たとえば、アカウントのセキュリティを強化するために多要素認証 (MFA) AWS を使用することを推奨しています。詳細については、「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

を初めて作成するときは AWS アカウント、 AWS のサービス アカウント内のすべてのリソースに完全にアクセスできるシングルサインイン ID から始めます。この ID は AWS アカウント root ユーザーと呼ばれ、アカウントの作成に使用した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されます。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、初期の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。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

ユーザーとは、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権限を持つ社内の AWS アカウント ID です。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。アクセスキーの生成方法の詳細については、「IAM 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。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、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

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、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。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。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用してロールを引き受けることができます。ロールの使用方法については、「IAM ユーザーガイド」の 「IAM ロールを使用する」を参照してください。

一時的な認証情報を持った IAM 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、特定のタスクのための複数の異なるアクセス許可を一時的に受け取るために、IAM ロールを引き受けることができます。
- フェデレーテッドユーザーアクセス — ユーザーを作成する代わりに、エンタープライズユーザーディレクトリ AWS Directory Service、またはウェブ ID プロバイダーの既存の ID を使用できます。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 では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーションユーザーにロールを割り当てます。フェデレーションユーザーの詳細については、「IAM ユーザーガイド」の「フェデレーションユーザーとロール」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 ポリシーを書き込んだり理解したりすることなく、リソース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、そのユーザーは、起動プロファイルを使用するために必要な IAM アクション (プロパティの表示、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) の実行を認可されます。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける 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、IAM

内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス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。

- 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 EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールを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る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、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」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

ポリシーを作成して IAM ID AWS またはリソースにアタッチすることで、アクセスを制御します。AWS ポリシーは、ID またはリソースに関連付けられると、 AWS そのアクセス権限を定義するオブジェクトです。ルートユーザーまたは単なる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 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が評価されます。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 JSON ドキュメントとして保存されます。 AWS 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、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。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、許可のない状態からスタートします。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方法を問わず、アクションの許可を定義します。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は AWS Management Console、、 AWS CLI、または AWS API からロール情報を取得できます。

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は、ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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、「IAM ユーザーガイド」の「IAM ポリシーの作成」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、および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、 AWS 管理ポリシーと顧客管理ポリシーが含まれます。マネージド型ポリシーとインラインポリシーの内、いずれ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比較」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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、ロール、フェデレーティッドユーザ、またはを含めることができます。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。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

Nimble Studio のアクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL 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は使用しません。

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。ACL の詳細については、「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 あまり一般的ではないポリシータイプもサポートしています。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によって IAM エンティティ (ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティに権限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、許可は無効になります。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 (SCP) – SCP とは、Organizations 内の組織または組織単位 (OU) に対し、アクセス許可の上限を指定するための JSON ポリシーです。Organizations は、ビジネスが所有する複数の AWS アカウント を、グループ化および一元管理するためのサービスです。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 (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 AWS アカウント root ユーザーを含むメンバーアカウント内のエンティティの権限を制限します。Organizations と SCP の詳細については、『 AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- 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ティッド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、許可は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」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。 AWS 複数のポリシータイプが関係している場合にリクエストを許可するかどうかを決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Amazon Nimble Studio で IAM を使用する方法

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 の機能について学びます。

Amazon Nimble Studio で使用できる IAM の機能

IAM 機能	Nimble Studio Support
Nimble Studio のポリシーアクション	はい
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 (ACL)	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
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	No

Nimble Studio などがほとんどの IAM AWS のサービス 機能でどのように動作するかを大まかに把握するには、『IAM ユーザーガイド』の「IAM との連携」を参照してくださいAWS のサービス 。

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	Yes

アイデンティティベースポリシーは、ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

IAM のアイデンティティベースポリシーでは、許可または拒否するアクションとリソース、また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学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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、またはが含まれます。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	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。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`要素には、ポリシー内の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が記述されます。ポリシーアクションは通常、関連する AWS API オペレーションと同じ名前です。一致する API オペレーションの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アクセス許可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	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。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。

Resource JSON ポリシーの要素は、オブジェクトあるい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は、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	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。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。

1 つのステートメントに複数の Condition要素を指定する場合、または 1 つの Condition要素に複数のキーを指定する場合、 AWS では AND論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、 AWS では OR論理演算子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、IAM ユーザーガイド の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS 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。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」の「AWS グローバル条件コンテキストキー」を参照してください。

