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 Web 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を作成し、デバイスを管理し、パラメーターを設定できます。

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方には、以下のセクションを初めに読むことをお勧めします。

- WorkSpaces シンクライアント管理者コンソールの開始
- WorkSpaces シンクライアント管理者コンソールの使用

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
- WorkSpaces アプリケーション
- Amazon WorkSpaces セキュアブラウザ

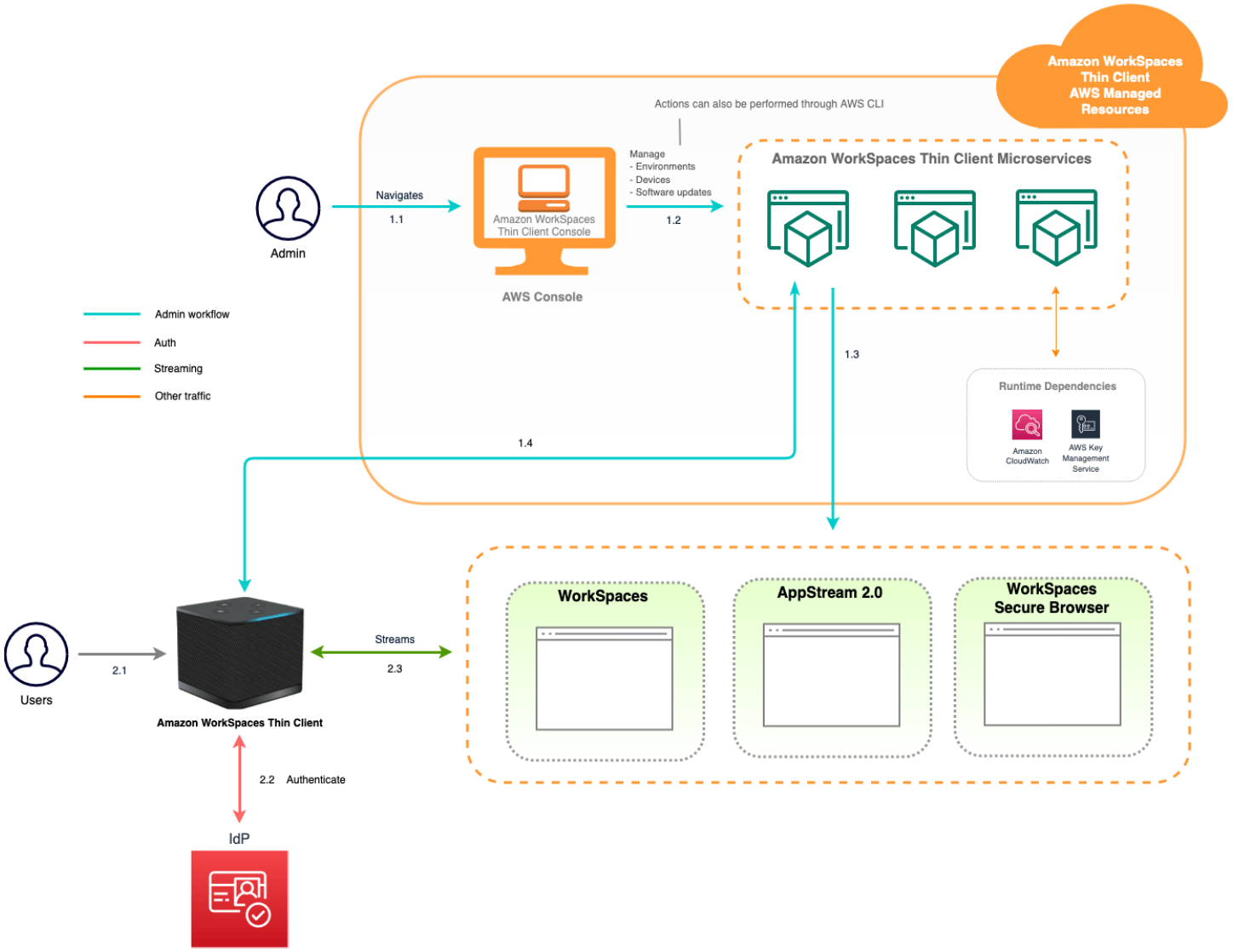
使用する VDI に応じて、WorkSpaces シンクライアントの情報はWorkSpaces アプリケーションのスタック、WorkSpaces Secure Browser のウェブポータルエンドポイントを介してアクセスおよび管理されます。

Amazon WorkSpaces の詳細については、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。これにより Directory Service、Simple AD、AD Connector、または AWS Managed Microsoft AD とも呼ばれる Directory Service for Microsoft Active Directory のオプションが提供されます。詳細については、Directory Service 管理ガイドを参照してください。

WorkSpaces アプリケーションの詳細については、Amazon WorkSpaces アプリケーションの開始方法: 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。WorkSpaces Applications 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、自動的にスケールし、オンデマンドでユーザーへのアクセスを提供します。WorkSpaces Applications を使用すると、ユーザーは選択したデバイスで必要なアプリケーションにアクセスでき、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滑らかなユーザーエクスペリエンスが得られます。

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、オンデマンドでフルマネージド型の Linux ベースのサービスで、内部ウェブサイトや 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ように設計されています。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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

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 アイデンティティセンター ユーザーガイドの「開始方法」の手順に従います。	AWS Command Line Interface ユーザーガイドの を使用する AWS CLI ように を設定 AWS IAM アイデンティティセンターして、プログラムによるアクセスを設定します。
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「緊急アクセス用の IAM ユーザーを作成する」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を管理する」の手順に従って、プログラムによるアクセスを設定します。

VDI for Amazon WorkSpaces シンクライアントの開始方法

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 シンクライアントでは、使用する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構成が必要です。

トピック

- WorkSpaces シンクライアント用の WorkSpaces Personal の設定
- WorkSpaces シンクライアントの WorkSpaces プールの設定
- Amazon WorkSpaces シンクライアント用の WorkSpaces アプリケーションの設定 Amazon WorkSpaces
- Amazon WorkSpaces シンクライアント用の Amazon WorkSpaces Secure Browser の設定

WorkSpaces シンクライアント用の WorkSpaces Personal の設定

WorkSpaces シンクライアントを Amazon WorkSpaces Personal で使用するには、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 Personal ディレクトリは、 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機能を変更することはお勧めしません。

[開始する前に]

WorkSpace 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ます。ただし、デバイスユーザーは WorkSpaces に接続して使用するために AWS アカウントは必要ありません。

設定に進む前に、次の概念を確認して理解してください。

- WorkSpace を起動するときは、WorkSpace バンドルを選択します。詳細については、「Amazon WorkSpaces バンドル」を参照してください。
- WorkSpace を起動するときに、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 WorkSpaces」を参照してください。
- WorkSpace を起動するときは、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 と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、WorkSpaces Personal のディレクトリを管理する」を参照してください。
- WorkSpace を起動するときは、WorkSpaces シンクライアント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、WorkSpaces シンクライアントの設定」を参照してください。

ステップ 1: システムが WorkSpaces Personal 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 Personal と適切に動作するには、システムが次の特定の要件を満たしている必要があります。この表は、サポートされているこれらの機能とその要件の一覧です。

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)

機能	要件
	• 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) • Microsoft Power with Windows 10 (Server 2016、2019、2022 ベース) w Office • Windows 10 を搭載した Microsoft PowerPro (Server 2016、2019、および 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、および 2022 ベース) • Microsoft Performance with Windows 10 (Server 2016、2019、および 2022 ベース) w Office
サポートされるプロトコル	DCV のみ

ステップ 2: 詳細セットアップを使用して WorkSpace を起動する

詳細設定を使用して WorkSpace を起動するには

1. https://console.aws.amazon.com/workspaces/v2/home/ で WorkSpaces コンソールを開きます。
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。

ビジネス継続性

WorkSpaces シンクライアントは、ビジネス継続性プラン (BCP) の一部としてビジネス継続性をサポートします。WorkSpaces シンクライアントの事業継続性は、WorkSpaces Personal でのみ使用できます。事業継続性の詳細については、「Amazon WorkSpaces 管理ガイド」の「WorkSpaces Personal の事業継続性」を参照してください。 Amazon WorkSpaces

前提条件

WorkSpaces シンクライアントでビジネス継続性を使用するには、次の前提条件を満たす必要があります。

- WorkSpaces クロスリージョンリダイレクトの場合 – DNS サービスとルーティングポリシーが設定されています。これらを設定するには、「DNS サービスの設定」と「DNS ルーティングポリシーの設定」を参照してください。
- WorkSpaces マルチリージョンレジリエンスの場合 – スタンバイ WorkSpaces が作成されました。これを作成するには、「スタンバイ WorkSpace を作成する」を参照してください。
- WorkSpaces シンクライアントを使用するリージョンの接続エイリアス。リージョンを確認するには、「対象リージョン」を参照してください。

WorkSpaces シンクライアントのビジネス継続性の設定

Amazon WorkSpaces シンクライアントで Amazon WorkSpaces Personal DR を有効にするには、SDK を使用して環境にマッピングするように接続エイリアスを設定する必要があります。

ディザスタリカバリを設定するためのサンプルドキュメントの説明:

Example

CLI AWS を使用して、ストリーミングデスクトップの WorkSpaces 接続エイリアスを使用して新しい環境を作成するコマンドの例:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

wsca-id を WorkSpaces Personal 接続エイリアスに置き換えます。WorkSpaces 接続エイリアスの ID は、WorkSpaces マネジメントコンソールまたは SDK から確認できます。

エンドユーザーエクスペリエンス

ビジネス継続性が設定されたら、過去 15 日以内にデバイスを登録してアクティブにする必要があります。その後、WorkSpaces シンクライアント管理サービスが使用できなくなった場合、ユーザーは最大 24 時間セッションに接続し続けることができます。この状態では、デバイスはソフトウェア更新を受信せず、体制情報を交換せず、アクティブ化できません。WorkSpaces シンクライアントコンソールの対応するデバイスエントリには、最新情報は表示されません。

