aws

管理者ガイド

Amazon WorkSpaces シンクライアント

Amazon WorkSpaces シンクライアント: 管理者ガイド

Table of Contents

Amazon WorkSpaces シンクライアント管理者コンソールとは

Amazon WorkSpaces シンクライアント管理者コンソールを使用すると、管理者は WorkSpaces シンクライアントポータルを通じて WorkSpaces シンクライアント環境とデバイスを管理できます。このウェブコンソールから、管理者はネットワーク内の WorkSpaces シンクライアントユーザーの環境の作成、デバイスの管理、パラメータの設定を行うことができます。

WorkSpaces シンクライアントに使用する仮想デスクトップ環境は、独自のコンソール内で作成または変更する必要があります。

> **Important**
>
> WorkSpaces シンクライアント管理者コンソールが正しく動作するためには、まずシステムが特定の要件を満たしている必要があります。これらの要件は、「前提条件」と「設定」に記載されています。

トピック

を初めてお使いになる方向けの情報

WorkSpaces シンクライアント管理者コンソールを初めて使用する場合は、まず以下のセクションを読むことをお勧めします。

アーキテクチャ

各 WorkSpaces シンクライアントは、仮想デスクトップインターフェイス (VDI) プロバイダーに関連付けられています。 WorkSpaces シンクライアントは 3 つの VDI プロバイダーをサポートしています。

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces Secure Browser

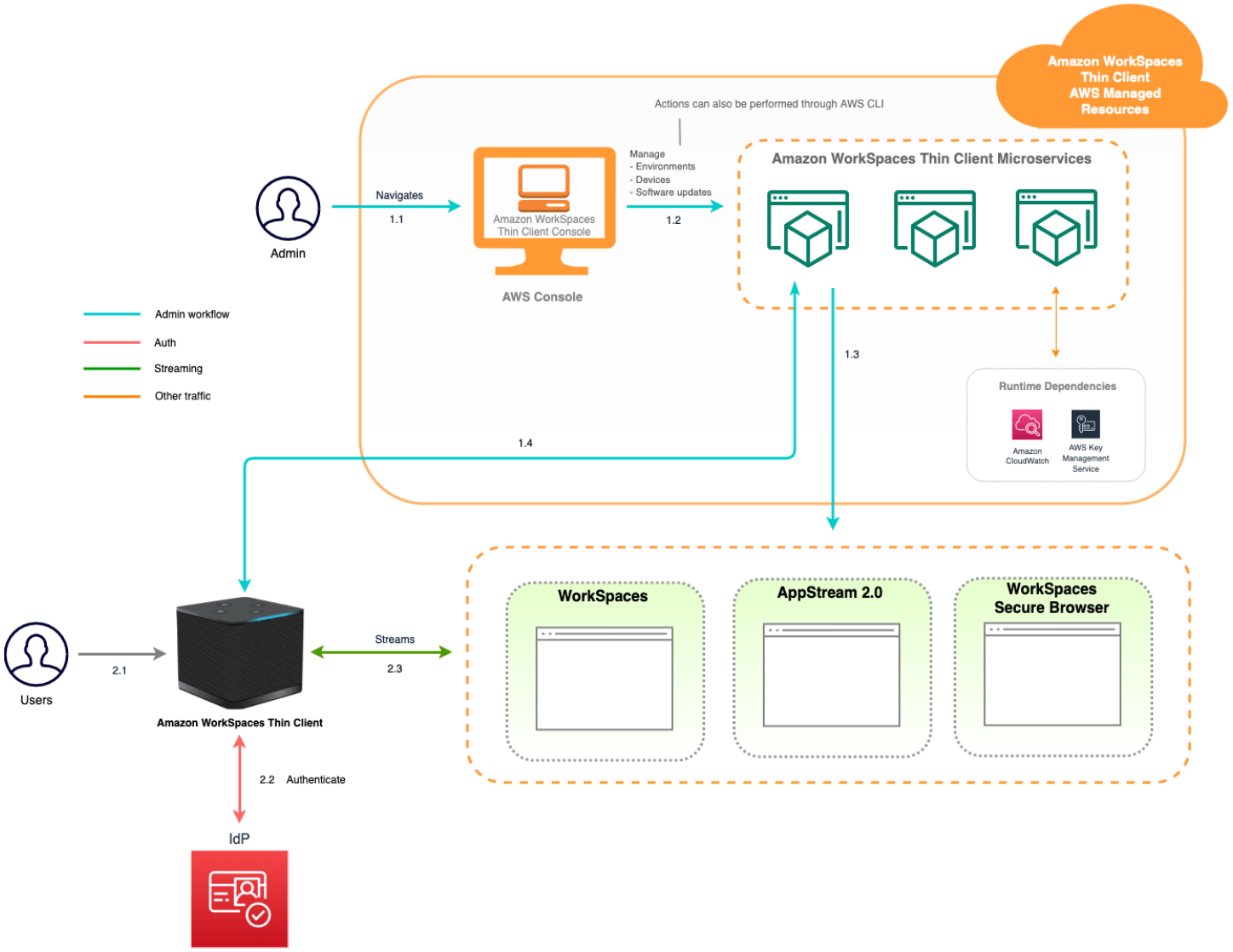
使用する VDI に応じて、 WorkSpaces シンクライアントの情報は、、 のディレクトリ WorkSpaces、 AppStream 2.0 のスタック、 WorkSpaces Secure Browser のウェブポータルエンドポイントのいずれかを介してアクセスおよび管理されます。

Amazon の詳細については WorkSpaces、 WorkSpaces 「クイックセットアップの開始方法」を参照してください。ディレクトリは、 を通じて管理されます。これは AWS Directory Service、Simple AD、AD Connector、または AWS Managed Microsoft AD とも呼ばれる Microsoft Active Directory AWS Directory Service 用のオプションを提供します。詳細については、AWS Directory Service 管理ガイドを参照してください。

AppStream 2.0 の詳細については、「Amazon AppStream 2.0 の開始方法: サンプルアプリケーションのセットアップ」を参照してください。 AppStream 2.0 は、アプリケーションのホストと実行に必要な AWS リソースを管理し、自動的にスケーリングし、オンデマンドでユーザーにアクセスできるようにします。 AppStream 2.0 は、ネイティブにインストールされたアプリケーションと区別できない応答的でスムーズなユーザーエクスペリエンスをユーザーに提供します。

WorkSpaces Secure Browser の詳細については、「Amazon WorkSpaces Secure Browser の開始方法」を参照してください。Amazon WorkSpaces Secure Browser は、内部ウェブサイトおよび software-as-a-service (SaaS) アプリケーションへの安全なブラウザアクセスを容易にするために設計された、オンデマンドのフルマネージド型 Linux ベースのサービスです。インフラストラクチャ管理、専用のクライアントソフトウェア、仮想プライベートネットワーク (VPN) ソリューションなど、管理上の負担がなく、既存のウェブブラウザからサービスにアクセスできます。

次の図は、 WorkSpaces シンクライアントのアーキテクチャを示しています。


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
Admin workflow
Auth
Streaming
Other traffic
1.4
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

Amazon WorkSpaces シンクライアント管理者コンソールのセットアップ

トピック

AWS にサインアップする

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。

IAM ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方法を 1 つ選択します	目的	方法	以下の操作も可能
IAM Identity Center 内 (推奨)	短期の認証情報を使用して AWSにアクセスします。 これはセキュリティのベストプラクティスと一致しています。ベストプラクティスの詳細については、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」を参照してください。	AWS IAM Identity Center ユーザーガイドの「開始方法」の手順に従います。	ユーザーガイド の を使用する AWS CLI ように を設定 AWS IAM Identity Centerして、プログラムによるアクセスを設定します。 AWS Command Line Interface
IAM 内 (非推奨)	長期認証情報を使用して AWSにアクセスする。	IAM ユーザーガイドの「最初の IAM 管理者のユーザーおよびグループの作成」の手順に従います。	IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」に従って、プログラムによるアクセスを設定します。

Amazon WorkSpaces シンクライアント用 VDI の開始方法

Amazon WorkSpaces シンクライアントは、 AWS エンドユーザーコンピューティングサービスと連携するように構築されたコスト効率の高いシンクライアントデバイスで、アプリケーションや仮想デスクトップに安全かつ瞬時にアクセスできます。

仮想デスクトップインフラストラクチャ (VDI) を選択し、 WorkSpaces シンクライアントで動作するように設定します。

> **Important**
>
> WorkSpaces シンクライアント管理者コンソールが正しく動作するためには、まずシステムが特定の要件を満たしている必要があります。これらの要件は、各仮想デスクトッププロバイダーの設定手順に記載されています。

WorkSpaces シンクライアントには、仮想デスクトッププロバイダーに応じて特定のソフトウェア設定が必要です。

トピック

- Amazon WorkSpaces シンクライアントの WorkSpaces の設定
- Amazon WorkSpaces シンクライアント用の AppStream 2.0 の設定
- Amazon WorkSpaces シンクライアントの Amazon WorkSpaces Secure Browser の設定

Amazon WorkSpaces シンクライアントの WorkSpaces の設定

WorkSpaces シンクライアントを Amazon で使用するには WorkSpaces、 WorkSpaces ディレクトリにアクセスするようにサービスを設定する必要があります。Amazon WorkSpaces は、 AWS コンソール内の WorkSpaces シンクライアント作成環境ページにディレクトリ名に基づいて一覧表示されます。

> **Note**
>
> コンソールを初めて使用する前に、設定を行う必要があります。コンソールの使用を開始した後に、前提条件となる機能を変更することはお勧めしません。

開始する前に

を作成または管理する AWS アカウントがあることを確認してください WorkSpace。ただし、デバイスユーザーは、 に接続して使用するために AWS アカウントを必要としません WorkSpaces。

設定に進む前に、次の概念を確認して理解してください。

- を起動するときに WorkSpace、 WorkSpace バンドルを選択します。詳細については、「Amazon WorkSpaces Bundles」を参照してください。
- を起動するときに WorkSpace、バンドルで使用するプロトコルを選択します。詳細については、「Amazon のプロトコル WorkSpaces」を参照してください。
- を起動するときは WorkSpace、ユーザー名や E メールアドレスなど、各ユーザーのプロファイル情報を指定します。ユーザーは、パスワードを作成してプロファイルを完了します。 WorkSpaces および ユーザーに関する情報は ディレクトリに保存されます。詳細については、「 のディレクトリを管理する WorkSpaces」を参照してください。
- を起動するときに WorkSpace、 WorkSpaces ウェブアクセスを有効にして設定します。詳細については、「Amazon WorkSpaces Web Access の有効化と設定」を参照してください。

ステップ 1: システムが WorkSpaces 必要な機能を満たしていることを確認する

WorkSpaces シンクライアント管理者コンソールが Amazon と適切に連携するには WorkSpaces、システムが以下の特定の要件を満たしている必要があります。この表には、サポートされているこれらの機能とその要件がすべて一覧表示されています。

機能	要件
Web Access	有効
サポートされるオペレーティングシステム	• Windows 10 • Windows 10 (Bring Your Own License) • Windows 11 • Windows 11 (Bring Your Own License)
サポート対象バンドル	• Microsoft Power with Windows 10 (Server 2016、2019、および 2022 ベース)

機能	要件
	• Microsoft Power with Windows 10 (Server 2016、2019、2022 ベース) w Office • Microsoft PowerPro with Windows 10 (Server 2016、2019、2022 ベース) • Microsoft PowerPro with Windows 10 (Server 2016、2019、2022 ベース) w Office • Windows 10 での Microsoft パフォーマンス (Server 2016、2019、2022 ベース) • Windows 10 (Server 2016、2019、2022 ベース) での Microsoft Performance w Office
サポートされるプロトコル	WSP のみ

ステップ 2: の詳細設定を使用して を起動する WorkSpace

詳細セットアップを使用して を起動するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. 次のいずれかのディレクトリタイプを選択してから、[Next] (次へ) をクリックします。
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. ディレクトリ情報の入力
4. 2 つの異なるアベイラビリティーゾーンのいずれかから VPC 内の 2 つのサブネットを選択します。詳細については、「パブリックサブネットを持つ VPC の設定」を参照してください。
5. ディレクトリ情報を確認し、ディレクトリの作成 を選択します。

