管理者ガイド

Amazon Nimble Studio

Amazon Nimble Studio: 管理者ガイド

Table of Contents

サポート終了通知: 2024 年 10 月 22 日、 AWS は Amazon Nimble Studio のサポートを終了します。2024 年 10 月 22 日以降、Nimble Studio コンソールまたは Nimble Studio リソースにアクセスできなくなります。

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。

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。や Nimble Studio ファイル転送などの AWS Thinkboxアプリケーションを追加および管理することもできます。

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 には AWS 経験は必要ありません。約 5 分で設定できます。

内容

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 Krakatoa Thinkbox 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 コストの管理については、AWS Cost Explorer Service「」および「」を参照してくださいAWS Budgets。

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、クリエイティブスタジオ AWS のサービス がストーリーボードのスケッチから最終的な成果物まで、完全にクラウドで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作成できるようにする 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 マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。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、一般的な職務機能にアクセス許可を付与するために使用されます。ジョブ関数ポリシーは、新しいサービスと API オペレーションが導入され AWS たときに によって維持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 などの部分的なアクセス AWS 管理ポリシーでは、フルアクセスを許可 AWS のサービス せずに特定のレベルのアクセスを に提供できます。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 は、 を管理するための幅広いサービスコンソールのコレクションへのアクセスを提供するウェブアプリケーションです AWS のサービス。

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 アイデンティティセンター)

IAM Identity Center は、複数の AWS アカウント およびビジネスアプリケーションへのアクセスを一元管理することを容易にする AWS 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。

AWS PrivateLink

AWS PrivateLink は AWS のサービス、トラフィックをパブリックインターネットに公開することなく、VPCs とオンプレミスネットワーク間のプライベート接続を提供します。 AWS PrivateLink

を使用すると、さまざまなアカウントや VPCs 間でサービスを簡単に接続できます。 AWS PrivateLinkは、 に請求される月額料金で利用できます AWS アカウント。

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 には、スタジオのデプロイを選択する 11 AWS リージョン の が用意されています。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、 AWS リソースをさまざまな方法で分類できます。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。

タグを使用すると、 AWS リソースを目的、所有者、または環境別に分類できます。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

IAM のセットアップ

開始する前に、次の AWS Identity and Access Management (IAM) 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 AWS アカウント として にサインインして、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

がない場合は AWS アカウント、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/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 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、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/ の [マイアカウント] 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ら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして、管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして 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 ユーザーガイド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。
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 「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。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   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、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 AWS IAM Identity Center ユーザーガイド」の「Configure user access with the default IAM アイデンティティセンターディレクトリ」を参照してください。

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 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 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、「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。 AWS サインイン

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
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、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」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の作成、 の確認 AWS リージョン、設定の確認、スタジオの作成を行う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。

初めての AWS お客様は、Nimble Studio のセットアップ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 データセンターの集合の物理的な場所です。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。これらの設定を使用すると、Nimble Studio のセットアップで に加えられたすべての変更を表示したり AWS アカウント、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 サービスは、ユーザーに代わってアクションを実行するサービスロールを引き受けることができます。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。

AWS Identity and Access Management (IAM) 管理ポリシーをスタジオユーザーロールにアタッチできます。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、「とは AWS IAM Identity Center」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、再暗号化に使用できる KMS キーのプライマリタイプです。

Nimble Studio には、次の AWS KMS 暗号化キータイプが含まれています。

- AWS 所有キー AWS 所有キーは、 が AWS のサービス 所有し、複数の で使用するために管理する KMS キーです AWS アカウント。 AWS 所有キーは には存在しませんが AWS アカウント、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。

  を使用するには AWS KMS、キーまたはそのキーポリシーを作成または維持する必要はありません。 AWS 所有キーの使用には料金はかかりません。また、 のクォータにも AWS KMS カウントされません AWS アカウント。
- 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 の KMS AWS アカウント 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 AWS KMS を超えて への API リクエストごとに料金が発生します。 AWS KMS 料金の詳細については、「 AWS Key Management Service の料金」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 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. Select a different AWS KMS key (advanced) 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. にサインイン AWS Management Console 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」 のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。 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、 AWS とお客様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説明しています。