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 (ACL)

ACL のサポート	No

Nimble Studio はアクセスコントロールリスト (ACL) をサポートしていません。ACL は、どのプリンシパル (アカウントメンバー、ユーザー、ロール) がリソースへのアクセス許可を持つかを制御します。ACL 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は使用しません。

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

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、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) AWS や多くのリソースにタグを付けることができます。エンティティとリソースのタグ付けは、ABAC の最初のステップです。次に、アクセスを試行する先のリソースのタグとプリンシパルのタグが一致した場合にオペレーションを許可するよう、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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」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	Yes

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機能しないものもあります。 AWS のサービス 一時的な認証情報で機能するものなど、追加情報については、『IAM ユーザーガイド』の「IAM と連携する」を参照してくださいAWS のサービス 。

ユーザー名とパスワード以外の方法でにサインインすると、 AWS Management Console 一時的な認証情報が使用されることになります。たとえば、会社のシングルサインオン (SSO) AWS リンクを使用してアクセスすると、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。ロールの切り替えに関する詳細については、「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。

または API 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 AWS その後、その一時的な認証情報を使用してアクセスできます AWS。 AWS 長期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すすめします。詳細については、「IAM の一時的セキュリティ認証情報」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	Yes

Nimble Studio のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける 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、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス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。

> **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	いいえ

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、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、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 アカウント内に表示され、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。

サービスリンクロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、[Service-linked role (サービスリンクロール)] 列に Yes と記載されたサービスを見つけます。サービスにリンクされた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、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することもできません。管理者は、リソースで必要なアクションを実行するための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 JSON ポリシードキュメント例を使用して IAM の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、「IAM ユーザーガイド」の「IAM ポリシーの作成」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を実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースのポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください。

- AWS 管理ポリシーを使い始める — Nimble Studio をすぐに使い始めるには、 AWS 管理ポリシーを使用して従業員に必要な権限を付与してください。これらのポリシーはアカウントで既に有効になっており、 AWSによって管理および更新されています。詳細については、IAM User Guide の「AWS 管理ポリシーでアクセス権限を使い始める」を参照してください。
- 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、IAM ユーザーガイドの「最小特権を認める」を参照してください。
- 機密性の高いオペレーションのために MFA を有効にする - 追加のセキュリティとして、機密性の高いリソースや API オペレーションにアクセスする際に多要素認証 (MFA) を使用することをユーザーに要求します。詳細については、「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。
- 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。指定された日付または時間範囲内でのみリクエストを許可する条件を書くことも、SSL や MFA の使用を要求することもできます。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

AWS Amazon Nimble Studio の管理ポリシー

ユーザー、グループ、ロールに権限を追加するには、 AWS 自分でポリシーを作成するよりも管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに始めるには、 AWS 管理ポリシーをご利用ください。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、IAM ユーザーガイドの「AWS 管理ポリシー」を参照してください。

AWS AWS サービスは管理ポリシーを維持および更新します。 AWS 管理ポリシーの権限は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、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、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。 AWS サービスは管理ポリシーから権限を削除しないため、ポリシーを更新しても既存の権限が損なわれることはありません。

さらに、 AWS 複数のサービスにまたがるジョブ機能の管理ポリシーもサポートします。たとえば、ReadOnlyAccess AWS AWS 管理ポリシーはすべてのサービスとリソースへの読み取り専用アクセスを提供します。あるサービスで新しい機能を立ち上げる場合は、 AWS は、追加された演算とリソースに対し、読み込み専用の権限を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

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場合、スタジオのペルソナごとに 1 つの IAM ロール (スタジオ管理者とスタジオユーザー) が作成されます。それぞれに 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。そのため、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の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ており、それぞれに IAM 管理ポリシーがアタッチされます。

ジョブ機能ポリシーのリストと説明については、「IAM ユーザーガイド」の「AWS ジョブ機能の 管理ポリシー」を参照してください。

AWS 管理ポリシー:**AmazonNimbleStudio-LaunchProfileWorker**

AmazonNimbleStudio-LaunchProfileWorker ポリシーは IAM ID にアタッチできます。

Nimble Studio Builder で作成された EC2 インスタンスにこのポリシーをアタッチして、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。

- ds- LaunchProfile 従業員が a AWS Managed Microsoft AD に関連する接続情報を発見できるようにします 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の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 管理ポリシー:**AmazonNimbleStudio-StudioAdmin**