Amazon WorkSpaces シンクライアント用の AppStream 2.0 の設定

AppStream 2.0 インスタンスはスタック名に基づいてリストされ、環境の作成ページで IdP ログイン URL を設定する必要があります。 AppStream 2.0 の SAML 認証は開始された認証のみをサポートするため、管理者は正しいログイン URL を手動で入力する必要があります。

> **Note**
>
> コンソールを初めて使用する前に、設定を行う必要があります。コンソールの使用を開始した後に、前提条件となる機能を変更することはお勧めしません。

ステップ 1: システムが AppStream 2.0 の必須機能を満たしていることを確認する

WorkSpaces シンクライアント管理者コンソールで AppStream 2.0 を適切に動作させるには、システムが以下の特定の要件を満たしている必要があります。この表には、サポートされているこれらの機能とその要件がすべて一覧表示されています。

機能	要件
ID プロバイダー	AppStream 2.0 管理者ガイドの「SAML のセットアップ」に移動して、ID プロバイダーを作成します。 環境コンソール を作成するように求められたら、IDP ログイン URL を入力します。
オペレーティングシステム	Windows
プラットフォームの種類	Windows Server (2012 R2、2016 または 2019)
ストリーミングプロトコル	TCP ストリーミング UDP が利用できない場合は TCP に戻ります。
フローのコピーと貼り付け	[無効]

機能	要件
	AppStream 2.0 スタックレベルで設定
ローカルフォルダー共有	[無効] AppStream 2.0 スタックレベルで設定
ローカルプリント	[無効] AppStream 2.0 スタックレベルで設定

AppStream 2.0 での SAML 認証による画面ロック要件もサポートされています。ユーザープールとプログラムによる認証メカニズムは、 WorkSpaces シンクライアントではサポートされていません。

ステップ 2: AppStream 2.0 スタックを設定する

アプリケーションをストリーミングするには、 AppStream 2.0 には、スタックに関連付けられたフリートと、少なくとも 1 つのアプリケーションイメージを含む環境が必要です。フリートとスタックを設定し、ユーザーにスタックへのアクセスを許可するには、次の手順に従います。まだ行っていない場合は、「Get Started with AppStream 2.0: Set Up with Sample Applications」の手順を実行することをお勧めします。

使用するイメージを作成する場合は、「チュートリアル: AppStream 2.0 コンソールを使用してカスタム AppStream 2.0 イメージを作成する」を参照してください。

フリートを Active Directory ドメインに結合する場合は、Active Directory ドメインを設定してから、以下のステップを行ってください。詳細については、「 AppStream 2.0 での Active Directory の使用」を参照してください。

タスク

- フリートを作成する
- スタックを作成する
- ユーザーへアクセスを提供する
- リソースのクリーンアップ

Amazon WorkSpaces シンクライアントの Amazon WorkSpaces Secure Browser の設定

Amazon WorkSpaces Secure Browser は、 AWS コンソール内の WorkSpaces シンクライアント作成環境ページにあるウェブポータルエンドポイントに基づいています。

> **Note**
>
> コンソールを初めて使用する前に、設定を行う必要があります。コンソールの使用を開始した後に、前提条件となる機能を変更することはお勧めしません。

ステップ 1: システムが Amazon WorkSpaces Secure Browser の必須機能を満たしていることを確認する

WorkSpaces シンクライアント管理者コンソールが Amazon WorkSpaces Secure Browser と適切に連携するには、システムが以下の特定の要件を満たしている必要があります。この表には、サポートされているこれらの機能とその要件がすべて一覧表示されています。

機能	要件
フローのコピーと貼り付け	[無効]
ローカルフォルダー共有	[無効]

> **Note**
>
> シングルサインオン用の WorkSpaces Secure Browser 拡張機能は、現在 WorkSpaces シンクライアントではサポートされていません。

ステップ 2: WorkSpaces Secure Browser ポータルを設定する

WorkSpaces シンクライアントは、特定の設定で WorkSpaces Secure Browser VPC と連携します。

1. Cloudformation テンプレート を使用して VPC を作成します。 AWS CodeBuild

2. ID プロバイダーをセットアップします。
3. Amazon WorkSpaces Secure Browser ポータルを作成します。
4. 新しい Amazon WorkSpaces Secure Browser ポータルをテストします。

WorkSpaces シンクライアント管理者コンソールの起動

WorkSpaces シンクライアントは、 AWS エンドユーザーコンピューティングサービスと連携するように構築されたコスト効率の高いシンクライアントデバイスで、アプリケーションや仮想デスクトップへの安全で即時のアクセスを提供します。

トピック

対象地域

WorkSpaces シンクライアントは、次のリージョンで使用できます。

これらのリージョンでは、 WorkSpaces シンクライアント管理者コンソールのみを使用できます。 WorkSpaces シンクライアントデバイスは、現在、米国、ドイツ、フランス、イタリア、スペインでのみ使用できます。

リージョン名	リージョン	エンドポイント	コンソールリンク
米国東部 (バージニア北部)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
米国西部 (オレゴン)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
アジアパシフィック (ムンバイ)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

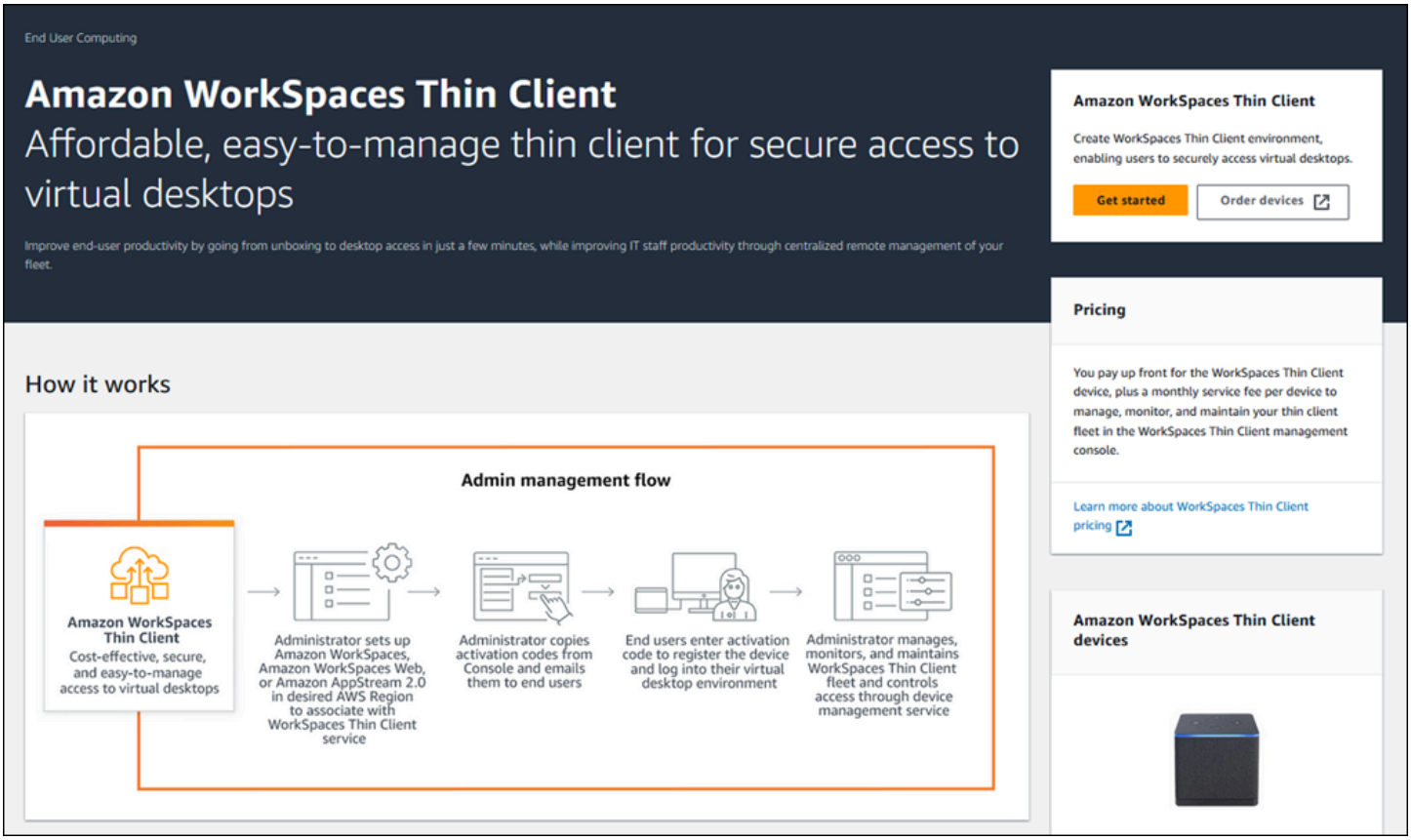
リージョン名	リージョン	エンドポイント	コンソールリンク
欧州 (アイルランド)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
カナダ (中部)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧州 (フランクフルト)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧州 (ロンドン)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

WorkSpaces シンクライアント管理者コンソールの起動

AWS アカウントがあれば、管理者コンソールを起動して WorkSpaces シンクライアントコンソールに移動できます。コンソールを起動するには、次の手順を実行します。

1. AWS アカウントにログオンします。
2. WorkSpaces シンクライアントコンソール にアクセスします。
3. [はじめに] を選択すると、[環境] に移動します。

WorkSpaces シンクライアント管理者コンソールの使用



WorkSpaces シンクライアント管理者コンソールへようこそ。

ここから、チームの WorkSpaces シンクライアントデバイスと環境のフリートを管理できます。

WorkSpaces シンクライアントデバイスの詳細については、WorkSpaces シンクライアントユーザーガイドを参照してください。

では、始めましょう。

トピック

- 環境
- デバイス
- ソフトウェアの更新

環境

各 WorkSpaces シンクライアントデバイスは、個々の仮想デスクトップ環境を使用してオンラインリソースにアクセスします。ユーザーは、次のいずれかの仮想デスクトッププロバイダーを使用してこの環境にアクセスします。

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces Secure Browser

環境リスト

環境リストの詳細

[名前] - この環境に関連付けられた一意の識別子。

[仮想デスクトップサービス] - この環境が使用する仮想デスクトッププロバイダー。

仮想デスクトップサービス ID - 仮想デスクトップサービスプロバイダーがこの環境に割り当てる一意の識別子。

アクティベーションコード - エンドユーザーが仮想デスクトップ環境にアクセスするために使用するコード。

デバイス数 - この環境にアクセスしている WorkSpaces シンクライアントデバイスの数。

環境リストアクション

[検索] - 管理しているすべての環境を検索します。

[更新] - 環境リストを更新します。

[詳細を表示] - 環境の詳細を表示します。

アクション - ???環境を編集または削除できるドロップダウンリストを開きます。

[環境を作成] - 環境を作成するプロセスを開始します。

[環境を作成] - 環境を作成するプロセスを開始します。

トピック

環境の詳細

環境を選択すると、 WorkSpaces シンクライアントコンソールにその環境の詳細が表示され、確認できるようになります。コンソールには、この環境が使用する仮想デスクトッププロバイダーの詳細も表示されます。

トピック

[概要]