WorkSpaces シンクライアントデバイス管理サービスが 24 時間以上使用できない場合、次のエラーメッセージが表示されます。

「エラーが発生しました。もう一度試してください。問題が解決しない場合は、IT 管理者にお問い合わせください。(エラーコード: 3006)。」

WorkSpaces シンクライアントの WorkSpaces プールの設定

WorkSpaces シンクライアントを Amazon WorkSpaces Pools で使用するには、SAML 2.0 ID プロバイダー (IdP) が WorkSpaces Pools ディレクトリにアクセスするように設定する必要があります。Amazon WorkSpaces Pools ディレクトリは、ユーザーのグループに割り当てられた WorkSpaces の非永続的なプールです。

> **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。

[開始する前に]

WorkSpace 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ます。ただし、デバイスユーザーは WorkSpaces に接続して使用するために AWS アカウントは必要ありません。

設定を進める前に、「Amazon WorkSpaces 管理ガイド」の「WorkSpaces Pools で Active Directory の使用を開始する前に」に記載されている概念を確認して理解してください。 Amazon WorkSpaces

WorkSpaces プールを作成する

ユーザーアプリケーションを起動してストリーミングするプールを設定および作成します。

> **Note**
>
> WorkSpaces プールを作成する前に、ディレクトリを作成する必要があります。詳細については、「SAML 2.0 の設定」およびWorkSpaces Pools ディレクトリの作成」を参照してください。

プールを設定して作成する

1. https://console.aws.amazon.com/workspaces/v2/home/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces]、[プール] の順に選択します。
3. [WorkSpaces プールの作成] を選択します。
4. オンボーディング (オプション) で、ユースケースに基づいてレコメンデーションオプションを選択して、使用する WorkSpaces のタイプに関するレコメンデーションを取得できます。WorkSpaces Pools を使用することがわかっている場合は、この手順を省略できます。
5. [WorkSpaces の設定] で、次の情報を入力します。

   - [名前] に、プール用の一意の名前識別子を入力します。特殊文字は使用できません。
   - [説明] に、プールの説明を入力します (最大 256 文字)。
   - [バンドル] で、WorkSpaces に使用するバンドルのタイプを以下から選択します。
     - 基本 WorkSpaces バンドルを使用する – ドロップダウンからバンドルのいずれかを選択します。選択したバンドルタイプの詳細を確認するには、[バンドルの詳細] を選択します。プールに提供されるバンドルを比較するには、[すべてのバンドルを比較] を選択します。
     - 独自のカスタムバンドルを使用する – 以前に作成したバンドルを選択します。カスタムバンドルを作成するには、WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する」を参照してください。

     > **Note**
     >
     > 現在、BYOL は WorkSpaces Pools では使用できません。

   - [Maximum session duration in minutes] (セッションの最大継続時間 (分単位)) には、ストリーミングセッションがアクティブな状態を維持できる最大時間を選択します。ユーザーがこの制限に達する 5 分前にストリーミングインスタンスにまだ接続している場合は、切断される前に開いているドキュメントを保存するように求められます。この時間が経過すると、インスタンスは終了し、新しいインスタンスに置き換えられます。WorkSpaces Pools コンソールで設

定できる最大セッション時間は 5,760 分 (96 時間) です。WorkSpaces Pools API と CLI を使用して設定できる最大セッション時間は 432,000 秒 (120 時間) です。

- [Disconnect timeout in minutes (切断タイムアウト (分単位))] では、ユーザーが切断した後にストリーミングセッションをアクティブのままにする時間を選択します。切断、またはこの時間間隔内のネットワークの中断の後、ユーザーが再接続を試みる場合、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。
- ユーザーがプールツールバーで [セッションの終了] や [ログアウト] を選択してセッションを終了した場合、切断タイムアウトは適用されません。代わりに、開いているドキュメントを保存するように求められ、すぐにストリーミングインスタンスから切断されます。その後、ユーザーが使用していたインスタンスは終了します。
- [Idle disconnect timeout in minutes (アイドル切断タイムアウト (分単位))] では、ユーザーがストリーミングセッションから切断されるまでにアイドル状態 (非アクティブ) であることができる時間と、[Disconnect timeout in minutes (切断タイムアウト (分単位))] 期間の開始時刻を選択します。ユーザーは、アイドル状態のために切断される前に通知されます。ユーザーが [Disconnect timeout in minutes (切断タイムアウト (分単位))] で指定した期間が経過する前にストリーミングセッションへの再接続を試みると、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。この値を 0 に設定すると無効になります。この値を無効にした場合、ユーザーはアイドル状態が原因で切断されることはありません。

  > **Note**
  >
  > ストリーミングセッション中にキーボードまたはマウス入力の提供を停止すると、ユーザーはアイドル状態と見なされます。ドメインに参加しているプールの場合、アイドル切断タイムアウトのカウントダウンは、ユーザーが Active Directory ドメインパスワードまたはスマートカードを使用してログインするまで開始されません。ファイルのアップロードとダウンロード、オーディオ入力、オーディオ出力、およびピクセルの変更は、ユーザーアクティビティとはなりません。[Idle disconnect timeout in minutes (アイドル切断タイムアウト (分単位))] の期間が経過した後でも引き続きアイドル状態である場合、ユーザーは切断されます。

- [スケジュールされた容量のポリシー] (オプション) で、[新しいスケジュールされた容量を追加] を選択します。予想される同時ユーザーの最小数に基づいて、プールの最小数のインスタンスと最大数のインスタンスをプロビジョニングする日時を指定します。

- [手動スケーリングポリシー] (オプション) で、プールの容量を増減するために使用するプールのスケーリングポリシーを指定します。手動スケーリングポリシーを展開して、新しいスケーリングポリシーを追加します。

  > **Note**
  >
  > プールのサイズは、指定した最小および最大容量によって制限されます。

  - [新しいスケールアウトポリシーを追加] を選択し、指定された容量使用率が指定されたしきい値を下回るか超えるかした場合に指定されたインスタンスを追加するための値を入力します。
  - [新しいスケールインポリシーを追加] を選択し、指定された容量使用率が指定されたしきい値を下回るか超えるかした場合に指定されたインスタンスを削除するための値を入力します。
- [タグ] で、使用するキーペアの値を指定します。キーは、特定の関連値を持つ「プロジェクト」、「所有者」、「環境」などの一般的なカテゴリにすることができます。

6. [ディレクトリを選択] ページで、作成したディレクトリを選択します。ディレクトリを作成するには、[ディレクトリの作成] を選択します。詳細については、WorkSpaces Pools のディレクトリを管理する」を参照してください。
7. [WorkSpaces プールの作成] を選択します。

WorkSpaces シンクライアントアクセスの設定

WorkSpaces シンクライアントを使用するように WorkSpaces Pools のウェブアクセスを設定する場合は、 AWS コマンドランドインターフェイスを使用する必要があります。

1. AWS Command Line Interface をインストールまたは更新する。
2. AWS CLI 設定を構成します。
3. を開きます AWS CLI。
4. 次の WORKSPACES_DIRECTORY_IDと を適切な情報REGIONに置き換えて実行します。

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

Amazon WorkSpaces シンクライアント用の WorkSpaces アプリケーションの設定 Amazon WorkSpaces

WorkSpaces アプリケーションインスタンスはスタック名に基づいて一覧表示され、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。WorkSpaces アプリケーションの SAML 認証は開始された認証のみをサポートしているため、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 WorkSpaces アプリケーションに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で WorkSpaces アプリケーション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。この表は、サポートされているこれらの機能とその要件の一覧です。

機能	要件
ID プロバイダー	WorkSpaces アプリケーション管理者ガイドの「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。 WorkSpaces env 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)
クリップボード	[無効] WorkSpaces Applications スタックレベルで設定

機能	要件
ファイル転送	[無効] WorkSpaces Applications スタックレベルで設定
ローカルデバイスへの印刷	[無効] WorkSpaces Applications スタックレベルで設定

WorkSpaces アプリケーションでの 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: WorkSpaces アプリケーション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、WorkSpaces Applications 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セットアップし、ユーザーにスタックへのアクセス権を付与するには、次の手順に従います。まだ行っていない場合は、WorkSpaces アプリケーションの開始方法: サンプルアプリケーションのセットアップ」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 シンクライアント用の 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の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 と適切に動作するには、システムが次の特定の要件を満たしている必要があります。この表は、サポートされているこれらの機能とその要件の一覧です。

機能	要件
クリップボード	[無効]
ファイル転送	[無効]
ローカルデバイスへの印刷	[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. AWS CodeBuild Cloudformation テンプレートを使用して VPC を作成します。
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https://docs.aws.amazon.com/workspaces-web/latest/adminguide/create-web-portal.html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開始

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費用対効果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。