- クラウドのセキュリティ – AWS は、 で AWS 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 クラウド。 AWS は、安全に使用できるサービスも提供します。AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。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。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、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**
>
> Security Pillar - AWS Well-Architected Framework を読んで理解しておくことを強くお勧めします。この記事には、 AWS インフラストラクチャを保護するための主要な原則が含まれています。

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、 Nimble Studioリソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

詳細情報

- セキュリティの柱 - 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

AWS アカウント セキュリティの設定

このガイドでは、 リソース AWS アカウント 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できるように を設定する方法を示します。を保護し AWS アカウント 、リソースを追跡するには、次の手順を実行します。

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 で CloudTrail を有効にする AWS リージョン
- Amazon GuardDuty および通知のセットアップ

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 APIs 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、 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 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 を使用した へのアクセスの保護

すべての で CloudTrail を有効にする 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 を今すぐオンにすることをお勧めします。これは、 サポート および AWS ソリューションアーキテクトが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するのに役立ちます。

すべての で CloudTrail のログ記録を有効にするには AWS リージョン、AWS CloudTrail 「更新 – すべてのリージョンで を有効にする」および「複数の証跡を使用する」を参照してください。

CloudTrail の詳細については、CloudTrail を有効にする: で API アクティビティをログ AWS アカウントに記録する」を参照してください。CloudTrail で Nimble Studio を監視する方法については、「を使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrail」を参照してください。

Amazon GuardDuty および通知のセットアップ

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、 AWS 環境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。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。GuardDuty は、悪意のある IP 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や機械学習を使用して、これらのアクティビティを識別します。例えば、GuardDuty はマルウェアやマイニングビットコインに使われている侵害された Amazon EC2 インスタンスを検出できます。

また、GuardDuty は AWS アカウント アクセス動作をモニタリングして侵害の兆候がないか調べます。これには、使用したことのない 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 AWS リージョン のデプロイが含まれます。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 は、セキュリティ上の検出結果を生成することで、 AWS 環境のステータスを通知します。これらの検出結果は、GuardDuty コンソールまたは Amazon CloudWatch Events 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。

GuardDuty の検出結果に対する EventBridge イベントのセットアップ

EventBridge のルールを作成して GuardDuty が生成するすべての検出結果に対するイベントを送信します。

GuardDuty の検出結果に対する EventBridge イベントを作成するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) にサインインします。
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. [イベントソース] で選択したAWS イベントまたは EventBridge パートナーイベントは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、[AWS サービス] に [GuardDuty] を、[イベントタイプ] には [GuardDuty の検出結果] 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. [Next (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. [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 AWS リソースを追跡する場合は、タグを追加します。
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。

AWS アカウント セキュリティを設定したので、特定のユーザーにアクセスを許可し、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。

Amazon Nimble Studio でのデータ保護

責任 AWS 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。ユーザーは、このインフラストラクチャでホストされ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に関する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。

データ保護の目的で、認証情報を保護し AWS アカウント 、 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 AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 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します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理された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 にアクセスするときに FIPS 140-3 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) 140-3」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を、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含めないことを強くお勧めします。これは、コンソールNimble Studio、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Amazon Nimble Studio でのデータ保護には、 AWS 責任共有モデルが適用されます。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。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および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。保管時の暗号化は、Nimble Studio AWS リージョン が利用可能なすべての で使用できます。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 が AWS KMS を使用して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。

AWS KMS キーでの許可の使用

グラントは、AWS プリンシパルが暗号化オペレーションで AWS KMS 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、保管中のデータを暗号化 AWS KMS するために と統合 AWS のサービス する によって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。

グラント AWS のサービス の使用方法の詳細については、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「 AWS のサービス の使用方法 AWS KMS 」または「保管時の暗号化」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
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。キーを完全に制御できます。 の AWS KMS 料金が適用されます。