AmazonNimbleStudio-StudioAdmin ポリシーは IAM ID にアタッチできます。

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 ユーザに委任された Nimble リソースへのアクセスを許可します。 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 がスタジオに関連付けられているワークステーションに仮想ワークステーションを追加できるようにします。 AWS Managed Microsoft AD

- ec2 - Nimble Studio で、設定された VPC への仮想ワークステーションのアタッチを許可します。
- fsx - Nimble Studio で、設定された Amazon FSx ボリュームへの仮想ワークステーションの接続を許可します。
- クラウドウォッチ-Nimble Studio がメトリクスを取得できるようにします。 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 管理ポリシー:**AmazonNimbleStudio-StudioUser**

AmazonNimbleStudio-StudioUser ポリシーは IAM ID にアタッチできます。

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 ユーザに委任された Nimble リソースへのアクセスを許可します。 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 がスタジオに関連付けられているワークステーションに仮想ワークステーションを追加できるようにします。 AWS Managed Microsoft AD
- ec2 - Nimble Studio で、設定された VPC への仮想ワークステーションのアタッチを許可します。
- fsx - Nimble Studio で、設定された Amazon FSx ボリュームへの仮想ワークステーションの接続を許可します。

```
{
  "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 での AWS 管理ポリシーの更新

このサービスが変更の追跡を開始して以降の Amazon Nimble Studio AWS の管理ポリシーの更新に関する詳細を表示します。

変更	説明	日付
AWS 管理ポリシー: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

変更	説明	日付
AWS 管理ポリシー: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 管理ポリシー: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 管理ポリシー: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 管理ポリシー:AmazonNimbleStudio-StudioUser – Updated policy	Amazon Nimble Studio は、スタジオ管理者がメトリックスを取得できるようにポリシーを更新しました。 CloudWatch	2021 年 11 月 11 日
AWS 管理ポリシー: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 管理ポリシー: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

変更	説明	日付
AWS 管理ポリシー: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 管理ポリシー: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
AWS 管理ポリシー: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 管理ポリシー: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 は、AWS 管理ポリシーの変更の追跡を開始しました。	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。では AWS、サービス間のなりすましによって、混乱した代理人問題が発生する可能性があります。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。これを防ぐために、 AWS には、アカウント内のリソースへのアクセス権が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールが用意されています。

リソースポリシーの `aws:SourceArn` および `aws:SourceAccount` のグローバル条件コンテキストキーを使用して、Identity and Access Management (IAM) が Amazon Nimble Studio に付与する、リソースへのアクセス許可を制限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。

`aws:SourceArn` 値はスタジオの ARN、`aws:SourceAccount` はアカウント ID 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ための最も効果的な方法は、リソースの完全な ARN を指定して `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。リソースの ARN 全体が不明の場合、または複数のリソースを指定する場合には、ARN の未知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。例えば `arn:aws:nimble::123456789012:*` です。

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 ロールを設定してポリシーを評価します。 AWS その後、いずれかのユーザーが 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、`aws:SourceArn` の StudioArn を使用できます。

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

次の情報は、Nimble Studio と IAM の使用時に発生する可能性のある、一般的な問題の診断や修復に役立ちます。

トピック

- Nimble Studio でアクションを実行する権限がない。
- iam: PassRole を実行する権限がありません。
- 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。
- 自分以外の人にも自分の Nimble AWS アカウント Studio リソースへのアクセスを許可したい。

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。

次の例は、mateojackson という IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細を表示しようとしたとき、架空の nimble:*GetWidget* アクセス許可がない場合に発生するエラーを示しています。

```
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、管理者に問い合わせてください。 AWS サインイン資格情報を提供した担当者が管理者です。

iam: PassRole を実行する権限がありません。

[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。

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。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、IAM ユーザーガイドの「アクセスキーの管理」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。手順については、「IAM ユーザーガイド」の「アクセスキーの管理」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。

他のユーザーの Nimble Studio へのアクセスを許可するには、アクセスする必要があるユーザー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。ユーザーまたはアプリケーションは、そのエンティティの認証情報を使用して AWSにアクセスします。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、 AWS Management Consoleで `AmazonNimbleStudio-StudioUser` を提供します。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許可を付与します。

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 が委任したユーザーおよびグループの作成」を参照してください。