トピック

対象リージョン

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、スペインでのみご利用いただけます。

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

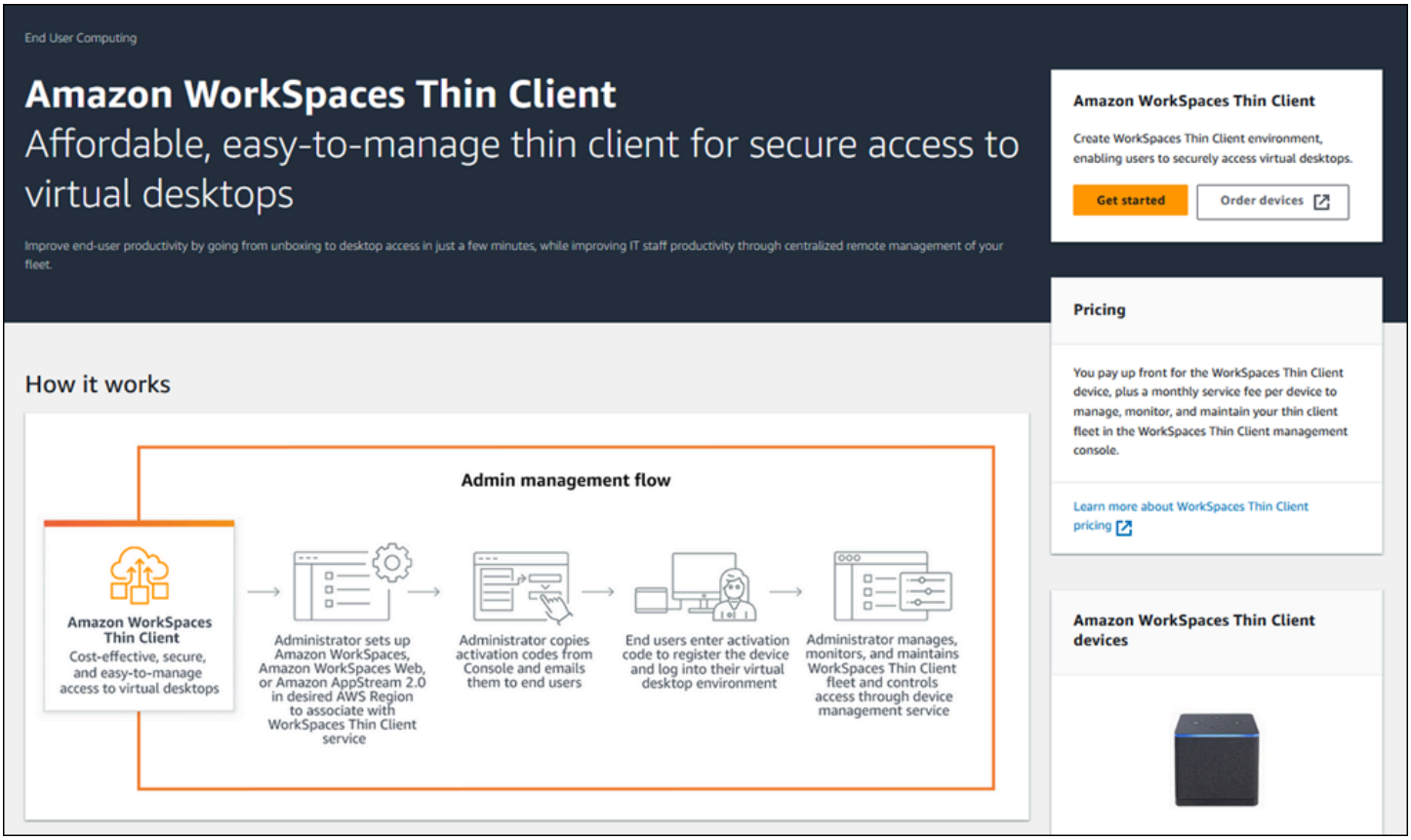
リージョン名	リージョン	エンドポイント	コンソールリンク
欧州 (アイルランド)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
カナダ (中部)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧州 (フランクフルト)	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 アカウントをお持ちの場合は、管理者コンソールを起動し、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

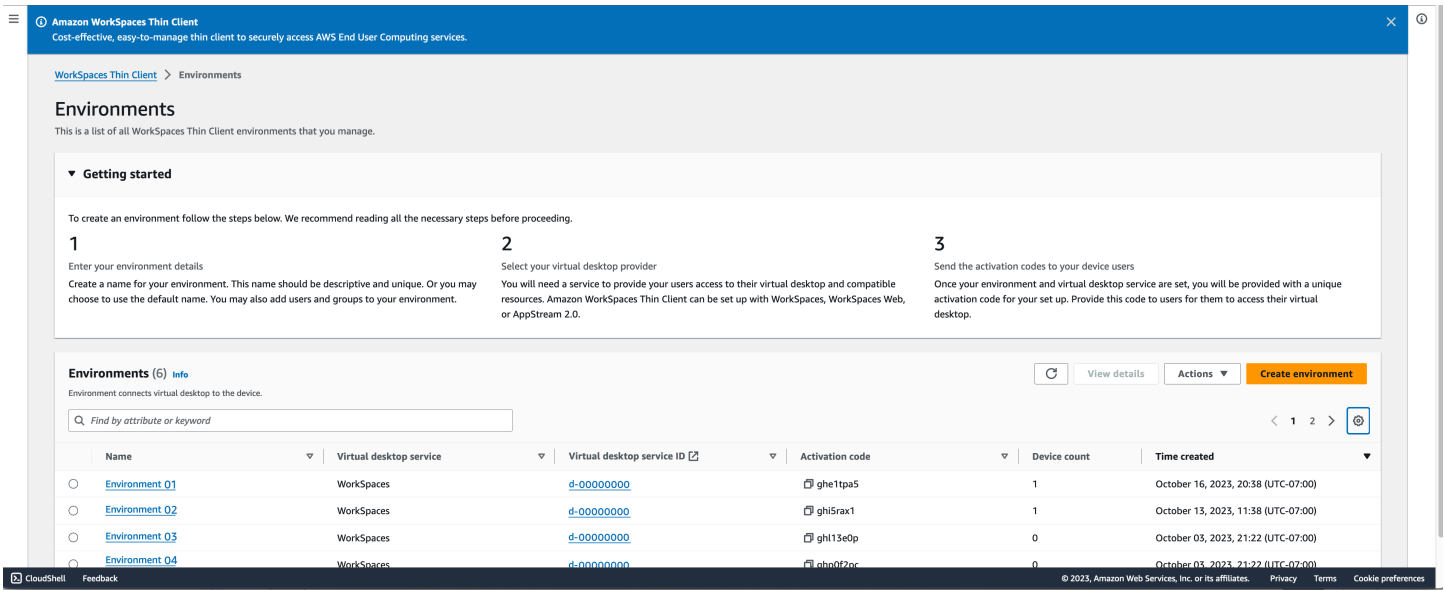
環境

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
- WorkSpaces アプリケーション
- Amazon WorkSpaces セキュアブラウザ

環境リスト

環境には、確認できるパラメータと実行できるアクションがいくつかあります。



環境リストの詳細

環境のパラメータがレビュー用に一覧表示されます。次の表に、概要の各要素とその機能を示します。

要素	説明
名前	この環境に関連付けられた一意の識別子。

要素	説明
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。
作成時刻	環境が作成された日時。

環境リストアクション

ここから実行できるアクションは多数あります。これらのいずれかを選択して、対応するアクションを実行します。

要素	説明
[検索]	管理す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。
環境を作成する	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
- 環境を作成する

- 環境を編集する
- 環境を削除する

環境の詳細

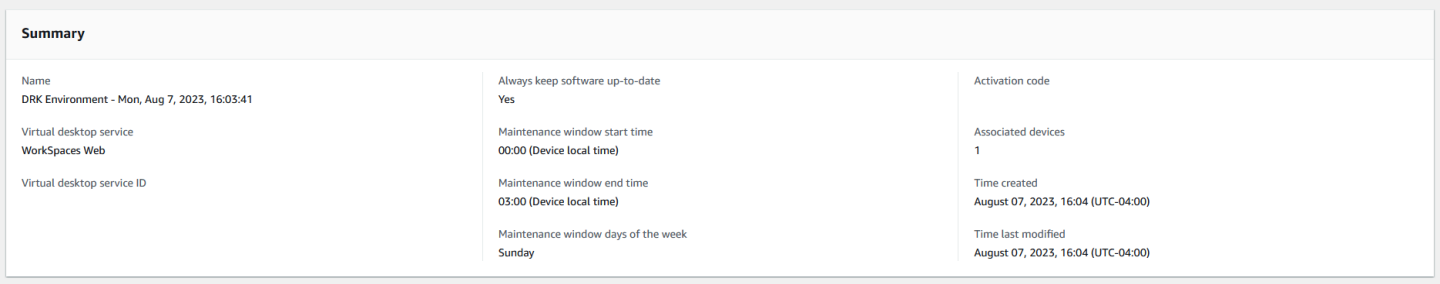
環境を選択すると、WorkSpaces シンクライアントコンソールにその環境の詳細が表示され、確認できるようになります。コンソールには、この環境が使用する仮想デスクトッププロバイダーの詳細も表示されます。

トピック

- 概要
- 仮想デスクトップ環境の詳細

概要

概要セクションでは、WorkSpaces シンクライアント環境の主な機能の概要を説明します。次の表に、概要の各要素とその機能を示します。



要素	説明
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名	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	このコードは、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します。

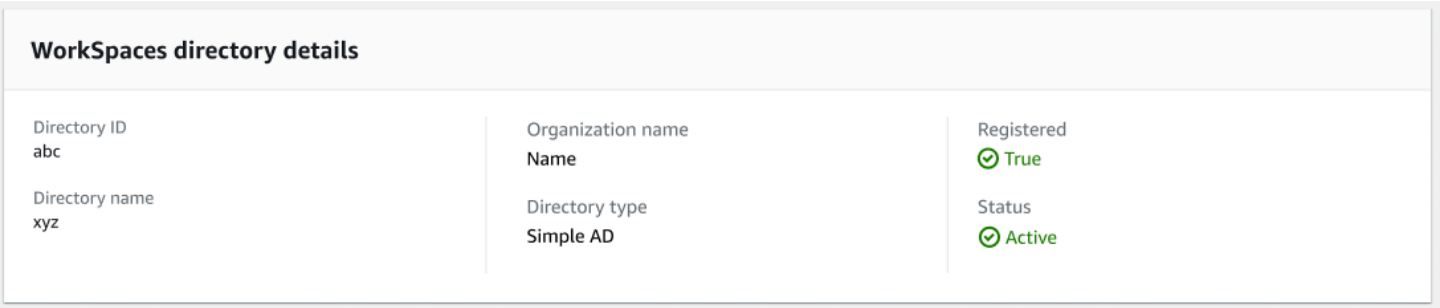
要素	説明
ソフトウェアを常にup-to-date状態に保つ	この設定により、ソフトウェアの自動更新が有効になります。
メンテナンスウィンドウの開始時刻	自動ソフトウェア更新が開始される毎週の時刻。
メンテナンスウィンドウの終了時刻	自動ソフトウェア更新が終了する毎週の時刻。
メンテナンスウィンドウの曜日	自動ソフトウェア更新が発生した日。
関連付けられたデバイス	この環境にアクセスしている WorkSpaces シンクライアントデバイスの数。
作成時刻	この環境が作成された日時。