[名前] - この環境に関連付けられた一意の識別子。

[仮想デスクトップサービス] - この環境が使用する仮想デスクトッププロバイダー。

仮想デスクトップサービス ID - 仮想デスクトップサービスプロバイダーがこの環境に割り当てる一意の識別子。

[アクティベーションコード] - エンドユーザーが仮想デスクトップ環境にアクセスする際に使用するコードです。

常にソフトウェアを保持する up-to-date - この設定では、ソフトウェアの自動更新を有効にします。

メンテナンスウィンドウの開始時刻 - 自動ソフトウェア更新が開始される毎週の時刻。

メンテナンスウィンドウの終了時刻 - 自動ソフトウェア更新が終了した毎週の時刻。

[メンテナンスウィンドウの曜日] - ソフトウェアの自動更新が行われる日。

関連付けられたデバイス - この環境にアクセスしている WorkSpaces シンクライアントデバイスの数。

作成日時 - この環境が作成された日時。

仮想デスクトップ環境の詳細

Amazon WorkSpaces ディレクトリの詳細

ディレクトリ ID - この環境に関連付けられている Amazon WorkSpaces ディレクトリ。

ディレクトリ名 - この Amazon WorkSpaces ディレクトリに関連付けられた一意の識別子。

組織名 - Amazon WorkSpaces ディレクトリを制御する組織の名前。

ディレクトリタイプ - Amazon WorkSpaces ディレクトリの形式。

登録済み - この Amazon WorkSpaces ディレクトリが登録されているかどうかを示します。

ステータス - この Amazon WorkSpaces ディレクトリがアクティブかどうか。

Amazon WorkSpaces Secure Browser ポータルの詳細

名前 - この Amazon WorkSpaces Secure Browser ポータルに関連付けられた一意の識別子。

作成日時 - この AppStream 2.0 スタックが作成された日時。

[Web ポータルエンドポイント] - 仮想デスクトップ環境へのアクセスに使用される URL。

AppStream 2.0 の詳細

スタック名 - この AppStream 2.0 スタックに関連付けられた一意の識別子。

IdP ログイン URL - AppStream 2.0 スタックのログインとログアウトに使用される ID プロバイダー URL。

作成日時 - この AppStream 2.0 スタックが作成された日時。

環境を作成する

開始するには、各デバイスに AWS エンドユーザーコンピューティングサービスが必要です。WorkSpaces Thin Client は次のサービスを使用します。

- 割り当てられたディレクトリ WorkSpaces を介した Amazon
- AppStream 割り当てられたスタックを介した 2.0

- ウェブポータルアドレスを介した Amazon WorkSpaces Secure Browser

既存の環境にサービスを割り当てるか、新しい環境を作成する必要があります。

> **Note**
>
> WorkSpaces シンクライアントは、同じリージョン内の仮想デスクトップのみを表示します。

トピック

ステップ 1: 環境の詳細を入力する

1. [環境の詳細] フィールドに環境の名前を入力します。
2. 自動ソフトウェアパッチを設定するには、「常にソフトウェアを保持する up-to-date」のチェックボックスをオンにします。

   > **Note**
   >
   > 自動ソフトウェア更新が有効になっていない場合、この環境に登録されているデバイスは、手動で更新をプッシュするか、ソフトウェアの有効期限が切れてシステムが強制的に更新するまで、ソフトウェア更新を受信しません。
   > また、デバイスのソフトウェアセットのバージョンはシステムによって決まります。このバージョンは最新のバージョンではない場合があります。

3. 環境のメンテナンスウィンドウをスケジュールするタイミングを選択します。
   - システム全体のメンテナンスウィンドウを適用する - 毎週決められた時間に環境ソフトウェアを自動的に更新します。
   - [カスタムメンテナンスウィンドウを適用] - 環境ソフトウェアを毎週更新したい日時を設定します。
4. 仮想デスクトップサービスを選択します。

- Amazon WorkSpaces
- Amazon WorkSpaces Secure Browser
- AppStream 2.0

ステップ 2: 仮想デスクトッププロバイダを選択する

ユーザーに仮想デスクトップと互換性のあるリソースへのアクセスを提供するサービスが必要です。

> **Important**
>
> WorkSpaces シンクライアント管理者コンソールが正しく動作するためには、システムが特定の要件を満たしている必要があります。これらの要件は、「前提条件」と「設定」に記載されています。
> コンソールを設定する前に、システムがこれらの要件を満たしていることを確認してください。

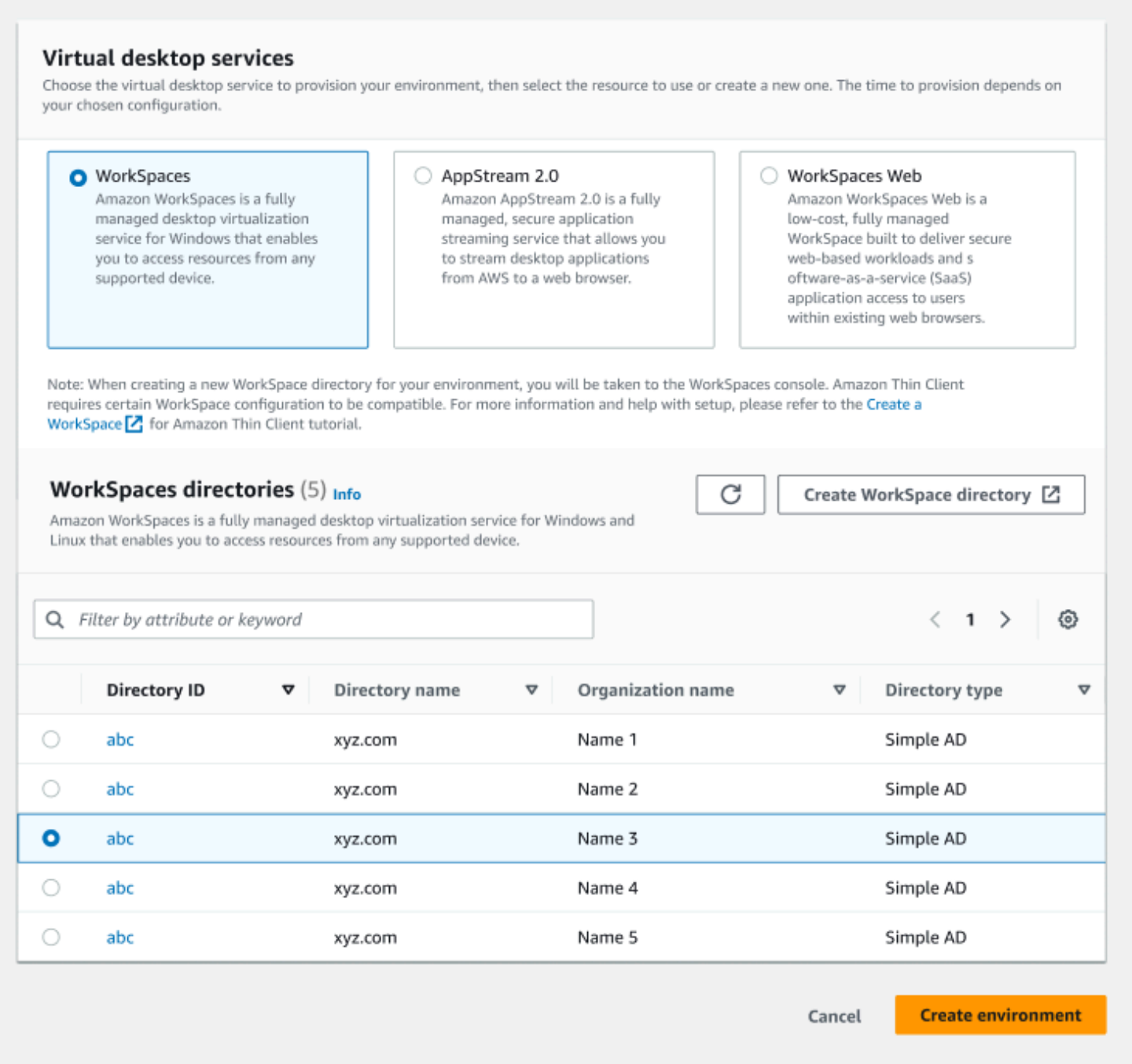
Amazon の使用 WorkSpaces

Amazon WorkSpaces は Windows 用のフルマネージドデスクトップ仮想化サービスで、サポートされている任意のデバイスから リソースにアクセスできます。

1. Amazon を使用するには WorkSpaces、次のいずれかを実行します。
   - ご使用の環境に合わせて使用したいディレクトリを選択してください。ドロップダウンリストを参照するか、検索フィールドを使用してディレクトリを検索できます。

     > **Note**
     >
     > 既存のディレクトリがリストに表示されない場合は、 WorkSpaces マネジメントコンソールで、それが WorkSpaces シンクライアント要件 を満たしていることを確認します。

   - ディレクトリの作成 ボタンを選択して、 WorkSpaces ディレクトリを作成します。 WorkSpaces ディレクトリの作成の詳細については、「 のディレクトリの管理 WorkSpaces」を参照してください。
2. 環境の作成ボタンを選択します。



環境を作成する場合でも、後で詳細を編集できます。詳細については、「環境を編集する」を参照してください。

AppStream 2.0 の使用

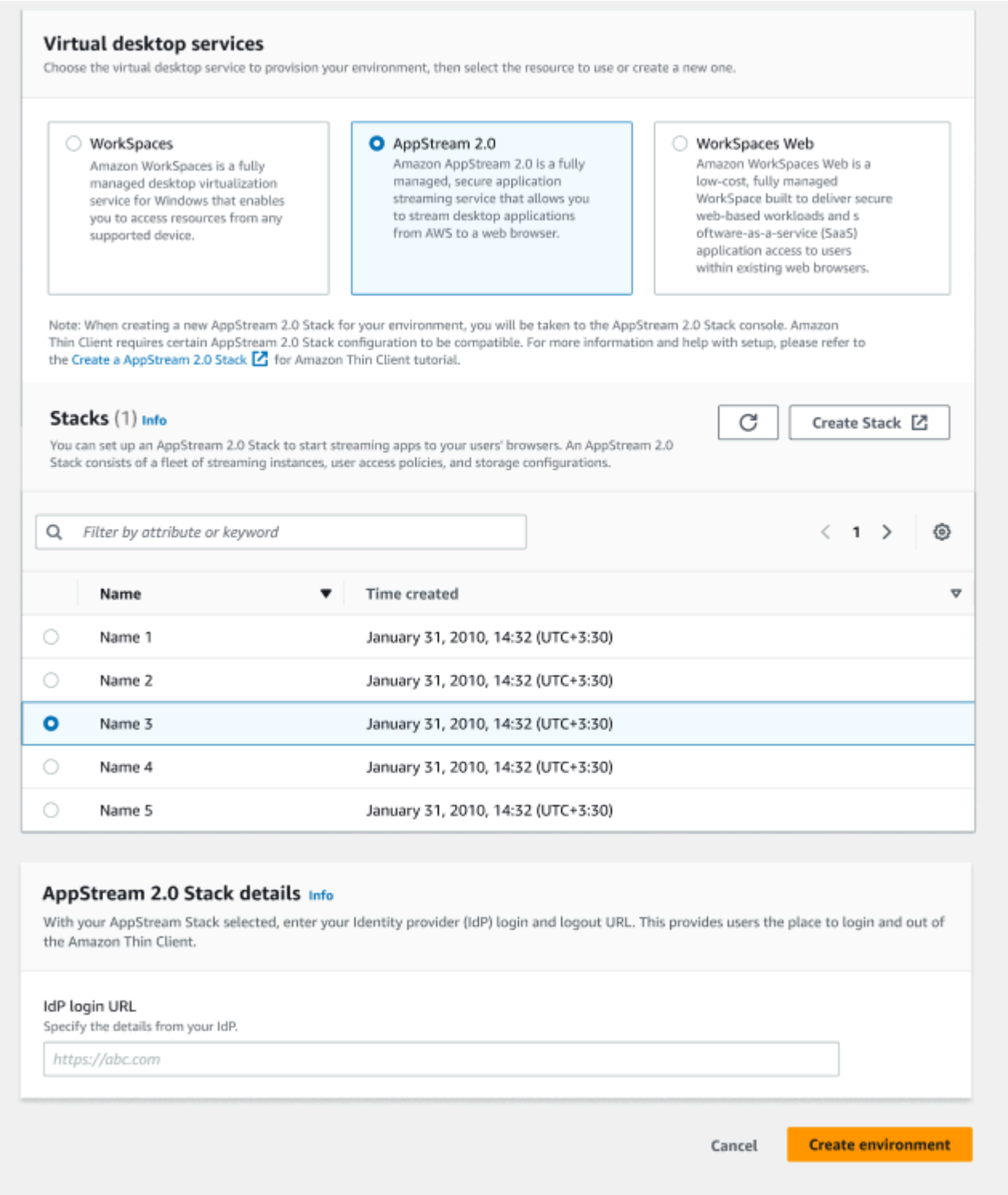
AppStream 2.0 は、デスクトップアプリケーションを からウェブブラウザにストリーミングするために使用できる、フルマネージド AWS 型の安全なアプリケーションストリーミングサービスです。