自分以外の人にも自分の Nimble AWS アカウント Studio リソースへのアクセスを許可したい。

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 (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

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 で IAM を使用する方法」を参照してください。
- AWS アカウント 所有しているリソース全体のリソースへの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「AWS アカウント 所有する別の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスを第三者に提供する方法については AWS アカウント、IAM ユーザーガイドの「AWS アカウント 第三者が所有するリソースへのアクセスの提供」を参照してください。
- ID フェデレーションを介し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「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」をご参照ください。
- 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の詳細については、「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との相違点」 をご参照ください。

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 とソリューションの信頼性、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 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ことで、マルチポイント障害が発生した場合でもより簡単にデバッグできます。

AWS また、Nimble Studio には、ユーザーガイドなどを使用して Nimble Studio の呼び出しをロギングする AWS CloudTrail、リソースを監視し、潜在的なインシデントに対応するためのツールが用意されています。AWS CloudFormation

JSON テンプレートや YAML テンプレートの例など AWS CloudFormation、Amazon Nimble Studio との連携方法の詳細については、ユーザーガイドの Amazon Nimble Studio リソースとプロパティリ

ファレンスを参照してください。 AWS CloudFormation CloudFormationテンプレートの使用方法については、「コンセプト」を参照してください。AWS CloudFormation

トピック

- を使用して Nimble Studio の呼び出しを口ギングする AWS CloudTrail

を使用して Nimble Studio の呼び出しを口ギングする AWS CloudTrail

Amazon Nimble Studio は、ユーザー AWS CloudTrail、ロール、または Nimble Studio AWS のサービス 内で実行されたアクションの記録を提供するサービスと統合されています。 CloudTrail Nimble Studio のすべての API コールをイベントとしてキャプチャします。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。

トレイルを作成すると、Nimble Studio CloudTrail のイベントを含め、Amazon S3 バケットへのイベントの継続的な配信を有効にできます。トレイルを設定しなくても、 CloudTrail コンソールの [イベント履歴] に最新のイベントが表示されます。によって収集された情報を使用して CloudTrail、Nimble Studio に対して行われた要求、要求が行われた IP アドレス、要求の実行者、実行日時、その他の詳細情報を確認できます。

の Nimble Studio の情報 CloudTrail

CloudTrail AWS アカウント アカウントを作成すると、ユーザー側で有効になります。Nimble Studio でアクティビティが発生すると、 CloudTrail AWS のサービス そのアクティビティはイベント履歴の他のイベントと共にイベントに記録されます。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、「 CloudTrail イベント履歴によるイベントの表示」を参照してください。

Nimble Studio のイベントを含め AWS アカウント、内のイベントを継続的に記録するには、トレイルを作成してください。トレイルを使用すると CloudTrail 、Amazon S3 バケットにログファイルを配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。トレイルは、 AWS パーティション内のすべてのリージョンからのイベントを記録し、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、 AWS のサービス CloudTrail ログに収集されたイベントデータをさらに分析して処理するように other を設定できます。

詳細については、次を参照してください:

「追跡の作成の概要」

CloudTrail サポート対象のサービスとインテグレーション

の Amazon SNS 通知の設定 CloudTrail

CloudTrail 複数のリージョンからのログファイルの受信

CloudTrail 複数のアカウントからのログファイルの受信

Nimble Studio CloudTrail のアクションはログに記録され、Amazon Nimble Studio API リファレンスに記載されています。たとえば、、を呼び出したり、 DeleteStudio アクションを実行したりすると CreateStudio GetStudio 、ログファイルにエントリが生成されます。 CloudTrail

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、以下を判別するために役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザーの認証情報を使用して行われたかどうか。
- 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 サービスによって送信されたかどうか。

詳細については、CloudTrail ユーザー Identity 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

トレイルは、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。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。 CloudTrail ログファイルはパブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序で表示されることはありません。

この JSON の例は、次の 3 つのアクションを示しています。

- アクション_1: CreateStudio
- アクション_2: GetStudio
- アクション_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、およびイベントの識別に役立つ「」や「」などのその他の「RrequestParameters」が表示されていることがわかります。userRoleArn adminRoleArn「creationDate」に時間と日付が表示され、リクエストが発生したソースは「eventSource」:「nimble.amazonaws.com」としてマークされています。