仮想デスクトップ環境の詳細

WorkSpaces シンクライアント環境は、仮想デスクトップインターフェイスで実行されます。各インターフェイスには、専用環境を制御するさまざまなパラメータのセットがあります。

Amazon WorkSpaces ディレクトリの詳細

Amazon WorkSpaces でAmazon WorkSpacesシンクライアント環境は、ディレクトリを使用して仮想デスクトップを作成および実行します。次の表に、詳細の各要素とその機能を示します。

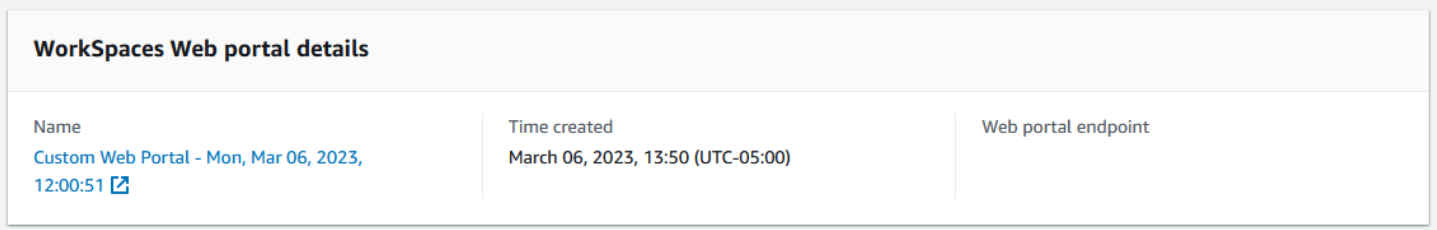


要素	説明
ディレクトリ ID	この環境に関連付けられている Amazon WorkSpaces ディレクトリ。

要素	説明
[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。
[Organization name] (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。
Status	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

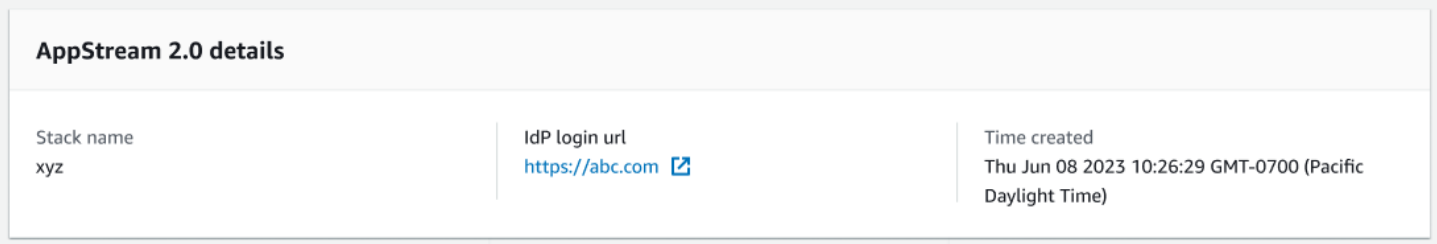
Amazon WorkSpaces Secure Browser でAmazon WorkSpacesシンクライアント環境は、ウェブポータルを使用して仮想デスクトップを作成および実行します。次の表に、詳細の各要素とその機能を示します。



要素	説明
名前	この WorkSpaces Secure Browser ポータルに関連付けられた一意の識別子。
作成時刻	この WorkSpaces Secure Browser ポータルが作成された日時。
ウェブ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。

WorkSpaces アプリケーションの詳細

WorkSpaces シンクライアント環境はWorkSpaces アプリケーション情報スタックで実行され、仮想デスクトップを作成して実行します。次の表に、詳細の各要素とその機能を示します。



要素	説明
スタック名	この WorkSpaces アプリケーションスタックに関連付けられた一意の識別子。
IdP ログイン URL	WorkSpaces アプリケーションスタックへ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。
作成時刻	この WorkSpaces アプリケーション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 シンクライアント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を介した Amazon WorkSpaces
- 割り当てられたスタックを介した WorkSpaces アプリケーション
- 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、新しいサービス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、[ソフトウェアを常に最新の状態に保つ] 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、更新を手動でプッシュするか、ソフトウェアの有効期限が切れてシステムが更新を強制するまで、この環境に登録されたデバイスは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 - 環境ソフトウェアを毎週決められた時刻に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 セキュアブラウザ
   - WorkSpaces アプリケーション

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常に動作するには、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 WorkSpaces の使用

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どのデバイスからでもリソースにアクセスできます。

1. Amazon WorkSpaces を使用するには、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。
   - WorkSpaces ディレクトリの作成ボタンを選択して、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、「WorkSpaces のディレクトリを管理する」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。

WorkSpaces アプリケーションの使用

WorkSpaces Applications 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 AWS 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。

> **Important**
>
> WorkSpaces アプリケーション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. WorkSpaces アプリケーションを設定するには、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。
   - 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。WorkSpaces アプリケーション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、低コストでフルマネージド型の WorkSpaces コンソールで、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設計されています。

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。
   - WorkSpaces Secure Browser 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にセットアップ用の一意のアクティベーションコードが送信されます。

このアクティベーションコードを任意の WorkSpaces シンクライアントデバイスユーザーに提供し、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設定する方法の詳細については、「Amazon 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。

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に移動します。
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。

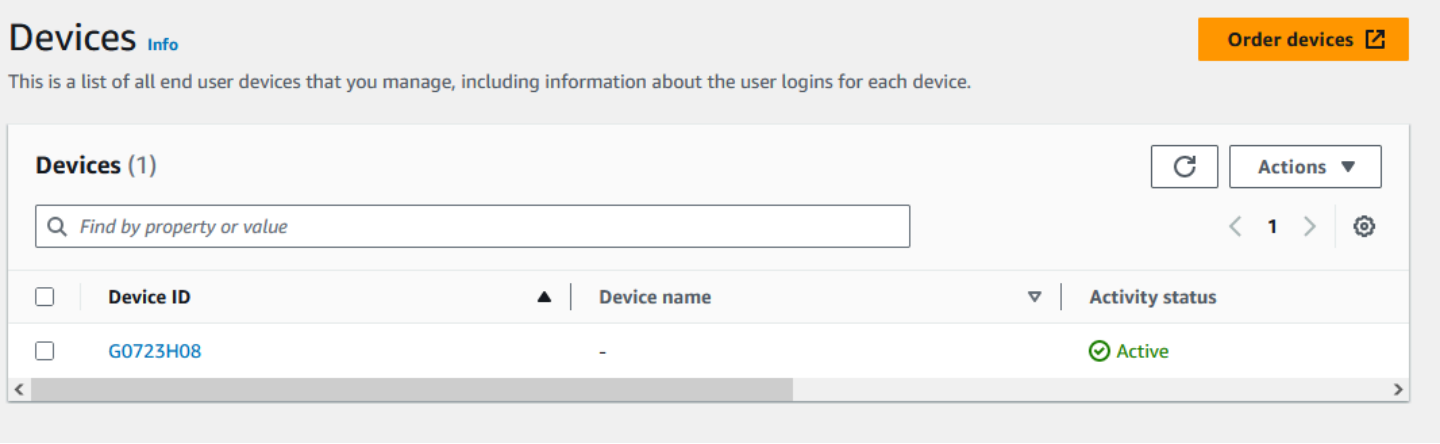
デバイス

WorkSpaces シンクライアントの各エンドユーザーは、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を所有しています。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で管理されます。

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

ネットワーク内の任意のデバイスには、確認できるパラメータと実行できるアクションがいくつかあります。



デバイスリストの詳細

デバイスのパラメータがレビュー用に一覧表示されます。次の表に、概要の各要素とその機能を示します。

要素	説明
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。
デバイス名	(オプション) デバイスに付ける一意の名前。
最終使用者	デバイスにアクセスするユーザーの識別番号。WorkSpaces Personal を使用する場合にのみ使用できます。
アクティビティのステータス	デバイスの現在のステータス。2 つのステータス状態があります。 • 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されています。 • 非アクティブ – 過去 7 日間にネットワークに接続されていません。
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を確認します。次のいずれかの状態になります。 • Registered – これはデフォルトのステータスです。 • 登録解除 — デバイスはリセットおよび登録解除プロセス中です。 **Note** 登録解除状態のデバイスを削除できます。

要素	説明
	• Deregsitered – 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いずれかである場合のみです。 • 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	このデバイスがアタッチ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。2 つのステータス状態があります。 • 準拠 • 非準拠

デバイスリストのアクション

ここから実行できるアクションは多数あります。これらのいずれかを選択して、対応するアクションを実行します。

要素	説明
[検索]	管理す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、以下を実行できます。

要素	説明
	• デバイス名を編集する • 登録解除 • アーカイブ • [Delete] (削除) • デバイスの詳細をエクスポートする
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