> **Warning**
>
> AppStream 2.0 環境を作成するには、 を `cli_follow_urlparam`に設定する必要がありますfalse。これを達成するには、次の操作を行います。
>
> - 既定のプロファイルでは、`aws configure set cli_follow_urlparam false` を実行します。
> - `ProfileName` という名前の付いたプロファイルの場合は、`aws configure set cli_follow_urlparam false --profile ProfileName` を実行してください。

1. AppStream 2.0 を設定するには、次のいずれかを実行します。
   - ご使用の環境に合わせて使用したいスタックを選択してください。ドロップダウンリストを参照するか、検索フィールドを使用してスタックを検索できます。

     > **Note**
     >
     > 既存のスタックがリストに表示されない場合は、 AppStream 2.0 マネジメントコンソールで WorkSpaces シンクライアント要件 を満たしていることを確認します。

   - スタックの作成 ボタンを選択してスタックを作成します。 AppStream 2.0 スタックの作成の詳細については、「スタックの作成」を参照してください。
2. ID プロバイダのログインとログアウト URL を [IdP ログイン URL] フィールドに入力します。これにより、ユーザーは WorkSpaces シンクライアントにログインおよびログアウトできます。
3. 環境の作成ボタンを選択します。



環境を作成した後でも、後で詳細を編集できます。詳細については、「環境を編集する」を参照してください。

Amazon WorkSpaces Secure Browser の使用

Amazon WorkSpaces Secure Browser は、既存のウェブブラウザ内のユーザーに安全なウェブベースのワークロードと Software as a Service (SaaS) アプリケーションアクセスを提供するように構築された、低コストのフルマネージド WorkSpaces コンソールです。

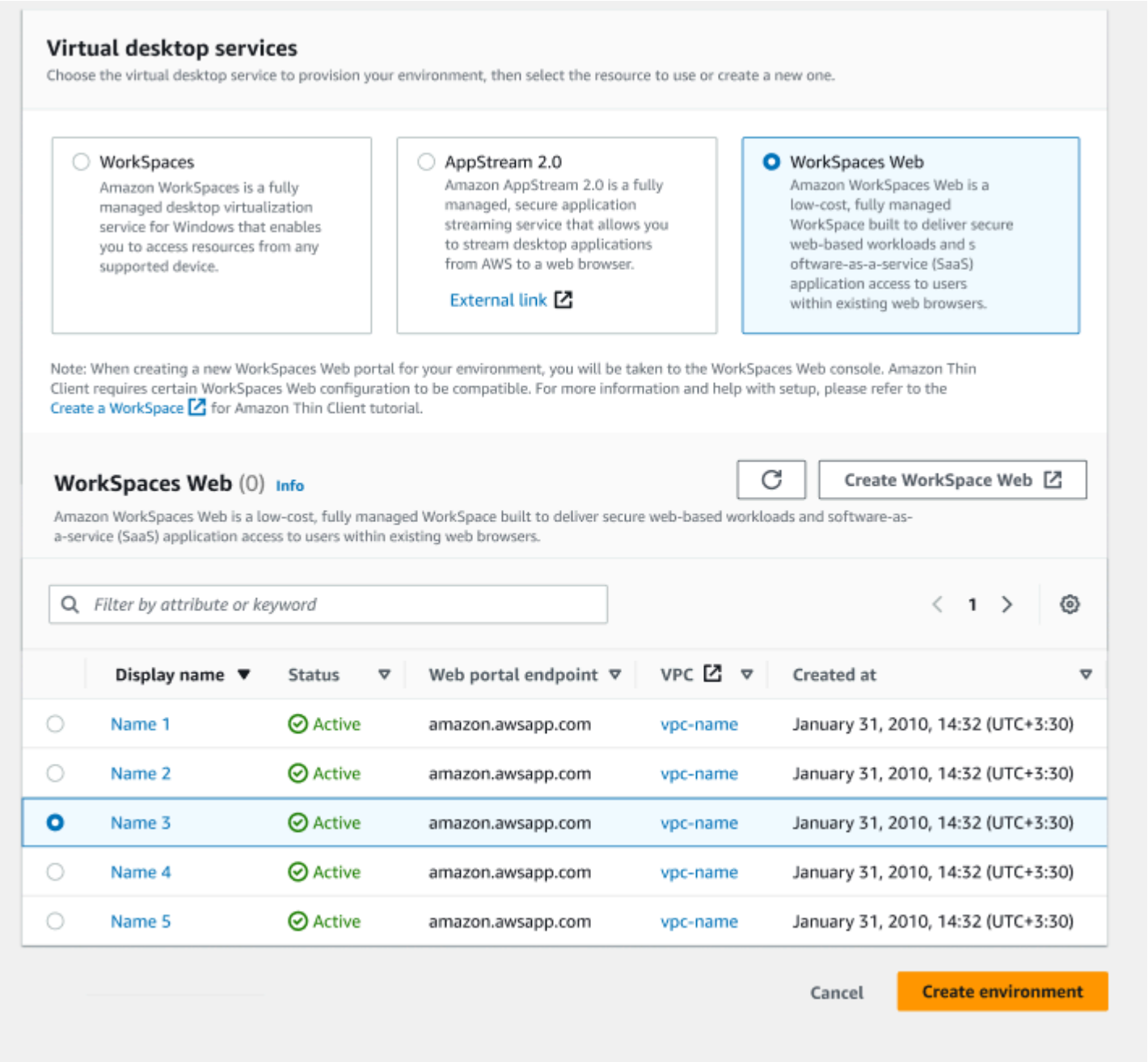
1. Amazon WorkSpaces Secure Browser を設定するには、次のいずれかを実行します。

   - 環境に使用するウェブポータルを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してウェブポータルを検索できます。

     > **Note**
     >
     > 既存のウェブポータルがリストに表示されない場合は、 WorkSpaces Secure Browser Management Console で、それが WorkSpaces シンクライアント要件 を満たしていることを確認します。

   - WorkSpaces セキュアブラウザの作成 ボタンを選択して、ウェブポータルを作成します。 WorkSpaces Secure Browser ウェブポータルの作成の詳細については、「Amazon WorkSpaces Secure Browser のセットアップ」を参照してください。

2. 環境の作成ボタンを選択します。



環境を作成した後でも、後で詳細を編集できます。詳細については、「環境を編集する」を参照してください。

ステップ 3: デバイスユーザーにアクティベーションコードを送信する

環境と仮想デスクトップサービスを設定すると、 AWS マネジメントコンソールでセットアップ用の一意のアクティベーションコードを受け取ります。

このアクティベーションコードを WorkSpaces シンクライアントデバイスユーザーに提供すると、ユーザーはこれを使用して仮想デスクトップにアクセスできます。

デバイスユーザーが Amazon WorkSpaces シンクライアントをセットアップするのに役立つ方法の詳細については、シンクライアントユーザーガイドを参照してください。 WorkSpaces

環境を編集する

WorkSpaces シンクライアント管理コンソールは、個々のユーザーの仮想デスクトップ環境を管理します。このコンソールから、仮想デスクトップ環境を編集または削除できます。

1. 編集する環境を選択します。

> **Note**
>
> ドロップダウンリストを参照するか、検索フィールドを使用して環境を検索できます。

2. アクションボタンを選択します。
3. ドロップダウンリストから編集を選択します。環境の編集ウィンドウが表示されます。
4. 次のいずれかを編集します。
   - [環境名] フィールドで環境の名前を変更します。
   - 自動ソフトウェアパッチ更新のソフトウェア更新の詳細のチェックボックスを変更します。
   - 環境に合わせてメンテナンスウィンドウをスケジュールするタイミングを変更します。
5. 環境の編集ボタンを選択します。

環境を削除する

> **Note**
>
> デバイスが登録されている環境は削除できません。まず、環境内のすべてのデバイスを登録解除して削除する必要があります。

1. 削除する環境を選択します。ドロップダウンリストを参照するか、検索フィールドを使用して環境を検索できます。
2. アクションボタンを選択します。

3. ドロップダウンリストから削除を選択します。環境の削除の確認ウィンドウが表示されます。
4. 確認ダイアログで、[Delete] (消去) と入力します。
5. [削除] ボタンを選択します。

デバイス

各 WorkSpaces シンクライアントエンドユーザーには、仮想デスクトップ環境とオンラインリソースに接続する専用デバイスがあります。これらのデバイスは、AWS サイト の WorkSpaces シンクライアント管理者コンソールを介して管理されます。

このコンソールから、チーム用のデバイスを注文できます。

デバイスリスト

デバイスリストの詳細

[デバイス ID] - 個々のデバイスに割り当てられる ID 番号。

デバイス名 - (オプション) デバイスに提供する一意の名前。

アクティビティステータス - デバイスの現在のステータス。ステータスには 2 つの状態があります。

- [アクティブ] - 過去 7 日間に少なくとも 1 回ネットワークに接続しています。
- [非アクティブ] - 過去 7 日間に少なくとも 1 回ネットワークに接続していません。

登録ステータス - デバイスがセットアップされ、この AWS アカウントに関連付けられ、特定の環境の一部であることの確認。次のいずれかの状態になります。

- 登録済み - これはデフォルトのステータスです。
- 登録解除中 - デバイスはリセットおよび登録解除プロセス中です。

> **Note**
>
> 登録解除状態にあるデバイスは削除できます。

- [登録解除] - デバイスは正常に登録解除されました。

> **Note**
>
> デバイスを削除できるのは、登録解除ステータスまたは登録解除ステータスの場合のみです。

- [アーカイブ済み] - デバイスはアーカイブされています。

[環境 ID] - このデバイスが接続されている環境の識別子。

[ソフトウェアコンプライアンス] - デバイスソフトウェアのコンプライアンスステータス。ステータスには 2 つの状態があります。

- 準拠
- 非準拠

デバイスリストのアクション

[検索] - 管理しているすべてのデバイスを検索します。

[更新] - デバイスリストを更新します。

[詳細を表示] - デバイスの詳細を表示します。

アクション - ドロップダウンリストを開き、次の操作を実行できます。

- デバイス名の編集
- 登録解除
- アーカイブ
- 削除
- デバイスの詳細を検索

[デバイスの注文] - デバイスの注文プロセスを開始します。

トピック

- デバイスの詳細
- デバイス名の編集
- デバイスのリセットと登録解除

- デバイスのアーカイブ
- デバイスの削除
- デバイスの詳細を検索

デバイスの詳細

[概要]

デバイスのシリアル番号 - 個々のデバイスに割り当てられた識別番号。

ARN - Amazon リソースネーム (ARN) 形式のデバイスの一意の識別子。

デバイス名 - デバイスに提供する名前。名前を作成していない場合は、名前を付けることができます。そうしないと、デフォルトの名前が付けられます。

デバイスタイプ - アカウントにリンクされているエンドユーザーデバイスのタイプ。

[アクティビティステータス] - このデバイスの現在のステータス。2 つのステータス状態は次のとおりです。

- [アクティブ]
- 無効

環境 ID - デバイスが使用する環境の識別番号。

登録ステータス - デバイスがセットアップされ、この AWS アカウントに関連付けられ、特定の環境の一部であることの確認。次の 4 つの状態のいずれかになります。

- 登録済み - これはデフォルトのステータスです。
- 登録解除中 - デバイスはリセットおよび登録解除プロセス中です。
- [登録解除] - デバイスは正常に登録解除されました。