CloudTrail AWS アカウント アカウントを作成すると、ユーザー側で有効になります。IAM または AWS STS でアクティビティが発生すると、 CloudTrail AWS のサービス そのアクティビティはイベント履歴の他のイベントとともにイベントに記録されます。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 コンソールからの呼び出しや API 呼び出しを含め、IAM と AWS Security Token Service (AWS STS) のすべての API 呼び出しをイベントとしてキャプチャします。IAM と併用する方法の詳細については AWS STS、「 CloudTrail での IAM と API 呼び出しのロギング」を参照してください。 AWS STS AWS CloudTrail

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

Amazon が提供するその他のモニタリングサービスについては、Amazon CloudWatch ユーザーガイド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 は責任分担モデルを採用しており、 AWS コンプライアンスはお客様とお客様の間で共有されています。

AWS のサービス が特定のコンプライアンスプログラムの適用範囲内にあるかどうかを確認するには、「AWS のサービス 対象範囲:コンプライアンスプログラム別」の「)」を参照して、関心のあるコンプライアンスプログラムを選択してください。AWS のサービス 一般的な情報については、「AWS」を参照してください。

サードパーティ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、の「レポートのダウンロード」の「 AWS Artifact」を参照してください AWS Artifact。

AWS のサービス を使用する際のコンプライアンス責任は、データの機密性、会社のコンプライアンス目標、および適用される法律と規制によって決まります。 AWS 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 — これらの導入ガイドでは、アーキテクチャ上の考慮事項について説明し、 AWS セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順を説明しています。
- Amazon Web Services での HIPAA 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 HIPAA 対応アプリケーションを作成する方法について説明しています。 AWS

  > **Note**
  >
  > すべての企業が AWS のサービス HIPAA に適格というわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS — この一連のワークブックとガイドは、お客様の業界や地域に当てはまる場合があります。
- 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見た責任分担モデルを理解してください。このガイドは、 AWS のサービス セキュリティを確保するためのベストプラクティスをまとめたもので、複数のフレームワーク (米国標準技術研究所 (NIST)、ペイメントカード業界セキュリティ標準審議会 (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティ管理へのガイダンスをまとめています。
- AWS Config 開発者ガイドのルールによるリソースの評価 — AWS Config このサービスでは、リソース構成が社内慣行、業界ガイドライン、規制にどの程度準拠しているかを評価します。
- AWS Security Hub— AWS のサービス これにより、内部のセキュリティ状態を包括的に把握できます。 AWS Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対する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。

- AWS Audit Manager— AWS のサービス これにより、 AWS 使用状況を継続的に監査して、リスクの管理や規制や業界標準への準拠を簡素化できます。

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

マネージド型サービスとして、Amazon Nimble Studio AWS はグローバルネットワークセキュリティによって保護されています。 AWS AWS セキュリティサービスとインフラストラクチャを保護する方法については、「AWS クラウドセキュリティ」を参照してください。 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して環境を設計するには、「Security Pillar AWS Well-Architected Framework におけるインフラストラクチャ保護」を参照してください。

AWS 公開されている API 呼び出しを使用して、ネットワーク経由で Nimble Studio にアクセスします。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)。TLS 1.2、できれば TLS 1.3 が必要です。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイート。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。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられている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) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

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

Nimble Studio とソリューションの信頼性、可用性、パフォーマンスを維持するには、モニタリングが重要です。 AWS 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

データ保護のため、 AWS アカウント 認証情報を保護し、 AWS Identity and Access Management (IAM) で個別のアカウントを設定することをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2 以降が推奨されます。
- を使用して API とユーザーアクティビティの口ギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- 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。
- コマンドラインインターフェースまたは API を使用して AWS にアクセスするときに FIPS 140−2 検証済みの暗号化モジュールが必要な場合は、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) 140-2」 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配置しないことを強くお勧めします。これには、コンソール、API AWS CLI、または AWS SDK AWS のサービス を使用して Amazon Nimble Studio やその他のツールを操作する場合も含まれます。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、診断口グへ含めるために取得される可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

アクセス許可

ユーザーや IAM AWS ロールを使用してリソースへのアクセスを管理し、ユーザーには最小限の権限を付与します。アクセス認証情報の作成、配布、ローテーション、取り消しに関する認証情報管理ポリシーと手順を確立します。 AWS 詳細については、IAM ユーザーガイドの「IAM ベストプラクティス」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。