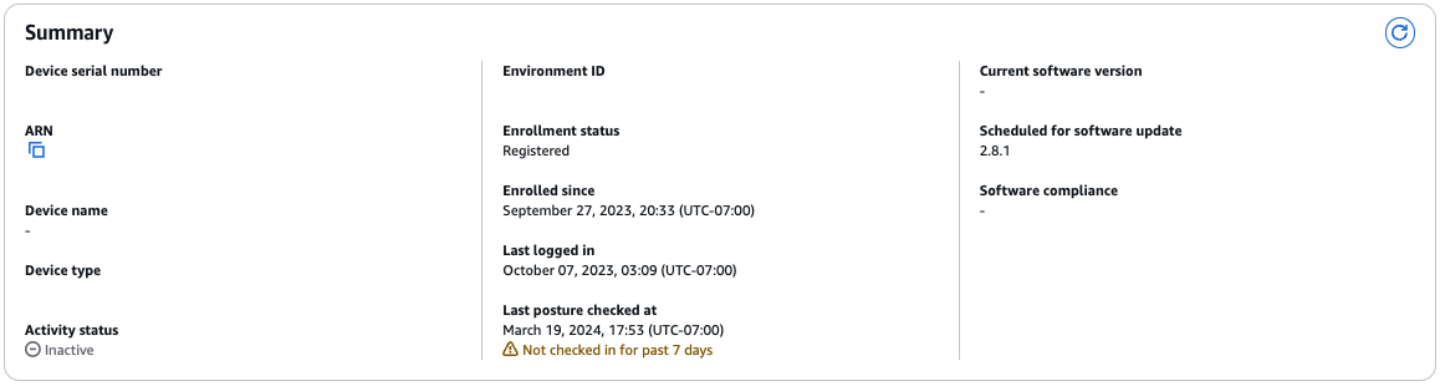
デバイスを選択すると、WorkSpaces シンクライアントコンソールにそのデバイスの詳細が表示され、確認できるようになります。コンソールには、デバイスのネットワークタイプと接続された周辺機器に関する詳細も表示されます。

トピック

- 概要
- デバイス設定
- ユーザーアクティビティ

概要

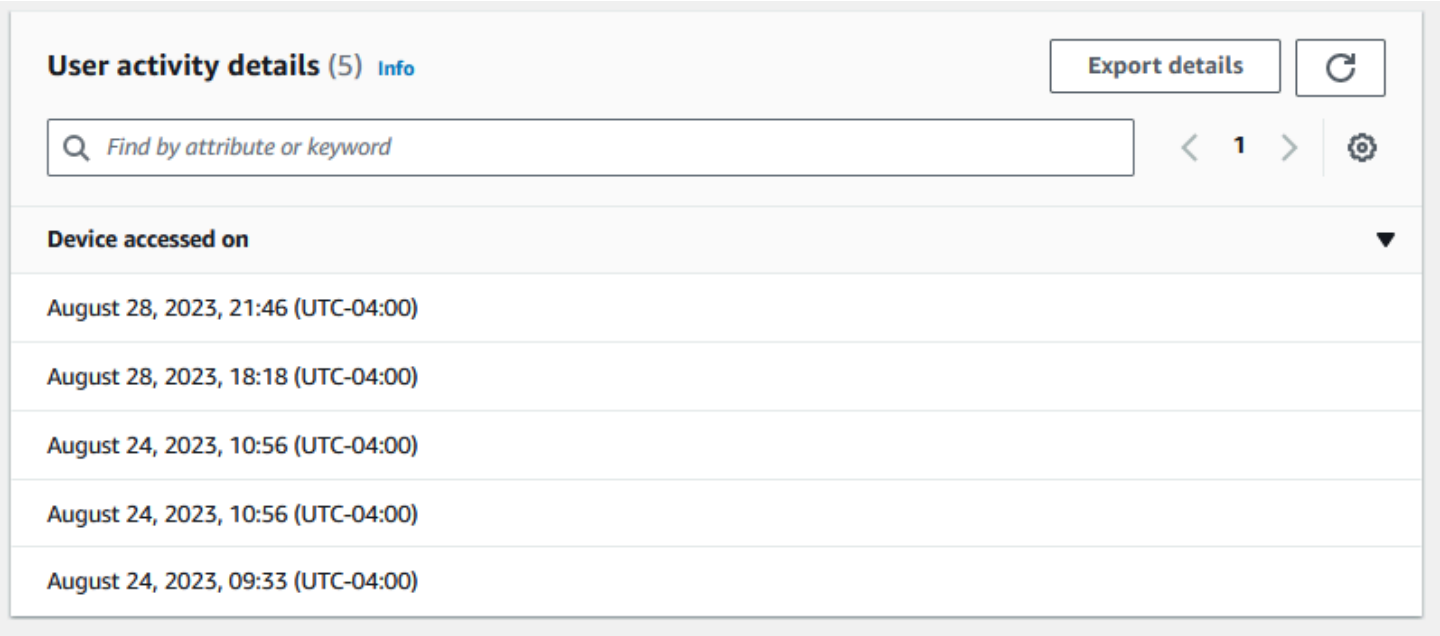
概要セクションでは、WorkSpaces シンクライアントデバイスの主な機能の概要を説明します。次の表に、概要の各要素とその機能を示します。



要素	説明
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	デバイスに付ける名前。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。
アクティビティのステータス	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 • 非アクティブ
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を確認します。これは、次の 4 つの状態のいずれかになります。 • Registered – これはデフォルトのステータスです。

要素	説明
	• 登録解除 — デバイスはリセットおよび登録解除プロセス中です。 • 登録解除済み – 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である場合のみです。 • 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。
以降に登録	デバイスがアクティブ化された日付。
最終ログイン	最新のログイン日時。
で最後にチェックされた姿勢	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	デバイスで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を確認します。2 つのステータス状態があります。 • 準拠 • 非準拠
最終使用者	デバイスにアクセスするユーザーの識別番号。WorkSpaces Personal を使用する場合にのみ使用できます。

ユーザーログ



要素	説明
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。

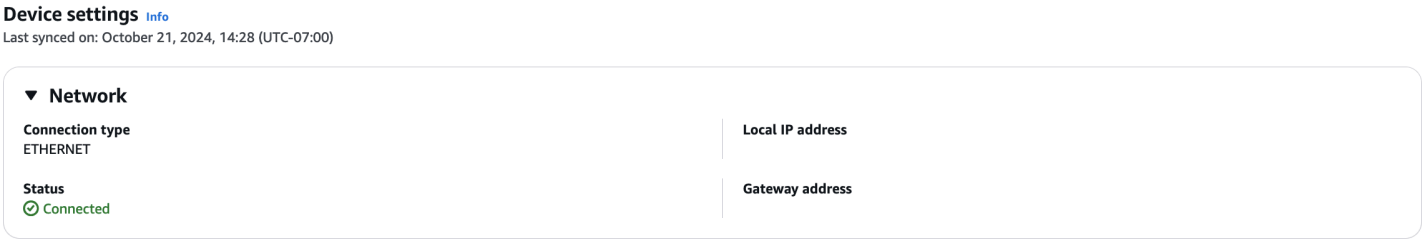
デバイス設定

デバイスのパラメータがレビュー用に一覧表示されます。次の表に、各要素とその機能を示します。

> **Note**
>
> デバイス設定情報は、デバイスがオンラインの場合にのみ更新されます。デバイスがオフラインの場合、一部の情報が古くなっている可能性があります。

見出しとネットワーク

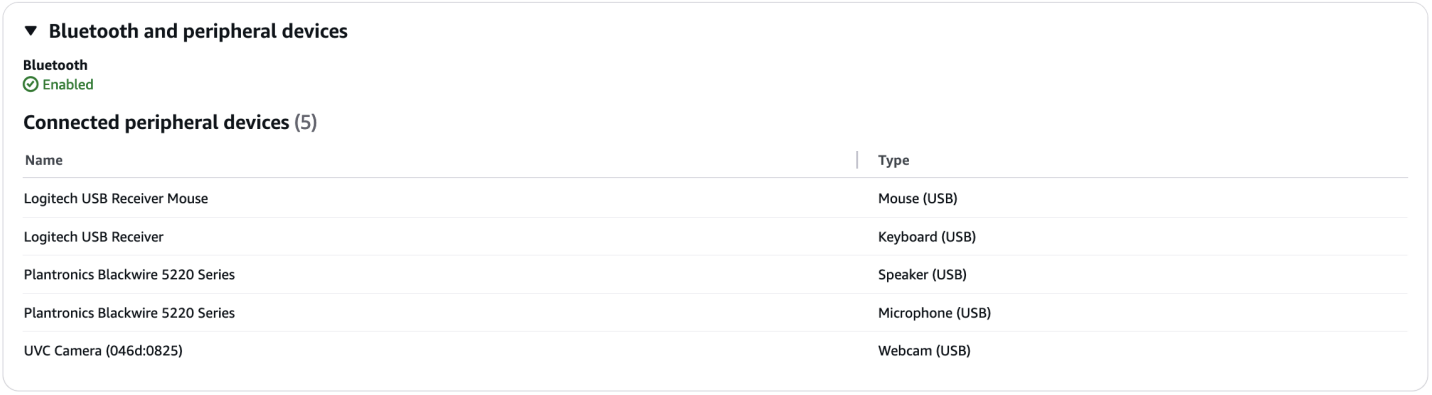
WorkSpaces シンクライアントデバイスの詳細には、デバイスのネットワーク接続の概要が表示されます。次の表に、各要素とその機能を示します。



要素	説明
最終同期日	最新のデバイス設定の日時がコンソールと同期されます。
[接続タイプ]	デバイスが使用するネットワーク接続のタイプ。接続タイプは、イーサネットまたは Wifi のいずれかです。
Status	ネットワークのステータス。デバイスが現在接続されているか、過去 20 分以内に接続されている場合、ステータスは「接続済み」と表示されます。ネットワークが 20 分以上切断されている場合、ステータスは「20 分前に最後に接続された」など、デバイスが最後にインターネットに接続されてから経過した時間を示すように変わります。
ローカル IP アドレス	接続されたネットワークのローカル IP アドレス。
ゲートウェイアドレス	接続されたネットワークのゲートウェイアドレス。