> **Note**
>
> デバイスを削除できるのは、登録解除ステータスまたはアーカイブステータスのいずれかの場合のみです。

- アーカイブ済み - このデバイスは、管理者によって現在稼働していないとマークされています。

[登録日時] - デバイスがアクティベーションされた日付。

[最終ログイン] - 最新のログイン日時。

最終体制チェック日時 - 最新のデバイスチェックインの日時。

[現在のソフトウェアバージョン] - このデバイスが現在使用しているソフトウェアバージョン。

ソフトウェア更新の予定 - デバイスのスケジュールされたソフトウェアバージョン。

[ソフトウェアコンプライアンス] - ソフトウェアセットが有効であることの確認。ステータスには 2 つの状態があります。

- 準拠
- 非準拠

ユーザーログ

最後のデバイスアクセス - このデバイスが最後に使用された日時。

デバイス名の編集

1. 編集するデバイスを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してデバイスを検索できます。
2. アクションボタンを選択します。
3. ドロップダウンリストからデバイス名の編集を選択します。デバイス名の編集ウィンドウが表示されます。
4. [デバイス名] 確認フィールドに新しいデバイス名を入力します。
5. [保存] ボタンを選択します。

デバイスのリセットと登録解除

1. 登録するデバイスを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してデバイスを検索できます。
2. アクションボタンを選択します。
3. ドロップダウンリストから登録解除を選択します。登録解除ウィンドウが表示されます。
4. 確認フィールドに「deregister」と入力します。
5. [登録解除] ボタンを選択します。

> **Note**
>
> 登録解除すると、ユーザーは強制的にログアウトされ、セッション中に WorkSpaces シンクライアントデバイスの再起動が必要になります。

デバイスのアーカイブ

1. アーカイブするデバイスを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してデバイスを検索できます。
2. アクションボタンを選択します。
3. ドロップダウンリストからアーカイブを選択します。アーカイブウィンドウが表示されます。
4. 確認フィールドに「reset and archive」と入力します。
5. [リセットしてアーカイブ] ボタンを選択します。

> **Note**
>
> デバイスをアーカイブすると、ユーザーを強制的にログアウトし、セッション中に WorkSpaces シンクライアントデバイスの再起動が必要になります。

デバイスの削除

1. 削除するデバイスを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してデバイスを検索できます。
2. アクションボタンを選択します。
3. ドロップダウンリストから削除を選択します。削除ウィンドウが表示されます。
4. 確認ダイアログで、[Delete] (消去) を選択します。
5. [削除] ボタンを選択します。

> **Note**
>
> デバイスが正常に削除されたら、ユーザーは WorkSpaces シンクライアントデバイスを Amazon に戻す必要があります。

デバイスの詳細を検索

1. 詳細をエクスポートするデバイスを選択します。ドロップダウンリストを参照するか、検索フィールドを使用してデバイスを検索できます。
2. アクションボタンを選択します。
3. ドロップダウンリストからデバイスの詳細のエクスポートを選択します。選択したデバイスの詳細をスプレッドシート形式でダウンロードします。

ソフトウェアの更新

WorkSpaces シンクライアントでは、新機能を導入し、セキュリティパッチを適用するソフトウェア更新が必要になる場合があります。これらの更新は、バージョニングされたソフトウェアセット によって表されます。

ソフトウェアセットには、 WorkSpaces シンクライアントデバイスのソフトウェアアプリケーションまたはオペレーティングシステムの更新を含めることができます。このコンソールから、ソフトウェアをすぐに更新するか、環境のメンテナンスウィンドウ中に自動更新をスケジュールするかを選択できます。

リリースされた WorkSpaces ソフトウェアセットのリストについては、シンクライアント環境ソフトウェアセットを参照してください。

トピック

- サービスソフトウェアの更新
- デバイスソフトウェアの更新
- WorkSpaces シンクライアントソフトウェアリリース

サービスソフトウェアの更新

WorkSpaces シンクライアントは、ユーザーが仮想デスクトップにアクセスできるようにする AWS エンドユーザーコンピューティングサービスです。これらの仮想デスクトップは、新しいソフトウェアセットで定期的に更新されます。環境ソフトウェアを更新するには、次の手順を実行します。

1. [利用可能なソフトウェア更新] のリストからソフトウェアセットを選択します。ソフトウェアセットのリストについては、WorkSpaces「シンクライアント環境ソフトウェアセット」を参照してください。

2. インストールボタンを選択します。
3. ページの上部で [環境] を選択します。
4. 環境セクションのリストから、更新する環境を選択します。
5. [更新をスケジュールする] で次のいずれかを選択して、環境を更新するタイミングを選択します。

   - [今すぐソフトウェアを更新] - 登録されているすべてのデバイスで環境ソフトウェアの更新を開始します。

     > **Note**
     >
     > ソフトウェアを更新すると、アクティブなユーザーセッションが中断される可能性があります。

   - 各環境のメンテナンスウィンドウ中にソフトウェアを更新する - 環境のスケジュールされたメンテナンスウィンドウ中に環境ソフトウェアを更新します。
6. このチェックボックスをオンにすると、更新が承認されます。ソフトウェアをアップデートするには、このボックスにチェックを入れる必要があります。
7. インストールボタンを選択します。

デバイスソフトウェアの更新

WorkSpaces シンクライアントは、ユーザーを専用の仮想デスクトップに接続するシンクライアントデバイスを提供する AWS エンドユーザーコンピューティングサービスです。これらのデバイスは、新しいソフトウェアで定期的に更新されます。デバイスソフトウェアを更新するには、次の手順を実行します。

1. [利用可能なソフトウェア更新] のリストからソフトウェアセットを選択します。
2. インストールボタンを選択します。
3. ページの上部で、[削除] を選択します。
4. デバイスセクションのリストから、更新するデバイスを選択します。ソフトウェアセットのリストについては、WorkSpaces「シンクライアント環境ソフトウェアセット」を参照してください。
5. [更新をスケジュールする] オプションで次のいずれかを選択して、環境を更新するタイミングを選択します。

- [今すぐソフトウェアを更新] - デバイスソフトウェアをただちに更新します。

> **Note**
>
> ここでソフトウェアを更新すると、アクティブなユーザーセッションが中断される可能性があります。

- 各デバイスのメンテナンスウィンドウ中にソフトウェアを更新する - デバイスのスケジュールされたメンテナンスウィンドウ中に環境ソフトウェアを更新します。

6. このチェックボックスをオンにすると、更新が承認されます。ソフトウェアをアップデートするには、このボックスにチェックを入れる必要があります。
7. インストールボタンを選択します。

WorkSpaces シンクライアントソフトウェアリリース

WorkSpaces シンクライアントは、デバイス上の仮想デスクトップへのアクセスをユーザーに許可する AWS エンドユーザーコンピューティングサービスです。これらのデバイスは、新しいソフトウェアセットで定期的に更新されます。次の表に、リリースされたすべてのソフトウェアセットを示します。管理者は、 AWS マネジメントコンソールを使用して、使用可能なソフトウェアセットを表示できます。

ソフトウェアセット	リリース日	変更
2.5.0	06-13-2024	• セッションを開始する前にスリープ状態から目覚めると、デバイスがキーボードとマウスのセットアップ画面を短時間表示していた問題を修正しました。 • デバイスツールバーのホームボタンの名前がサインイン に変更されました。 • セッションでのオーディオ/ビデオ通話のパフォーマンスが向上しました。

ソフトウェアセット	リリース日	変更
2.4.3	05-29-2024	• Chromium の CVE-2024-5274 の重要なセキュリティ問題に対するゼロデイ修正。
2.4.2	05-17-2024	• Chromium の CVE-2024-4947 の重要なセキュリティ問題に対するゼロデイ修正。
2.4.1	05-15-2024	• Chromium の CVE-2024-4671 および CVE-2024-4761 の重要なセキュリティ問題に対するゼロデイ修正。 • WorkSpaces サインインページで AWS とプライバシーのリンクを右クリックして、スタンドアロンモードでブラウザを開くことができる問題を修正しました。
2.4.0	05-09-2024	• accounts.google.com」をブロックし、Google Workspace を AppStream 2.0 セッションの IDP として使用できない問題を修正しました。 • デバイス設定ツールバーは、画面上の任意のエリアをクリックすると自動的に折りたたまれます。

ソフトウェアセット	リリース日	変更
2.3.0	04-05-2024	• デバイス設定は折りたたまれたツールバーに表示されるため、表示画面の使用率が高くなります。 • エンドユーザーは、デバイスが非アクティブ状態でスリープするまでの待機時間を設定できるようになりました。 • 2 番目のディスプレイに「about:blank」URL が表示される問題を修正しました。 • 拡張ディスプレイが閉じられたときに白画面が表示される問題を修正しました。 • エンドユーザーが設定したボリュームレベルは、デバイスの再起動後も維持されるようになりました。
2.2.1	02-16-2024	• サインインプロセス中に、ユーザーが SAML 2.0 認証で WorkSpaces 設定されたにログインできない問題を修正しました。
2.2.0	02-08-2024	• 英語 (英国) 、フランス語、ドイツ語、イタリア語、スペイン語の口ケールを持つ ISO キーボードのサポートが追加されました。

ソフトウェアセット	リリース日	変更
2.1.2	01-26-2024	• Chromium の CVE-2024-0519 の重要なセキュリティ問題に対するゼロデイ修正。 • ロック機能に関連するエンドユーザーのレイテンシーを改善しました。 • 内部デバイス向けエンドポイントは「thinclient*」ドメインに切り替えられます。
2.1.1	12-21-2023	• Chromium の CVE-2023-7024 の重要なセキュリティ問題に対するゼロデイ修正。
2.1.0	12-20-2023	• デバイス設定にホームボタンを追加し、メタキーのサポートを有効にします。これにより、エンドユーザーは Meta+L を押してロック画面を呼び出すことができます。
2.0.1	12-06-2023	• Chromium の CVE-2024-6345 の重要なセキュリティ問題に対するゼロデイ修正。
2.0.0	11-15-2023	• 初回リリース

WorkSpaces シンクライアントリソースでのタグの使用

WorkSpaces シンクライアントのリソースを整理および管理するには、各リソースに独自のメタデータをタグとして割り当てます。タグごとにキーと値を指定します。キーとしては、一般的なカテゴリの「project」(プロジェクト)、「owner」(所有者)、「environment」(環境) などを特定の関連値と共に指定できます。タグは、AWS リソースを管理し、請求データを含むデータを整理するシンプルで強力な方法として使用できます。

既存のリソースにタグを追加すると、これらのタグは翌月の初日までコスト配分レポートに表示されません。例えば、7 月 15 日に既存の WorkSpaces シンクライアントデバイスにタグを追加すると、そのタグは 8 月 1 日までコスト配分レポートに表示されません。詳細については、AWS 請求ユーザーガイドの「コスト配分タグの使用」を参照してください。

> **Note**
>
> Cost Explorer で WorkSpaces シンクライアントリソースタグを表示するには、「 AWS Billing ユーザーガイド」の「ユーザー定義のコスト配分タグのアクティブ化」の手順に従って、 WorkSpaces シンクライアントリソースに適用したタグをアクティブ化する必要があります。 Cost Explorer https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html
> タグはアクティベーションから 24 時間後に表示されますが、それらのタグに関連付けられた値が Cost Explorer に表示されるまでに 4～5 日かかる場合があります。さらに、Cost Explorer でコストデータを表示して提供するには、タグ付けされた WorkSpaces Thin Client リソースにその時間中に料金が発生する必要があります。Cost Explorer には、タグがアクティブ化されたときのコストデータのみが表示されます。現時点では、履歴データはありません。

タグ付けできるリソース :

- タグは、作成時にWorkSpaces Thin Client 環境というリソースに追加できます。
- WorkSpaces Thin Client 環境、デバイス、ソフトウェアセットの既存のリソースにタグを追加できます。

タグの制限

- リソースあたりのタグの最大数 – 50

- 最大キー長 - 128 Unicode 文字
- 値の最大長 - 256 Unicode 文字
- タグのキーと値は大文字と小文字が区別されます。使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。ただし、先頭または末尾にはスペースを使用しないでください。
- タグ名または値に aws: プレフィックスを使用しないでください。このプレフィックスは AWS 使用のために予約されています。このプレフィックスが含まれるタグの名前または値は編集または削除できません。

コンソールを使用して既存の環境のタグを更新するには

1. WorkSpaces シンクライアントコンソール を開きます。
2. 環境を選択して詳細ページを開く
3. [編集] を選択します。
4. タグセクションで、次のいずれかを実行します。
   - 新しいタグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) の値を編集します。
   - タグを更新するには、値 の値を編集します。
   - タグを削除するには、タグの横にある 削除を選択します。
5. タグの更新が完了したら、保存 を選択します。