AWS Key Management Service （ AWS KMS) でカスタマーマネージド KMS キーを削除すると、破壊的になり、危険にさらされる可能性があります。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 では、キーを削除する前に最大 30 日間の待機期間がお客様に与えられます。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ます。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 は、削除保留中のカスタマーマネージドキーのバッキングキーをローテーションしません。 AWS KMS

カスタマーマネージド AWS KMS キーの削除の詳細については、「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

データ保護の目的で、 AWS アカウント 認証情報を保護し、 AWS Identity and Access Management (IAM) を使用して個々のアカウントを設定することをお勧めします。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 AWS リソースと通信します。TLS 1.2 以降が推奨されます。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- 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を使用します AWS のサービス。
- コマンドラインインターフェイスまたは 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入力しないことを強くお勧めします。これは、コンソール、API、、 AWS CLIまたは SDK AWS のサービス を使用して Amazon Nimble Studio または他の を使用する場合も同様です。 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。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

StudioBuilder のデプロイと削除中に Amazon Nimble Studio が特定のメトリクスを収集し、問題の診断と、Nimble Studio の機能改善およびユーザーエクスペリエンス向上のために使用します。

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。
- システムと環境情報 — Python のバージョン、オペレーティングシステム (Windows、Linux、macOS)、StudioBuilder が実行される環境です。

Amazon Nimble Studio 向けの Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ 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 は、追加料金なしで AWS のサービス 使用できる です。

トピック

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すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。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 認証情報 AWS を使用して にサインインする方法です。を使用したサインインの詳細については AWS Management Console、IAM ユーザーガイドの「IAM ユーザーまたはルートユーザー AWS Management Console として にサインインする」を参照してください。

AWS アカウント ルートユーザー、ユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) される必要があります。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。別の会社の認証情報 AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

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。 AWS ツールを使用しない場合は、リクエストに自分で署名します。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。例えば、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強化することをお勧めします。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。

AWS アカウント ルートユーザー

を初めて作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つシングルサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、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、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

ユーザーは、単一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 AWS アカウントを持つ 内のアイデンティティです。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、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。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。ロールを切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 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。

IAM ロールと一時的な認証情報は、次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。
- フェデレーティッドユーザーアクセス – ユーザーを作成する代わりに、 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 プロバイダーから既存の 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 で実行されてい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 CLI または AWS API リクエストを実行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。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。AWS ロールを EC2 インスタンスに割り当て、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、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

でアクセスを制御する AWS には、ポリシーを作成し、IAM ID または AWS リソースにアタッチします。ポリシーは のオブジェクト AWS であり、ID またはリソースに関連付けられると、そのアクセス許可を定義します。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、 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 AWS 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 JSON ドキュメント AWS として に保存されます。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 JSON AWS 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ーは、 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、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 管理ポリシーとカスタマー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 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。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

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。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。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 は、一般的ではない追加のポリシータイプを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 (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 ルートユーザー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を制限します。Organizations と SCPs「 AWS Organizations ユーザーガイド」のSCPs」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、「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。複数のポリシータイプが関係する場合に がリクエストを許可するかどうか AWS 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	あり
Nimble Studio のポリシーリソース	あり
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)	なし
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	あり
Nimble Studio のクロスサービスプリンシパル許可	あり
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	いいえ

Nimble Studio およびその他の がほとんどの IAM 機能と AWS のサービス 連携する方法の概要を把握するには、AWS のサービス 「IAM ユーザーガイド」の「IAM と連携する 」を参照してください。

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	はい

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	いいえ

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 を含めることができます 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	はい

管理者は JSON AWS 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の名前は通常、関連する AWS API オペレーションと同じです。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を確認するには、「サービス認可リファレンス」の「Amazon Nimble Studio で定義されるアクション」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	はい

管理者は JSON AWS 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	はい

管理者は JSON AWS 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して、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 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ています。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	いいえ

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。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。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	はい

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する機能などの詳細については、AWS のサービス「IAM ユーザーガイド」の「IAM と連携する」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、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。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 AWS を動的に生成することをお勧めします。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	はい