Bluetooth および周辺機器

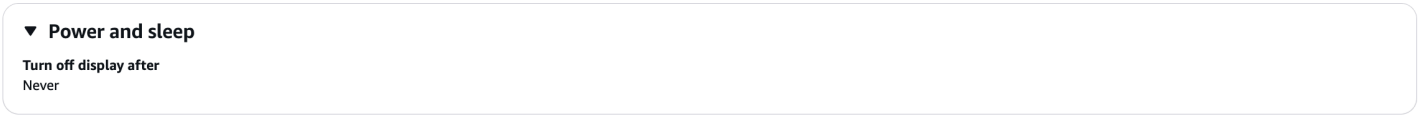
WorkSpaces シンクライアントデバイスの詳細には、デバイスに接続されている周辺機器のリストが表示されます。次の表に、各要素とその機能を示します。



要素	説明
Bluetooth	デバイスの Bluetooth ステータス。2 つのステータス状態は次のとおりです。 • 有効 • 無効
接続された周辺機器	Logitech マウスなどの接続された周辺機器の名前と、マウス (USB) などの接続された周辺機器のタイプのリスト。

電源とスリープ

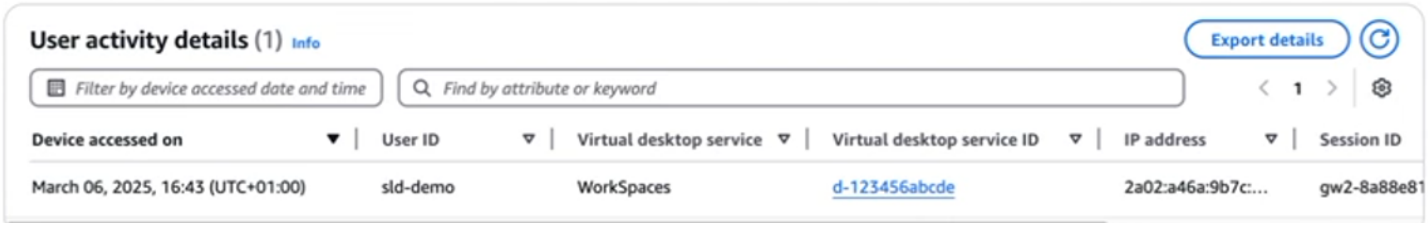
各 WorkSpaces シンクライアントデバイスには省電力モードがあります。次の表に、このモードのステータスを示します。



要素	説明
表示をオフにする	デバイスが表示をオフにするまでの非アクティブ時間。

ユーザーアクティビティ

このタブには、特定のデバイスのセットアップと使用状況に関する情報のログが表示されます。次の表に、このログの各要素を示します。



要素	説明
でアクセスされたデバイス	デバイスがアクティブ化された日時。
ユーザー ID	デバイスにアクセスするユーザーの識別番号。
仮想デスクトップサービス	デバイスが使用する仮想デスクトップサービス。
仮想デスクトップサービス ID	ユーザーに関連付けられた仮想デスクトップサービス ID 番号。
IP アドレス	デバイスにアクセスする IP の識別番号。
イベントタイプ	デバイスの使用方法に関する詳細。

> **Note**
>
> WorkSpaces Personal を除き、VDIs にはログイン開始イベントのみが表示されます。

テーブルの上にある検索バーを使用して、テーブル内の特定の情報を検索できます。テーブルの結果を日時でフィルタリングすることもできます。

詳細のエクスポートボタンを選択して、テーブルを csv ファイルにエクスポートできます。

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**
>
> 登録を解除すると、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。

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を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。

Amazon WorkSpaces シンクライアント - デバイスの使用によって生成されたデータ

Amazon WorkSpaces シンクライアントは、そのクライアントとのやり取りに関するデータを生成して収集します。

データのタイプ: Amazon WorkSpaces シンクライアントは、デバイスのパフォーマンス、使用パターン、および他の AWS サービスとのインタラクションに関するデータを生成します。これには、技術データ (ステータスや設定など) 、使用状況データ (ログインタイムスタンプなど) 、診断データ (必要に応じてシステムログなど) が含まれます。

データ量と収集: 生成されるデータ量は、デバイスとサービスの使用方法によって異なります。データはデバイスのオペレーション中に継続的に収集されます。

データストレージ: デバイスからのデータは、デバイス自体または AWS サーバーに安全に保存されます。構造化された機械読み取り可能な形式で保存されます。

データアクセス: ここに記載されている手順に従って、 AWS アカウントからデバイスデータにアクセスできます。データのダウンロード手順やサービス品質に関する情報などの詳細については、これらのページを参照してください。

データ管理: AWS アカウントを通じてデバイスデータを確認できます。デバイスのデータプラクティスの詳細については、当社のサービス条件とプライバシー通知を参照してください。

データ削除: AWS アカウントを通じてデバイスデータを削除できます。データ保持および削除オプションの詳細については、「デバイスの削除」を参照してください。

他のユーザーとのデータ共有: AWS デバイスデータをサードパーティーと共有しません。当社の Identity and Access Management プロセスを通じて、承認された第三者のみがお客様のデータにアクセスできます。 は、AWS プライバシー通知に含まれる限られたケースで個人データを第三者 AWS と共有します。

ヘルプが必要ですか? カスタマーサポートにアクセスして、サポートチームにお問い合わせください。これは、適用法に基づく苦情を申し立てるお客様の権利を損なうものではありません。

データ所有者: Amazon Web Services EMEA SARL、38 Avenue John F. Kennedy、L-1855、ルクセンブルク

ソフトウェアの更新

WorkSpaces シンクライアントでは、新しい機能を導入し、セキュリティパッチを適用するために、ソフトウェアを定期的に更新する必要があります。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、ソフトウェアアプリケーションまたは WorkSpaces シンクライアントデバイスの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。

ソフトウェアセットには 2 つのタイプがあります。

- 新機能を導入し、欠陥を修正し、一般的な改善を行うソフトウェアセット。これらは毎月リリースされます。
- 重大な問題に対するセキュリティパッチと修正を含むソフトウェアセット。これらは必要に応じてリリースされます。

管理者として、環境で自動ソフトウェア更新を有効にしていない場合、その環境に登録されているデバイスは、更新を手動でプッシュするまでソフトウェア更新を受信しません。

新しいソフトウェアセットがリリースされると、古いソフトウェアセットは期限切れになります。新機能を持つソフトウェアセットのリリース日から、以前のソフトウェアセットの有効期限が切れる 40 日前になります。

デバイスのセキュリティ体制が損なわれないように、期限切れのソフトウェアが検出されると、サービスによってデバイスが自動的に更新されます。このタイプの更新では、メンテナンスウィンドウが適用されず、エンドユーザーが更新を遅延させないため、アクティブなセッションが中断される可能性があります。これを回避するには、ソフトウェアセットを少なくとも 30 日に 1 回更新することをお勧めします。

> **Note**
>
> セキュリティパッチまたは重要な更新を含むソフトウェアセットがリリースされた場合、以前のすべてのソフトウェアセットは 3 日後に期限切れに設定されます。デバイスの安全性を維持し、日常業務の中断を最小限に抑えるために、これらのソフトウェアセットをすぐに更新することをお勧めします。

リリースされた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。

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、以下を実行します。

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、以下を実行します。

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**
>
> 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
2.20.1	11-18-2025	• Chromium の CVE-2025-13223 および CVE-2025-13224 の重要なセキュリティ問題を修正しました。
2.20.0	11-5-2025	• デバイスの認証が改善されました。
2.19.0	9-30-2025	• 再起動、シャットダウン、スリープなどのツールバーアクションでは、エンドユーザーが WorkSpaces で再認証する必要があるようになりました。 • エンドユーザーが Ctrl+Space キーを使用して Excel の列を選択できない問題を修正しました。

ソフトウェアセット	リリース日	変更
		• ロックページとライセンスページの内部 URLs を変更しました。
2.18.0	8-28-2025	• デバイスツールバーにセッション終了ボタンを追加しました。 • デバイスにアクティビティステータス通知が正しく表示されない問題を修正しました。 • セッション認証で FIDO2 のサポートを追加しました。 • 一般的な修正と改善。
2.17.0	7-30-2025	• プラグ可能な USB ハブ UD-3900Z が WorkSpaces シンクライアントでの使用がサポートされるようになりました。 • スペイン語キーボードを使用した AltGr キーのサポートが追加されました。 • デバイスのユーザーセッションアクティビティのエントリが重複する問題を修正しました。 • 数値キーパッドの Enter キーのサポートが追加されました。 • 一般的な修正と改善。

ソフトウェアセット	リリース日	変更
2.16.2	7-22-2025	• Chromium の CVE-2025-6558 の重要なセキュリティ問題を修正しました。
2.16.1	7-3-2025	• Chromium の CVE-2025-6554 の重要なセキュリティ問題を修正しました。
2.16.0	6-27-2025	• ネットワークレイテンシーの通知を追加しました。 • セッション中に暗くなる 2 番目のモニターから回復する機能を追加しました。 • デバイスがスリープモードから戻った後にモニターが白画面を表示するか、自動拡張されない問題を修正しました。
2.15.0	6-19-2025	• ラテンアメリカスペイン語および国際英語キーボードのサポートが追加されました。 • エンドユーザーは、デバイスがキーボードまたはマウスのアクティビティを長時間検出しない場合に通知を表示します。
2.14.1	6-09-2025	• Chromium の CVE-2025-5419 の重要なセキュリティ問題を修正しました。