コンソールを使用して既存のデバイスのタグを更新するには

1. WorkSpaces シンクライアントコンソール を開きます。
2. デバイスを選択して、詳細ページを開きます。
3. [タグ] を選択します。
4. [Manage tags (タグの管理)] を選択します。
5. 次の 1 つ以上の操作を行います。
   - 新しいタグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) の値を編集します。
   - タグを更新するには、値 の値を編集します。
   - タグを削除するには、タグの横にある 削除を選択します。

6. タグの更新が完了したら、保存 を選択します。

コンソールを使用してソフトウェア更新のタグを更新するには

1. WorkSpaces シンクライアントコンソール を開きます。
2. ソフトウェア更新を選択して、詳細ページを開きます。
3. タグセクションで、タグの管理 を選択します。
4. 次の 1 つ以上の操作を行います。
   - 新しいタグを追加するには、[Add new tag] (新しいタグの追加) を選択し、[Key] (キー) と [Value] (値) の値を編集します。
   - タグを更新するには、値 の値を編集します。
   - タグを削除するには、タグの横にある 削除を選択します。
5. タグの更新が完了したら、保存 を選択します。

Amazon WorkSpaces シンクライアントのセキュリティ

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利点を得られます。

セキュリティは、 AWS とユーザー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 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を担います AWS クラウド。また、 は、ユーザーが安全に使用できるサービス AWS も提供します。コンプライアンスAWS 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が定期的にセキュリティの有効性をテストおよび検証。Amazon WorkSpaces シンクライアントに適用され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AWS による対象範囲内の のサービスコンプライアンスプログラム」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、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。

このドキュメントは、 WorkSpaces シンクライアント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 WorkSpaces シンクライアントを設定する方法を示します。また、 WorkSpaces シンクライアントリソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

Amazon WorkSpaces シンクライアントでのデータ保護

AWS https://aws.amazon.com/compliance/shared-responsibility-model/、Amazon WorkSpaces Thin Client 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 AWS クラウド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。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記事「AWS 責任共有モデルおよび GDPR」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 を使用してリソースと通信します。 AWS TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- 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極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、コンソール、API、または SDK AWS のサービス を使用して WorkSpaces Thin Client などを操作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。

Amazon WorkSpaces Thin Client は、 WorkSpaces ユーザーによるシンクライアントデバイスの使用状況や仮想デスクトップサービスとのやり取りに関する情報を収集して提供します。たとえば、使用可能なメモリ、ネットワーク診断、ネットワーク情報、デバイス接続、SAML 認証情報、デバイス ID 情報、クラッシュレポートなどです。この情報はサービスの提供に使用され、サービスのユーザーエクスペリエンスを向上させるために使用される場合があります。さらに、お客様へのサービスの提供のみを目的として、 AWS 当該情報はユーザーが本サービスを利用している地域外に転送される場合があります。AWS 当社はこの情報をプライバシー通知に従って処理します。

トピック

データ暗号化

WorkSpaces Thin Client は、ユーザー設定、デバイス ID、ID プロバイダー情報、ストリーミングデスクトップ ID などの環境およびデバイスのカスタマイズデータを収集します。 WorkSpaces Thin Client はセッションのタイムスタンプも収集します。収集されたデータは Amazon DynamoDB と Amazon S3 に保存されます。 WorkSpaces シンクライアントは AWS Key Management Service (KMS) を使用して暗号化します。

コンテンツを保護するには、次のガイドラインに従ってください。

- 最小限の権限アクセスを実装し、 WorkSpaces シンクライアントのアクションに使用する特定のロールを作成します。
- end-to-end 顧客が管理するキーを提供することでデータを保護し、 WorkSpaces Thin Client が保存中のデータを指定したキーで暗号化できるようにします。
- 環境アクティベーションコードのとユーザー認証情報を共有する場合は注意が必要です。
  - WorkSpaces 管理者はシンクライアントコンソールにログインする必要があり、 WorkSpaces ユーザーはシンクライアントセットアップのアクティベーションコード、ストリーミングデスクトップへのログインには認証情報を入力する必要があります。
  - WorkSpaces 物理的にアクセスできる人なら誰でもシンクライアントをセットアップできますが、ログインするための有効なアクティベーションコードとユーザー認証情報がないとセッションを開始できません。

- ユーザーは、デバイスツールバーを使用して画面をロックするか、再起動するか、デバイスをシャットダウンするかを選択することで、セッションを明示的に終了できます。これにより、デバイスセッションが破棄され、セッション認証情報がクリアされます。

WorkSpaces Thin Client は、すべての機密データを KMS AWS で暗号化することにより、デフォルトでコンテンツとメタデータを保護します。既存の設定を適用する際にエラーが発生した場合、ユーザーは新しいセッションにアクセスできず、デバイスにソフトウェアアップデートを適用することはできません。

Amazon WorkSpaces シンクライアントの保存時のデータ暗号化

Amazon WorkSpaces Thin Client はデフォルトで暗号化機能を備えており、 AWS 所有している暗号化キーを使用して保存されている顧客の機密データを保護します。

- AWS 所有キー — Amazon WorkSpaces Thin Client はデフォルトでこれらのキーを使用して、個人を特定できるデータを自動的に暗号化します。 AWS 所有キーを表示、管理、使用したり、その使用を監査したりすることはできません。ただし、データを暗号化するキーを保護するために何らかの操作を行ったり、プログラムを変更したりする必要はありません。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS 所有キー」を参照してください。

保管中のデータをデフォルトで暗号化して、機密データの保護に伴う運用のオーバーヘッドと複雑な作業を軽減できます。同時に、安全なアプリケーションを構築して、厳格な暗号化のコンプライアンスと規制要件に対応できます。

この暗号化レイヤーを無効にしたり、別の暗号化タイプを選択したりすることはできませんが、シンクライアント環境を作成するときにお客様が管理するキーを選択することで、既存の AWS 所有の暗号化キーの上に 2 つ目の暗号化レイヤーを追加できます。

- 顧客管理キー — Amazon WorkSpaces Thin Client では、ユーザーが作成、所有、管理する対称型顧客管理キーを使用して、 AWS 既存の所有暗号化に第 2 層の暗号化を追加できます。この暗号化レイヤーはユーザーが完全に制御できるため、次のようなタスクを実行できます。
  - キーポリシーの策定と維持
  - IAM ポリシーとグラントの策定と維持
  - キーポリシーの有効化と無効化
  - 暗号化素材のローテーション
  - タグの追加

- キーエイリアスの作成
- キー削除のスケジュール設定

詳細については、「AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキー」を参照してください。

次の表は、Amazon WorkSpaces Thin Client が個人を特定できるデータを暗号化する方法をまとめたものです。

データタイプ	AWS が所有するキーの暗号化	カスタマーマネージドキーの暗号化 (オプション)
環境名 WorkSpaces シンクライアント環境名	有効	有効
デバイス名 WorkSpaces シンクライアントデバイス名	有効	有効

> **Note**
>
> Amazon WorkSpaces Thin Client は、 AWS 所有キーを使用して個人を特定できるデータを無料で保護することで、保存時の暗号化を自動的に有効にします。
> ただし、お客様が管理するキーの使用には AWS KMS 料金がかかります。料金の詳細については、「AWS Key Management Service の料金表」を参照してください。

Amazon WorkSpaces シンクライアントが AWS KMS でグラントを使用する方法

Amazon WorkSpaces Thin Client では、カスタマーマネージドキーを使用するには許可が必要です。

WorkSpaces カスタマーマネージドキーで暗号化されたシンクライアント環境を作成すると、Amazon WorkSpaces Thin Client はユーザーに代わって AWS KMS CreateGrant にリクエストを送信して許可を作成します。 AWS KMS の権限は、Amazon WorkSpaces Thin Client が顧客アカウントの KMS キーにアクセスできるようにするために使用されます。

新しいシンクライアントデバイスが、 WorkSpaces お客様が管理するキーを使用してシンクライアント暗号化環境に登録され、そのデバイスの名前が変更されると、Amazon WorkSpaces Thin Client はお客様に代わって AWS KMS CreateGrant にリクエストを送信して許可を作成します。 AWS KMS の権限は、Amazon WorkSpaces Thin Client が顧客アカウントの KMS キーにアクセスできるようにするために使用されます。

Amazon WorkSpaces Thin Client では、以下の内部操作にカスタマーマネージドキーを使用する許可が必要です。

- 暗号化解除リクエストを AWS KMS に送信して、暗号化されたデータを復号化します。

権限へのアクセス権を取り消したり、カスタマー管理キーへのサービスのアクセス権をいつでも削除したりできます。その場合、Amazon WorkSpaces Thin Client はカスタマーマネージドキーによって暗号化されたデータにアクセスできなくなり、そのデータに依存する操作に影響します。たとえば、Amazon WorkSpaces Thin Client がアクセスできない環境の詳細を取得しようとすると、`AccessDeniedException`オペレーションはエラーを返します。さらに、 WorkSpaces WorkSpaces シンクライアントデバイスはシンクライアント環境を使用できなくなります。

カスタマーマネージドキーを作成する

AWS マネジメントコンソールまたは AWS KMS API オペレーションを使用して、対称的な顧客管理キーを作成できます。

対称カスタマーマネージドキーを作成するには

「AWS Key Management Service デベロッパーガイド」にある対称カスタマーマネージドキーの作成ステップを実行します。

キーポリシー

キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーポリシーが 1 つだけ必要です。このポリシーには、そのキーを使用できるユーザーとその使用方法を決定するステートメントが含まれています。カスタマーマネージドキーを作成する際に、キーポリシーを指定することができます。詳細については、「AWS Key Management Service デベロッパーガイド」の「カスタマーマスターキーへのアクセスを制御する」を参照してください。

カスタマーマネージドキーを Amazon WorkSpaces Thin Client リソースで使用するには、キーポリシーで次の API オペレーションを許可する必要があります。

- kms:DescribeKey— Amazon WorkSpaces Thin Client がキーを検証できるように、お客様が管理するキーの詳細を提供します。
- kms:GenerateDataKey — カスタマーマネージドキーを使用してデータを暗号化できるようにします。
- kms:Decrypt — カスタマーマネージドキーを使用してデータを復号できるようにします。
- kms:CreateGrant - カスタマーマネージドキーにグラントを追加します。指定した KMS キーへのアクセスを制御します。これにより、Amazon WorkSpaces Thin Client が必要とする付与オペレーションにアクセスできるようになります。グラントの使用の詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

  これにより、Amazon WorkSpaces シンクライアントは次のことができるようになります。

  - Decrypt を呼び出して、暗号化されたデータを復号します。

Amazon WorkSpaces Thin Client に追加できるポリシーステートメントの例は次のとおりです。

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
```

```
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

ポリシーでの権限の指定に関する詳細については、「AWS Key Management Service デベロッパーガイド」の「ポリシーで権限を指定する」を参照してください。

キーアクセスのトラブルシューティングについての詳細は、「AWS Key Management Service デベロッパーガイド」を参照してください。

WorkSpaces シンクライアント用のカスタマー管理キーの指定

カスタマーマネージドキーは、以下のリソースの第 2 レイヤー暗号化として指定できます。

- WorkSpaces シンクライアント環境

環境を作成するときに、Amazon WorkSpaces Thin Client が識別可能な個人データを暗号化するために使用するデータキーを指定することでデータキーを指定できます。`kmsKeyArn`

- `kmsKeyArn`— AWS KMS カスタマー管理キーのキー識別子。キー ARN を提供します。

WorkSpaces WorkSpaces 顧客管理キーで暗号化された新しいシンクライアントデバイスをシンクライアント環境に追加すると、 WorkSpaces WorkSpaces シンクライアントデバイスはシンクライアント環境からカスタマー管理キーの設定を継承します。

暗号化コンテキストは、データに関する追加のコンテキスト情報を含むキーと値のペアのオプションセットです。

AWS KMS は、認証済み暗号化をサポートするための追加の認証データとして暗号化コンテキストを使用します。データを暗号化するリクエストに暗号化コンテキストを含めると、 AWS KMS は暗号化コンテキストを暗号化されたデータにバインドします。データを復号するには、同じ暗号化コンテキストをリクエストに含めます。