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。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はできません。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 管理ポリシーを使用して開始する – Nimble Studio の使用をすばやく開始するには、 AWS 管理ポリシーを使用して、従業員に必要なアクセス許可を付与します。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 ユーザーガイド」の「 AWS マネージドポリシーでアクセス許可の使用を開始する」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 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、自分でポリシーを作成するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する 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。すぐに開始するには、 AWS マネージドポリシーを使用できます。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 サービスは、 AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。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。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

さらに、 は、複数のサービスにまたがる職務機能の管理ポリシー AWS をサポートします。例えば、ReadOnlyAccess AWS マネージドポリシーは、すべての AWS 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。サービスが新しい機能を起動する場合、 AWS は新たなオペレーションとリソース用に、読み取り専用の許可を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドのジョブ機能のAWS 管理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、そのスタジオの使用者 (スタジオ管理者とスタジオユーザー) ごとに 1 つの IAM ロールが作成されます。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 StudioBuilder を使用してスタジオを作成すると、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ており、それぞれに IAM 管理ポリシーがアタッチされます。

職務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 職務機能の管理ポリシーを参照してください。

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

AmazonNimbleStudio-LaunchProfileWorker ポリシーを IAM アイデンティティ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 ワーカーが、LaunchProfile に関連付けられている AWS Managed Microsoft AD に関する接続情報を検出できるようにします。
- ec2 - LaunchProfile ワーカーが、LaunchProfile 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。
- fsx - LaunchProfile ワーカーが、LaunchProfile に関連付けられている 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。

```
{
  "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**

AmazonNimbleStudio-StudioAdmin ポリシーを IAM アイデンティティ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 - StudioAdmins によって委任された Nimble リソースに Studio ユーザーのアクセスを許可します。
- 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 AWS Managed Microsoft AD に関連付けられた に仮想ワークステーションを追加できるようにします。
- 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。
- cloudwatch - Nimble Studio で、CloudWatch メトリクスの取得を許可します。

```
{
  "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**

AmazonNimbleStudio-StudioUser ポリシーを IAM アイデンティティ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 - StudioAdmins によって委任された Nimble リソースに Studio ユーザーのアクセスを許可します。

- 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 AWS Managed Microsoft AD に関連付けられた に仮想ワークステーションを追加できるようにします。
- 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

Amazon Nimble Studio の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
AWS マネージドポリシー: AmazonNimbleStudio-StudioUser – ポリシーを更新	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 – ポリシーを更新	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 – ポリシーを更新	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 – ポリシーを更新	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

変更	説明	日付
AWS マネージドポリシー: AmazonNimbleStudio-StudioUser – Updated policy	Amazon Nimble Studio は、スタジオ管理者が CloudWatch メトリクスを取得できるようにポリシーを更新しました。	2021 年 11 月 11 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 AWS マネージド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り、混乱した代理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、1 つのサービス (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、 AWS では、アカウント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を提供しています。

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:* 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、 はロール AWS を設定し、ポリシーを評価します。 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 AWS 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 を実行する権限がない。
- 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 Nimble Studio リソース AWS アカウント 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。

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、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。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なnimble:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
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、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がない。

[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。

一部の AWS のサービス では、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、既存のロールをそのサービスに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、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。

自分の 以外のユーザーに Nimble Studio リソース AWS アカウント 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。
- 所有 AWS アカウント する 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「所有 AWS アカウント する別の 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サードパーティー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「サードパーティー AWS アカウント が所有する へのアクセスを提供する」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 AWS 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。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ように、 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します。

AWS および Nimble Studio には、 を使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrailおよび AWS CloudFormation ユーザーガイドなど、 リソースをモニタリングし、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。

JSON テンプレートや YAML テンプレートの例など AWS CloudFormation、Amazon Nimble Studio での の仕組みの詳細については、 AWS CloudFormation 「 ユーザーガイド」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。CloudFormation テンプレートの使用方法については、「AWS CloudFormation の概念」を参照してください。

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 AWS CloudTrail、Nimble Studio のユーザー、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である と統合 AWS のサービス されています。CloudTrail は、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。

追跡を作成すると、Nimble Studio のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追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。CloudTrail で収集された情報を使用して、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。