ソフトウェアセット	リリース日	変更
2.13.0	3-31-2025	• エンドユーザーには、製品満足度フィードバックアンケートが通知として表示されます。 • FIDO2 認証フローのプレリリース機能のサポートを追加しました。FIDO2 セッション前の詳細」を参照してください。 • セッションでオーディオ/ビデオが再生されている場合、デバイスはスリープ状態になりません。 • モニタが接続および切断されると、エンドユーザーに通知が表示されます。 • デバイスは、サービスの改善のためにオペレーティングシステムから診断情報を収集します。 • ソフトウェアのインストール日の設定に誤った日付が表示される問題を修正しました。
2.14.0	4-29-2025	• ユーザビリティの向上とバグ修正。

ソフトウェアセット	リリース日	変更
2.13.0	3-31-2025	• エンドユーザーには、製品満足度フィードバックアンケートが通知として表示されます。 • FIDO2 認証フローのプレリリース機能のサポートを追加しました。FIDO2 セッション前の詳細」を参照してください。 • セッションでオーディオ/ビデオが再生されている場合、デバイスはスリープ状態になりません。 • モニタが接続および切断されると、エンドユーザーに通知が表示されます。 • デバイスは、サービスの改善のためにオペレーティングシステムから診断情報を収集します。 • ソフトウェアのインストール日の設定に誤った日付が表示される問題を修正しました。
2.12.0	1-30-2025	• マウスのバックボタンを押すとエンドユーザーがセッションからログアウトする問題を修正しました。
2.11.2	1-24-2025	• モニター間でマウスを動かす呼び出し中に音声がひび割れる問題を修正しました。

ソフトウェアセット	リリース日	変更
2.11.1	12-27-2024	• デュアルモニターの自動拡張の問題を修正しました。 • VoiceView ラベルの軽微な改善。
2.11.0	12-19-2024	• WorkSpaces シンクライアントが VoiceView と Magnifier をサポートするようになりました。
2.10.0	11-22-2024	• エンドユーザーは、キーボードショートカットを使用してデバイスツールバーを折りたたむことができます。

ソフトウェアセット	リリース日	変更
2.9.0	10-28-2024	• 管理者は、特定のデバイスのデバイスの詳細ページの AWS コンソールでエンドユーザーのデバイス設定を表示できるようになりました。 • WorkSpaces シンクライアントは、単一画面の 2K 解像度モニターをサポートするようになりました。 • エンドユーザーは、WorkSpaces シンクライアントデバイスでネットワーク診断に関連する通知を表示できます。 • エンドユーザーは、必要に応じてデバイスツールバーを左右に配置することができるようになりました。 • スリープ時間またはアイドル時間中にデバイスがソフトウェア更新をインストールしなかった問題を修正しました。
2.8.1	09-26-2024	• デバイスがスリープ状態から起動した後に 2 番目のモニタをオンにできないという重大な問題を修正しました。

ソフトウェアセット	リリース日	変更
2.8.0	09-06-2024	• シンクライアントは、4K 解像度のモニターをサポートしています。 • WorkSpaces シンクライアントデバイス管理サービスが一時的に利用できない場合でも、ユーザーは VDI セッションに接続できます。 • AWS コンソールのユーザーアクティビティの詳細セクションに重複するエントリが表示される問題を修正しました。 • エンドユーザーは、WorkSpaces シンクライアントで WorkSpaces をストリーミングするときに PrintScreen オプションを使用できます。
2.7.1	08-27-2024	• Chromium の CVE-2024-7971 および CVE-2024-7965 の重要なセキュリティ問題のゼロデイ修正。

ソフトウェアセット	リリース日	変更
2.7.0	07-29-2024	• 2 番目のモニターのパフォーマンスが向上しました。 • ツールバー言語がデバイス言語の変更に影響を与えない問題を修正しました。 • デバイスは、サービスの改善のために診断情報を収集するようになりました。
2.6.0	07-09-2024	• ユーザーは、受信するソフトウェア更新を延期して、中断することなく作業を完了できます。 • デバイス設定により、ユーザーは保存された WiFi ネットワークを忘れることができます。 • 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。 • VDI セッションの一部のユーザー設定は、デバイスの再起動後も保持されます。

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、デバイスがスリープ状態から目を覚ましたときにキーボードとマウスのセットアップ画面が短時間表示される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。
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のゼロデイ修正。
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のゼロデイ修正。 • WorkSpaces の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、ブラウザをスタンドアロンモードで開く問題を修正しました。

ソフトウェアセット	リリース日	変更
2.4.0	05-09-2024	• 「accounts.google.com」をブロックし、WorkSpaces アプリケーションセッションの IDP として Google Workspace を使用しない問題を修正しました。 • デバイス設定ツールバーは、画面上の任意の領域をクリックすると自動的に折りたたまれます。
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、表示画面の使用率が向上します。 • 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待機する期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になる問題を修正しました。 • エンドユーザーによって設定され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。

ソフトウェアセット	リリース日	変更
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 認証で設定された WorkSpaces 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。
2.1.2	01-26-2024	• Chromium の CVE-2024-0519 の重要なセキュリティ問題のゼロデイ修正。 • 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。

ソフトウェアセット	リリース日	変更
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は、タグ形式で各リソースに独自のメタデータを割り当てることによって整理および管理できます。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、8 月 1 日までタグは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にする必要があります。
> タグはアクティベーション後 24 時間に表示されますが、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 シンクライアントリソースにその期間中に料金が発生している必要があります。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 :

- WorkSpaces シンクライアント環境を作成するときには、次のリソースにタグを追加できます。
- WorkSpaces シンクライアント環境、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。
- 環境内のデバイスのタグを設定して、デバイスの登録時に自動的に適用されるようにできます。

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 用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管理するには

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、Value 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管理するには

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、Value 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新しいデバイスのタグを管理するには

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、詳細ページを開きます。
3. [編集] を選択します。
4. 「デバイス作成タグ」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、Value 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。

デバイスが作成されると、そのデバイスは環境に登録され、デバイス作成タグが適用されます。これは、新しいデバイス登録中にのみ発生します。さらに、`aws:thinclient:environment-id`システムタグは、値として使用される環境 ID で適用されます。

コンソールを使用してソフトウェア更新のタグを管理するには

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、Value 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 シンクライアントに関するセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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 とお客様の間の責任共有です。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を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、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、当社のセキュリティの有効性を定期的にテストおよび検証。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、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。

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共有責任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ように、WorkSpaces シンクライアント VPN を設定する方法を示します。WorkSpaces シンクライアントリソースのモニタリングと保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

Amazon WorkSpaces シンクライアントにおけるデータ保護

責任 AWS 共有モデル、Amazon WorkSpaces シンクライアントのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。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 アイデンティティセンターまたは 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、API、AWS CLIまたは SDK を使用して WorkSpaces シンクライアントまたは他の 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 WorkSpaces シンクライアントは、WorkSpaces シンクライアントデバイスのユーザー使用と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。例えば、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、デバイス識別情報、クラッシュレポートなどです。この情報は、サービスを提供するために使用され、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、サービスを提供するためにのみ、ユーザーがサービスを使用している AWS リージョンの外部に情報が転送される場合があります。この情報は、AWS プライバシー通知に従って処理されます。

トピック

データ暗号化

WorkSpaces シンクライアントは、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 などの環境とデバイスのカスタマイズデータを収集します。WorkSpaces シンクライアント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、暗号化に AWS Key Management Service (KMS) を使用します。

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。

- 最小特権アクセスを実装し、WorkSpaces シンクライアントアクションに使用する特定のロールを作成します。
- カスタマーマネージドキーを提供することでデータをエンドツーエンドで保護します。これにより、WorkSpaces シンクライアントは保管中のデータを指定したキーで暗号化できます。
- 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。
  - 管理者は、WorkSpaces 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ます。ユーザーは、WorkSpaces 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を入力し、認証情報を使用してストリーミングデスクトップにログインする必要があります。

- 物理的なアクセス権があれば誰でも WorkSpaces シンクライアントをセットアップできますが、有効なアクティベーションコードとログインするためのユーザー認証情報がない限り、セッションを開始することはできません。
- ユーザーは、デバイスツールバーを使用して、画面のロック、再起動、またはデバイスのシャットダウンを選択することで、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 シンクライアントは、 AWS KMS ですべての機密データを暗号化することで、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管中のデータ暗号化

Amazon WorkSpaces シンクライアントは、デフォルトで暗号化を提供し、 AWS 所有の暗号化キーを使用して保管中の機密データを保護します。

- AWS 所有キー — Amazon WorkSpaces シンクライアントは、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。

- カスタマーマネージドキー — Amazon WorkSpaces シンクライアントは、作成、所有、管理する対称カスタマーマネージドキーの使用をサポートし、既存の AWS 所有暗号化に 2 番目の暗号化レイヤーを追加します。この暗号化レイヤーは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 ポリシーの策定と維持
- キーポリシーの有効化と無効化
- キー暗号化マテリアルのローテーション
- 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 シンクライアントがどのように個人を特定できるデータを暗号化するかをまとめたものです。

データ型	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
ユーザーアクティビティ WorkSpaces シンクライアントユーザーのアクティビティ	有効	有効
デバイス設定 WorkSpaces シンクライアントデバイス設定	有効	有効
デバイス作成タグ	有効	有効

データ型	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)
WorkSpaces シンクライアント環境デバイス作成タグ		

> **Note**
>
> Amazon WorkSpaces シンクライアントは、 AWS 所有キーを使用して個人を特定できるデータを無償で保護することで、保管中の暗号化を自動的に有効にします。
> ただし、カスタマーマネージドキーの使用には AWS KMS 料金が適用されます。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 を使用する方法

Amazon WorkSpaces シンクライアントでは、カスタマーマネージドキーを使用するためのキーポリシーが必要です。

Amazon WorkSpaces シンクライアントでは、次の内部オペレーションにカスタマーマネージドキーを使用するためのキーポリシーが必要です。

- KMS AWS に`GenerateDataKey`リクエストを送信してデータを暗号化します。
- KMS AWS に`Decrypt`リクエストを送信して、暗号化されたデータを復号します。