Amazon WorkSpaces シンクライアント暗号化コンテキスト

Amazon WorkSpaces Thin Client は、すべての AWS KMS 暗号化オペレーションで同じ暗号化コンテキストを使用します。キーは Amazon リソースネーム (ARN) `aws:thinclient:arn` で、値は Amazon リソースネーム (ARN) です。

環境暗号化コンテキストは次のとおりです。

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

デバイス暗号化コンテキストは次のとおりです。

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

暗号化コンテキストによるモニタリングに暗号化コンテキストを使用する

WorkSpaces シンメトリックカスタマー管理キーを使用してシンクライアント環境とデバイスデータを暗号化する場合、監査レコードとログの暗号化コンテキストを使用して、カスタマー管理キーがどのように使用されているかを識別することもできます。暗号化コンテキストは、AWS CloudTrail または Amazon Logs CloudWatch によって生成されたログにも表示されます。

暗号化コンテキストを使用して顧客マネージドキーへのアクセスを制御する

対称カスタマーマネージドキー (CMK) へのアクセスを制御するための条件として、キーポリシーと IAM ポリシー内の暗号化コンテキストを使用することもできます。付与する際に、暗号化コンテキストの制約を使用することもできます。

Amazon WorkSpaces Thin Client は、グラントの暗号化コンテキスト制約を使用して、アカウントまたはリージョンのカスタマー管理キーへのアクセスを制御します。権限の制約では、権限によって許可されるオペレーションで指定された暗号化コンテキストを使用する必要があります。

次に、特定の暗号化コンテキストのカスタマーマネージドキーへのアクセスを付与するキーポリシーステートメントの例を示します。このポリシーステートメントの条件では、kms:Decrypt 呼び出しに暗号化コンテキストを指定する暗号化コンテキスト制約が必要です。

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Amazon WorkSpaces シンクライアントの暗号化キーのモニタリング

Amazon WorkSpaces シンクライアントリソースで AWS KMS カスタマー管理キーを使用する場合、 AWS CloudTrail または Amazon CloudWatch ログを使用して Amazon WorkSpaces シンクライアントが AWS KMS に送信するリクエストを追跡できます。

以下の例はDescribeKey、、CreateGrantGenerateDataKeyDecrypt、Decrypt (を使用してGrant) お客様管理キーで暗号化されたデータにアクセスするために Amazon WorkSpaces Thin Client によって呼び出される KMS AWS CloudTrail オペレーションを監視するためのイベントです。

以下の例では、 WorkSpaces シンクライアント環境について説明しています。encryptionContext CloudTrail WorkSpaces シンクライアントデバイスでも同様のイベントが記録されます。

DescribeKey

Amazon WorkSpaces Thin Client は、DescribeKeyオペレーションを使用して AWS KMS カスタマー管理キーを検証します。

以下のイベント例では DescribeKey オペレーションを記録しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
```

```
}
```

CreateGrant

Amazon WorkSpaces Thin Client `CreateGrant` はこのオペレーションを使用して KMS グラントを作成します。これにより、デバイスがデータにアクセスしているときにデータを復号化できます。

以下のイベント例では `CreateGrant` オペレーションを記録しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
```

```
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces GenerateDataKey シンクライアントはオペレーションを使用してデータを暗号化します。

以下のイベント例では GenerateDataKey オペレーションを記録しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces シンクライアントは、Decryptオペレーションを使用してデータを復号化します。

以下のイベント例では Decrypt オペレーションを記録しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

WorkSpaces シンクライアントデバイスが環境またはデバイス情報にアクセスすると、KMS `Decrypt` キーによって許可される操作が使用されます。`Grant`

以下のイベント例では、`Decrypt`を介して承認された操作を記録しています。`Grant`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


詳細はこちら

次のリソースは、保管時のデータ暗号化についての詳細を説明しています。

- 詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS Key Management Service の基本概念」を参照してください。
- AWS Key Management Service のセキュリティベストプラクティスの詳細については、『AWS キー管理サービス開発者ガイド』を参照してください。

転送中の暗号化

WorkSpaces シンクライアントは HTTPS と TLS 1.2 経由で転送中のデータを暗号化します。コンソールまたは直接 API WorkSpaces 呼び出しを使用してシンクライアントにリクエストを送信できます。転送されるリクエストデータは、HTTPS または TLS 接続を介して送信されることで暗号化されます。リクエストデータは、 AWS コンソール、 AWS コマンドラインインターフェイス、または AWS SDK WorkSpaces からシンクライアントに転送できます。これには、デバイス上のすべてのソフトウェアアップデートも含まれます。

転送時の暗号化はデフォルトで構成され、安全な接続 (HTTPS、TLS) はデフォルトで構成されます。

キー管理

独自のカスタマー管理 AWS KMS キーを提供して、顧客情報を暗号化できます。キーを指定しない場合、 WorkSpaces Thin Client AWS は所有キーを使用します。 AWS SDK を使用してキーを設定できます。

インターネット仕事用トラフィックのプライバシー

管理者は、開始時間や保留中のソフトウェアアップデート情報など、 WorkSpaces シンクライアントセッションイベントを表示できます。これらのログは暗号化され、 WorkSpaces シンクライアントコンソールで顧客に安全に配信されます。個々のストリーミングデスクトップセッションに関するユーザー情報と詳細情報は、デスクトップサービスによって記録されます。詳細については、「監視」、「 AppStream 2.0 の監視と報告」、または「 WorkSpaces Web のユーザーアクセスログ」を参照してください。 WorkSpaces

Amazon WorkSpaces シンクライアントの 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。IAM 管理者は、誰を認証 (サインイン) し、誰に

WorkSpaces シンクライアントリソースの使用を承認する (アクセス許可を付与する) かを制御します。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、 WorkSpaces シンクライアントで行う作業によって異なります。

サービスユーザー – WorkSpaces シンクライアントサービスを使用してジョブを実行する場合は、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの WorkSpaces シンクライアント機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。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。WorkSpaces シンクライアントの機能にアクセスできない場合は、「」を参照してくださいAmazon WorkSpaces シンクライアント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。

サービス管理者 – 社内の WorkSpaces シンクライアントリソースを担当している場合は、通常、 WorkSpaces シンクライアントへのフルアクセスがあります。サービスのユーザーがどの WorkSpaces シンクライアント機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。シンクライアントで IAM を利用する方法の詳細については、 WorkSpaces 「」を参照してくださいAmazon WorkSpaces シンクライアントと IAM の連携方法。

IAM 管理者 – IAM 管理者は、 WorkSpaces シンクライアントへのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる WorkSpaces シンクライアントアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces シンクライアントのアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって認証 (にサインイン AWS) される必要があります。

ID ソース (AWS IAM Identity Center) から提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーションアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS にロールを引き受けます。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、 認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストを自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、「IAM ユーザーガイド」のAWS 「 API リクエストの署名」を参照してください。

使用する認証方法を問わず、セキュリティ情報の提供を追加でリクエストされる場合もあります。例えば、 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高めることを AWS 推奨しています。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証 (MFA)」および「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

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインイン ID から始めます。このアイデンティティは 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。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行してください。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーション ID

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な AWS のサービス 認証情報を使用して にアクセスする ID プロバイダーとのフェデレーションの使用を要求します。

フェデレーティッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、、Identity Center ディレクトリのユーザー、または ID ソースから提供された認証情報 AWS のサービス を使用して にアクセスするすべてのユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、すべての およびアプリケーションで使用できるように、独自の ID ソース内のユーザー AWS アカウント とグループのセットに接続して同期することもできます。IAM アイデンティティセンターの詳細については、[AWS IAM Identity Center ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM 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。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーション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「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団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権限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「IAM 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 IAM 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、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」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。

- フェデレーションユーザーアクセス – フェデレーションアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーションアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、

を呼び出すプリンシパルのアクセス許可を使用し AWS のサービス、ダウンストリームサービスにリクエストを行う AWS のサービス リクエストと組み合わせて使用します。FAS リクエストは、他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストをサービスが受信した場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- 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。IAM 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。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

- 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 リクエストを作成しているアプリケーションの一時的な認証情報を管理できます。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 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、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 ロールを使用して権限を付与する」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 ロールの作成が適している場合 (ユーザーではなく)」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には AWS 、ポリシーを作成し、 AWS ID または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、それらのアクセス許可を定義します。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシー 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 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。

デフォルトでは、ユーザーやロールに権限はありません。IAM 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権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。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。こ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、IAM ユーザー、ユーザーグループ、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、 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。管理ポリシーまたはインラインポリシーの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。ポリシーが添付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は、プリンシパルを指定する必要があります。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 IAM の AWS マネージドポリシーを使用することはできません。

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権限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。

Amazon S3、、および Amazon VPC は AWS WAF、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、追加の一般的でないポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- 権限の境界 - 権限の境界は、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 (IAM ユーザーまたはロール) に付与できる権限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権限は、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権限の境界の共通部分になります。`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では、権限の境界は制限されません。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。権限の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの権限の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。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 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 AWS アカウントのルートユーザー。組織と 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。結果としてセッションの権限される範囲は、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になります。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。複数のポリシータイプが関連する場合に 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「ポリシーの評価ロジック」を参照してください。

Amazon WorkSpaces シンクライアントと IAM の連携方法

IAM を使用して WorkSpaces シンクライアントへのアクセスを管理する前に、 WorkSpaces シンクライアントで使用できる IAM 機能について学びます。

Amazon WorkSpaces シンクライアントで使用できる IAM の機能

IAM 機能	WorkSpaces シンクライアントのサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	いいえ
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー	はい
ACL	なし
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	いいえ

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

WorkSpaces シンクライアントのアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限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 アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付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。

WorkSpaces シンクライアントのアイデンティティベースのポリシーの例

WorkSpaces シンクライアントのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces シンクライアントのアイデンティティベースのポリシーの例。

WorkSpaces シンクライアント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

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。ポリシーが添付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は、プリンシパルを指定する必要があります。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。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、リソースへのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。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」を参照してください。

WorkSpaces シンクライアントのポリシーアクション

ポリシーアクションに対するサポート	はい

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んなリソースにどんな条件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。

WorkSpaces シンクライアントアクションのリストを確認するには、「サービス認証リファレンス」の「Amazon WorkSpaces シンクライアントで定義されるアクション」を参照してください。

WorkSpaces シンクライアントのポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
workspaces-thin-client
```

1 つのステートメントで複数のアクションを指定するには、次の例に示すように、カンマで区切ります。

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

WorkSpaces シンクライアントのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces シンクライアントのアイデンティティベースのポリシーの例。

WorkSpaces シンクライアント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 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、リソースレベルの権限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、リソースレベルのアクセス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示すために、ワイルドカード (*) を使用します。

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

WorkSpaces シンクライアントのリソースタイプとその ARNs」の「Amazon WorkSpaces シンクライアントで定義されるリソースタイプ」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「Amazon WorkSpaces シンクライアント で定義されるアクション」を参照してください。

WorkSpaces シンクライアントのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces シンクライアントのアイデンティティベースのポリシーの例。

WorkSpaces シンクライアントのポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

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んなリソースにどんな条件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 ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。equal や less than などの条件演算子を使用して条件式を作成することによって、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 は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理OR演算を使用して条件 AWS を評価します。ステートメントの権限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 IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。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。

WorkSpaces シンクライアント条件キーのリストを確認するには、「サービス認証リファレンス」の「Amazon WorkSpaces シンクライアントの条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「Amazon WorkSpaces シンクライアントで定義されるアクション」を参照してください。

WorkSpaces シンクライアントのアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces シンクライアントのアイデンティティベースのポリシーの例。

WorkSpaces シンクライアントの ACLs

ACL のサポート	なし

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権限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。

WorkSpaces シンクライアントでの 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 の最初の手順です。次に、プリンシパルのタグがアクセスを試行するリソースのタグと一致したとき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。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを制御するには、`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。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーすべてをサポートする場合、値は Partial です。

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手順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。