CloudTrail の Nimble Studio 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。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イベント履歴内の他の AWS のサービス のイベントと共に、CloudTrail 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イベント履歴でのイベントの表示」を参照してください。

Nimble Studio のイベントなど AWS アカウント、 のイベントの継続的な記録については、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きに、証跡がすべての AWS リージョンに適用されます。証跡は、 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ログに記録し、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、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動 AWS のサービス するように他の を設定できます。

詳細については、次を参照してください:

追跡を作成するための概要

「CloudTrail がサポートされているサービスと統合」

「CloudTrail の Amazon SNS 通知の設定」

CloudTrail ログファイルの複数のリージョンからの受け取り

複数のアカウントから CloudTrail ログファイルを受け取る

Nimble Studio のアクションは、CloudTrail によってログに記録されます。これらのドキュメントは、Amazon Nimble Studio の API リファレンスで参照できます。例えば、CreateStudio、GetStudio、DeleteStudio の各アクションを呼び出すと、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。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー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。
- 要求が、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 userIdentity エレメント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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。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、公開 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 の例は、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、リージョン、IP アドレス、およびイベントの識別に役立つ「userRoleArn」や「adminRoleArn」などの、その他の「requestParameters」がイベントに表示されていることがわかります。「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 は、アカウントの作成 AWS アカウント 時に 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、そのアクティビティはイベント履歴の他の AWS のサービス イベ

ントとともに CloudTrail 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 は、コンソールからの呼び出しや API コールなど、IAM および AWS Security Token Service（ AWS STS) 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。IAM およびでの CloudTrail の使用の詳細については AWS STS、「 での IAM および AWS STS API 呼び出しのログ記録 AWS CloudTrail」を参照してください。

CloudTrailの詳細については、「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 は責任共有モデルに従い、コンプライアンスは AWS とお客様の間で共有されます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによる対象範囲内コンプライアンス」を参照し、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、AWS「 Compliance ProgramsAssurance」を参照してください。

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

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、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS 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、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 AWS を にデプロイする手順を示します。
- アマゾン ウェブ サービスでの 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 AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべてが HIPAA 対応 AWS のサービス である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 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、お客様の業界と場所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。このガイドは、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を保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この 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 Config
- AWS Security Hub – これにより AWS のサービス 、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一覧については、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 – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、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、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と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

マネージドサービスである Amazon Nimble Studio は グローバル AWS ネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS 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。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 AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected フレームワーク」の「インフラストラクチャの保護」を参照してください。

AWS が公開した API コールを使用して、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 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。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適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

モニタリング

モニタリングは、Nimble Studio と AWS 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。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、 AWS アカウント 認証情報を保護し、 AWS Identity and Access Management (IAM) を使用して個々のアカウントを設定することをお勧めします。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 AWS リソースと通信します。TLS 1.2 以降が推奨されます。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。

- 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を使用します 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。
- 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。これは、コンソール、API、または SDK AWS のサービス を使用して Amazon Nimble Studio AWS CLIまたは他の を操作する場合も同様です。 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。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、IAM ロール、およびユーザーに最小限の権限を付与して、 AWS リソースへのアクセスを管理します。 AWS アクセス認証情報を作成、配布、ローテーション、および取り消すための認証情報管理ポリシーと手順を確立します。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。

内容

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。そこで、Nimble Studio の機能、技術的な問題、トラブルシューティングのヘルプについて、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。

サポート センター

サポート 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。請求および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動画、 AWS ドキュメント、トレーニングおよび認定など、さまざまなリソースにアクセスできます。

サポート プラン

サポート 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、コストの制御に役立ちます。 サポート プランの詳細については、サポート「プランの比較」を参照してください。

AWS がお客様をサポートする方法の詳細については、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
- ドキュメントの最終更新日: 2024 年 10 月 2 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	
サポート終了通知	サポート終了通知: 2024 年 10 月 22 日、 AWS は Amazon Nimble Studio のサポートを終了します。2024 年 10 月 22 日以降、Nimble Studio コンソールまたは Nimble Studio リソースにアクセスできなくなります。	2024 年 10 月 2 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
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 用語集

最新の AWS 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。