WorkSpaces シンクライアント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。一時的な認証情報を AWS のサービス 使用できる などの詳細については、IAM ユーザーガイドの「IAM AWS のサービス 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は、一時的な認証情報を使用しています。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して に

アクセスすると、そのプロセスは自動的に一時的な認証情報を作成します。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、長期的なアクセスキーを使用する代わりに、動的に一時的な認証情報を生成する AWS. AWS recommends にアクセスできます。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。

WorkSpaces シンクライアントのクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用し AWS のサービス、ダウンストリームサービスにリクエスト AWS のサービス を行うリクエストと組み合わせて使用します。FAS リクエストは、他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストをサービスが受信した場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

WorkSpaces シンクライアントのサービスロール

サービスロールのサポート	いいえ

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。IAM 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**
>
> サービスロールのアクセス許可を変更すると、 WorkSpaces シンクライアントの機能が中断される可能性があります。 WorkSpaces シンクライアントが指示する場合以外は、サービスロールを編集しないでください。

WorkSpaces シンクライアント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

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 に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS サービス」を参照してください。表の中から、「サービスにリンクされたロール」列に「Yes」と記載されたサービスを見つけます。サービス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 WorkSpaces シンクライアントのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、 WorkSpaces シンクライアント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 Command Line Interface （ AWS CLI ） AWS Management Console、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。IAM 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権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者がロールに IAM ポリシーを追加すると、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM 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。

各リソースタイプの ARN の形式など、 WorkSpaces シンクライアントで定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「Amazon WorkSpaces シンクライアントのアクション、リソース、および条件キー」を参照してください。 ARNs

トピック

- ポリシーのベストプラクティス
- WorkSpaces シンクライアントコンソールの使用
- WorkSpaces シンクライアントへの読み取り専用アクセス権を付与する
- 自分の許可の表示をユーザーに許可する
- WorkSpaces シンクライアントへのフルアクセスを許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウント内で誰かが WorkSpaces シンクライアントリソースを作成、アクセス、または削除できる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 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的ユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らす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 マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションを使用する場合 AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語

(JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

WorkSpaces シンクライアントコンソールの使用

Amazon WorkSpaces シンクライアントコンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、 の WorkSpaces シンクライアントリソースの詳細をリストおよび表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

WorkSpaces シンクライアントへの読み取り専用アクセス権を付与する

この例では、IAM ユーザーが WorkSpaces シンクライアント設定を表示することを許可するが、変更を許可しないポリシーを作成する方法を示します。このポリシーには、AWS CLI または AWS API を使用して、コンソールまたはプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
```

```
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

自分の許可の表示をユーザーに許可する

この例では、ユーザーアイデンティティに添付されたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces シンクライアントへのフルアクセスを許可する

この例では、 WorkSpaces シンクライアントの IAM ユーザーにフルアクセスを許可するポリシーを作成する方法を示します。このポリシーには、AWS CLI または AWS API を使用して、コンソールまたはプログラムですべての WorkSpaces シンクライアントアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Amazon WorkSpaces シンクライアント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、 WorkSpaces シンクライアントと IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- WorkSpaces シンクライアントでアクションを実行する権限がない
- アクセスキーを表示したい
- 管理者として WorkSpaces シンクライアント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 WorkSpaces シンクライアントリソース AWS アカウント へのアクセスを許可したい

WorkSpaces シンクライアントでアクションを実行する権限がない

から、アクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、ユーザーにユーザー名とパスワードを提供した人です。

以下のエラー例は、mateojackson IAM ユーザーがコンソールを使用して架空の *my-thin-client-device* リソースに関する詳細情報を表示しようとしているが、架空の workspaces-thin-client:*ListDevices* アクセス許可がないという場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

この場合、Mateo は workspaces-thin-client:*ListDevices*アクションを使用して*my-thin-client-device*リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

アクセスキーを表示したい

IAM ユーザーアクセスキーを作成した後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーを再表示することはできません。シークレットアクセスキーを紛失した場合は、新しいアクセスキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: AKIAIOSFODNN7EXAMPLE) とシークレットアクセスキー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) の 2 つの部分で構成されています。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーは安全に管理してください。

> **Important**
>
> 正規のユーザー ID を検索するためであっても、アクセスキーを第三者に提供しないでください。これにより、 への永続的なアクセス権を誰かに付与することができます AWS アカウント。

アクセスキーペアを作成する場合、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、IAM ユーザーに新規アクセスキーを追加する必要があります。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、

新規キーペアを作成する前に、いずれかを削除する必要があります。手順を表示するには、「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 WorkSpaces シンクライアントへのアクセスを他のユーザーに許可したい

WorkSpaces シンクライアントへのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。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、 WorkSpaces シンクライアントで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する必要があります。

すぐにスタートするには、「IAM ユーザーガイド」の「IAM が委任した初期のユーザーおよびグループの作成」を参照してください。

詳細については、「 WorkSpaces シンクライアントへのフルアクセスを許可する」を参照してください。

自分の 以外のユーザーに WorkSpaces シンクライアントリソース 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:

- WorkSpaces シンクライアント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、「」を参照してくださいAmazon WorkSpaces シンクライアントと IAM の連携方法。
- 所有 AWS アカウント する 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権を付与する」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の 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「第三者 AWS アカウント が所有する へのアクセスの許可」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) へのアクセス権の提供」を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、「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」を参照してください。

Amazon WorkSpaces シンクライアントの耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン とアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS グローバルインフラストラクチャに加えて、 WorkSpaces Thin Client には、データの耐障害性とバックアップのニーズに対応できるように複数の機能が用意されています。

Amazon WorkSpaces シンクライアントでの脆弱性の分析と管理

設定と IT コントロールは、 AWS とユーザー間で共有される責任です。詳細については、 AWS 「責任共有モデル」を参照してください。

Amazon WorkSpaces シンクライアントは、Amazon WorkSpaces、Amazon AppStream 2.0、および WorkSpaces Web と相互統合されています。これらの各サービスの更新管理の詳細については、次のリンクを参照してください。

- Amazon AppStream 2.0 での更新管理
- Amazon での更新管理 WorkSpaces
- Amazon WorkSpaces Web での設定と脆弱性の分析

Amazon WorkSpaces シンクライアントのモニタリング

モニタリングは、Amazon WorkSpaces シンクライアントおよびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 は、 WorkSpaces シンクライアントを監視したり、問題が発生したときに報告したり、必要に応じて自動アクションを実行したりするために、以下のモニタリングツール AWS を提供しています。

- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールと関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出し日時を特定できます。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。

を使用した Amazon WorkSpaces シンクライアント API コールのログ記録 AWS CloudTrail

Amazon WorkSpaces シンクライアントは、シンクライアントのユーザー AWS CloudTrail、ロール、または AWS サービス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 と統合されています。 は WorkSpaces 、 WorkSpaces シンクライアントのすべての API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、 WorkSpaces シンクライアントコンソールからの呼び出しと WorkSpaces 、シンクライアント API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、 WorkSpaces シンクライアントのイベントなど、Amazon S3 バケットへのイベントの継続的な配信 CloudTrailを有効にすることができます。証跡を設定しない場合でも、コンソールのイベント履歴 で最新の CloudTrail イベントを表示できます。 で収集された情報を使用して CloudTrail、 WorkSpaces シンクライアントに対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

WorkSpaces のシンクライアント情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 は で有効になります。 WorkSpaces シンクライアントでアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウンロードできます。詳細については、「イベント履歴 を使用した CloudTrail イベントの表示」を参照してください。

WorkSpaces シンクライアントのイベントなど 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、 はログファイル CloudTrail 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 ログで収集されたデータをより詳細に分析し、それに基づく対応を行うように他の AWS サービスを設定できます。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 でサポートされているサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

WorkSpaces シンクライアントのすべてのアクションは によってログに記録 CloudTrail され、「Amazon WorkSpaces シンクライアント API リファレンス」に記載されています。例えば、`CreateEnvironment`、、および `GetSoftwareSet` アクションを呼び出すと`ListDevices`、 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のどちらを使用して送信されたか。
- 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 AWS 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 要素」を参照してください。

WorkSpaces シンクライアントのログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元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、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 GetDeviceアクションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
```

```
}
```

を使用した Amazon WorkSpaces シンクライアントリソースの作成 AWS CloudFormation

Amazon WorkSpaces シンクライアントは AWS CloudFormation、 AWS リソースのモデル化とセットアップに役立つサービスである と統合されています。これにより、リソースとインフラストラクチャの作成、管理に費やす時間を短縮できます。必要なすべての AWS リソース (環境など) を記述するテンプレートを作成すると、 はそれらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用して WorkSpaces シンクライアントリソースをいつでも繰り返しセットアップできます。リソースを一度記述すると、同じリソースを複数の AWS アカウント およびリージョンで繰り返しプロビジョニングできます。

WorkSpaces シンクライアントと AWS CloudFormation テンプレート

WorkSpaces シンクライアントおよび関連サービスのリソースをプロビジョニングして設定するには、 AWS CloudFormation テンプレートを理解する必要があります。テンプレートは、JSON または YAML 形式のフォーマット済みテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックにプロビジョニングするリソースを記述します。JSON または YAML 形式に慣れていない場合は、 AWS CloudFormation デザイナーを使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation デザイナー とは」を参照してください。

WorkSpaces シンクライアントは、 での環境の作成をサポートしています AWS CloudFormation。環境の JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation 「 ユーザーガイド」の「Amazon WorkSpaces シンクライアントリソースタイプのリファレンス」を参照してください。

の詳細はこちら AWS CloudFormation

の詳細については AWS CloudFormation、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド

- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

インターフェイスエンドポイント (AWS PrivateLink) を使用して Amazon WorkSpaces シンクライアントにアクセスする

を使用して AWS PrivateLink 、VPC と Amazon WorkSpaces シンクライアントの間にプライベート接続を作成できます。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、 WorkSpaces シンクライアントに VPC としてアクセスできます。VPC のインスタンスは、 WorkSpaces シンクライアントにアクセスするためにパブリック IP アドレスを必要としません。

このプライベート接続を確立するには、 を使用するインターフェイスエンドポイントを作成します AWS PrivateLink。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、 WorkSpaces シンクライアント宛てのトラフィックのエントリポイントとして機能するリクエスタマネージド型のネットワークインターフェイスです。

詳細については、『AWS PrivateLink ガイド』の「AWS PrivateLinkによるアクセス」を参照してください。

WorkSpaces シンクライアントに関する考慮事項

WorkSpaces シンクライアントのインターフェイスエンドポイントを設定する前に、AWS PrivateLink 「 ガイド」の「考慮事項」を確認してください。

WorkSpaces シンクライアントは、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

WorkSpaces シンクライアントのインターフェイスエンドポイントを作成する

Amazon VPC コンソールまたは AWS Command Line Interface () を使用して、 WorkSpaces シンクライアントのインターフェイスエンドポイントを作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の「インターフェイスエンドポイントを作成」を参照してください。

次のサービス名を使用して、 WorkSpaces シンクライアントのインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.thinclient.api
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、デフォルトのリージョン DNS 名を使用して WorkSpaces シンクライアントに API リクエストを行うことができます。例えば `api.thinclient.us-east-1.amazonaws.com` です。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイントを介して WorkSpaces シンクライアントへのフルアクセスが許可されます。VPC から WorkSpaces シンクライアントに付与されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは、以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドのControl access to services using endpoint policies (エンドポイントポリシーを使用してサービスへのアクセスをコントロールする)を参照してください。

例: WorkSpaces シンクライアントアクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている WorkSpaces シンクライアントアクションへのアクセスが許可されます。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
```

```
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

WorkSpaces シンクライアント管理者ガイドのドキュメント履歴

次の表に、 WorkSpaces シンクライアント管理者ガイドのリリースのドキュメント履歴を示します。

変更	説明	日付
• WorkSpaces Amazon WorkSpaces シンクライアントの の設定 • Amazon WorkSpaces シンクライアントの AppStream 2.0 の設定	• オペレーティングシステムのリストを更新しました。 • ID プロバイダーの手順を更新しました。	2024 年 2 月 12 日
初回リリース	初回リリース	2023 年 11 月 26 日

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。