カスタマーマネージドキーへのサービスのアクセスはいつでも削除できます。これを行うと、Amazon WorkSpaces シンクライアントはカスタマーマネージドキーによって暗号化されたすべてのデータにアクセスできなくなり、そのデータに依存しているオペレーションが影響を受けます。例えば、WorkSpaces シンクライアントがアクセスできない環境の詳細を取得しようとすると、オペレーションは`AccessDeniedException`エラーを返します。さらに、WorkSpaces シンクライアントデバイスは WorkSpaces 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、対称カスタマーマネージド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。キーポリシーは、カスタマーマネージドキーの作成時に指定できます。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 シンクライアント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 シンクライアントがキーを検証できるように、カスタマーマネージド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。

Amazon WorkSpaces シンクライアントに追加できるポリシーステートメントの例を以下に示します。

```
{
    "Statement":
    [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                        "arn:aws:thinclient:region:111122223333:*",
                    "kms:EncryptionContext:aws:thinclient:arn":
                        "arn:aws:thinclient:region: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*"
            ],
            "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 シンクライアントのカスタマーマネージドキーの指定

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 シンクライアント が識別可能な個人データを暗号化するために使用する `kmsKeyArn` を指定することでデータキーを指定できます。

- `kmsKeyArn` — KMS AWS カスタマーマネージドキーのキー識別子。キー ARN を提供します。

カスタマーマネージドキーで暗号化された WorkSpaces シンクライアント環境に新しい WorkSpaces シンクライアントデバイスを追加すると、WorkSpaces シンクライアントデバイスは WorkSpaces シンクライアント環境からカスタマーマネージドキー設定を継承します。

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、追加の認証済みデータとして暗号化コンテキストを使用して、認証済み暗号化をサポートします。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、リクエストに同じ暗号化コンテキストを含めます。

Amazon WorkSpaces シンクライアントの暗号化コンテキスト

Amazon WorkSpaces シンクライアントは、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 で、`aws:thinclient:arn`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"
}
```

モニタリングに暗号化コンテキストを使用する

対称カスタマーマネージドキーを使用して WorkSpaces シンクライアント環境を暗号化する場合は、カスタマーマネージドキーがどのように使用されているかを特定するために、暗号化コンテキストを監査記録やログで使用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 CloudWatch Logs によって生成されたログの中にも記載されます。

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。

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 カスタマーマネージドキーを使用すると、 AWS CloudTrail または Amazon CloudWatch Logs 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。

次の例はDescribeKey、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するために Amazon WorkSpaces シンクライアントによって呼び出される KMS オペレーションをモニタリングするための、GenerateDataKey、、Decrypt、 の AWS CloudTrail イベントです。

次の例では、WorkSpaces シンクライアント環境encryptionContextの を確認できます。WorkSpaces シンクライアントデバイスには、同様の CloudTrail イベントが記録されます。

DescribeKey

Amazon WorkSpaces シンクライアントは、 DescribeKeyオペレーションを使用して KMS カスタマーマネージドキーを検証します AWS 。

次に、DescribeKey オペレーションを記録するイベントの例を示します。

```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
```

```
    "eventTime": "2024-04-08T13:44:22Z",
    "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"
}
```


GenerateDataKey

Amazon WorkSpaces シンクライアントは、GenerateDataKey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": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
```

```
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

Amazon WorkSpaces シンクライアントがデバイス情報GenerateDataKeyを保存する場合、GenerateDataKeyオペレーションを使用してデータを暗号化します。

GenerateDataKey オペレーションは、Sid がAmazon WorkSpaces シンクライアントサービスにデータの暗号化と復号を許可する」の KMS キーポリシーステートメントで許可されます。

次のイベント例では、GenerateDataKey オペレーションを記録します。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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。

次に、Decrypt オペレーションを記録するイベントの例を示します。

```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
```

```
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```


Decrypt (by service)

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、Decryptオペレーションを使用してデータを復号化します。Decrypt オペレーションは、Sid が

Amazon WorkSpaces シンクライアントサービスにデータの暗号化と復号を許可する」の KMS キーポリシーステートメントで許可されます。

次のイベント例では、 を介して承認された Decryptオペレーションを記録しますGrant。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
```

```
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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 のセキュリティのベストプラクティス 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。

転送中の暗号化

WorkSpaces シンクライアントは、HTTPS と TLS 1.2 を介して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 呼び出しを使用して WorkSpaces 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 接続を介して送信す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 から WorkSpaces シンクライアントに転送できます。これには、デバイス上のソフトウェア更新も含まれます。

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

独自のカスタマーマネージド AWS KMS キーを指定して、顧客情報を暗号化できます。キーを指定しない場合、WorkSpaces シンクライアントは AWS 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。

インターネットワーク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 シンクライアントの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 で顧客に安全に配信されます。ユーザー情報と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詳細は、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、WorkSpaces のモニ

タリング」、WorkSpaces アプリケーションのモニタリングとレポート」、またはWorkSpaces Web のユーザーアクセスログ記録」を参照してください。

Amazon WorkSpaces シンクライアントの ID およびアクセス管理

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、WorkSpaces シンクライアントのリソースを使用するための認証 (サインイン) および 承認 (アクセス許可の保有) できる人を制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon WorkSpaces シンクライアントと IAM との連携方法
- Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例
- AWS Amazon WorkSpaces シンクライアントの マネージドポリシー
- Amazon WorkSpaces シンクライアント ID とアクセスのトラブルシューティング

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Amazon WorkSpaces シンクライアント ID 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 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Amazon WorkSpaces シンクライアントと IAM との連携方法」を参照してください)
- IAM 管理者 - アクセスを管理するポリシーを記述します (「Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例」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。、IAM ユーザー 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で認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」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、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 AWS アカウント ルートユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID は、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター 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、1 人のユーザーまたは 1 つのアプリケーションに対して特定のアクセス許可を持つ ID です。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用してにアクセスすることを人間のユーザーに要求する AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーのアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーのユースケース」を参照してください。

IAM ロール

IAM ロールは、一時的な認証情報を提供する特定のアクセス許可を持つ ID です。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行されているアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス 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、ID AWS またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられたときにアクセス許可を定義します。は、プリンシパルがリクエストを行うときにこれらのポリシー AWS を評価します。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。

ポリシーを使用して、管理者は、どのプリンシパルがどのリソースに対して、どんな条件でアクションを実行できるかを定義することによって、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成し、それらをユーザーが担うことができるロールに追加します。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

ID ベースのポリシーは、ID (ユーザー、グループ、またはロール) にアタッチする JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ID 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ポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

ID ベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または 管理ポリシー (複数の ID にアタッチされるスタンドアロンポリシー) にすることができます。マネージド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いずれかを選択する」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。例としては、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。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。

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。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。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) - 組織または組織単位の最大限のアクセス許可を AWS Organizationsで指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – アカウント内のリソースで利用できる最大限のアクセス許可を設定します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。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アクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか 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 WorkSpaces シンクライアントと IAM との連携方法

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利用できる IAM の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 の特徴量	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	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	不可

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については、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 ID ベースのポリシー

アイデンティティベースのポリシーのサポート: 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 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、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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。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 ID ベースのポリシーの例

WorkSpaces シンクライアント ID ベースのポリシーの例は、「Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例」でご確認ください。

WorkSpaces シンクライアント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、全体のアカウント、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。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセス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のサポート: あり

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。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、「サービス認可リファレンス」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。

```
thinclient
```

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": [
      "thinclient:action1",
      "thinclient:action2"
         ]
```

WorkSpaces シンクライアント ID ベースのポリシーの例は、「[Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例]」でご確認ください。

WorkSpaces シンクライアントのポリシーリソース

ポリシーリソースのサポート: あり

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。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。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 シンクライアントリソースタイプとその ARNsAmazon WorkSpaces シンクライアントで定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、「Amazon WorkSpaces シンクライアントで定義されているアクション」を参照してください。

WorkSpaces シンクライアント ID ベースのポリシーの例は、「Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例」でご確認ください。

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: あり

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` 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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、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。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、「サービス認可リファレンス」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。どのアクションおよびリソースと条件キーを使用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 ID ベースのポリシーの例は、「Amazon WorkSpaces シンクライアントの ID ベースのポリシーの例」でご確認ください。

WorkSpaces シンクライアントの ACL

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。

ABAC と WorkSpaces シンクライアント

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

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。

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ありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」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コントロール (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一時的な認証情報を使用する

一時的な認証情報のサポート: あり

一時的な認証情報は AWS 、リソースへの短期的なアクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS 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「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」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アクセス許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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: なし

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 のサービスに許可を委任するロールを作成する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: なし

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、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の「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 WorkSpaces シンクライアントの ID 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。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。

これらのサンプルの 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 ポリシーを作成する (コンソール)」を参照してください。

WorkSpaces シンクライアントが定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」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。

トピック

ポリシーに関する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では、 AWS アカウントに費用が発生する場合があります。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 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的な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することで、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 ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。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、最小特権アクセス許可とも呼ばれています。IAM を使用して許可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 でのポリシーとアクセス許可 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。たとえば、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、サービスアクションが などの特定の を通じて使用されている場合に 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 CloudFormation。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。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的なアクセス権限を確保する - 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 でポリシーを検証する 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、MFA をオンにしてセキュリティを強化します。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 を使用した安全な API アクセス 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、最小限のアクセス許可のセットが必要です。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一覧表示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 ユーザーに WorkSpaces シンクライアント設定の表示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。

JSON

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

自分の権限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アタッチ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の作成方法を示します。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権限の付与

この例では、WorkSpaces シンクライアント IAM ユーザーへの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完了するアクセス許可が含まれています。

JSON

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

AWS Amazon WorkSpaces シンクライアントの 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。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパ

ル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

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」を参照してください。

AWS マネージドポリシー: AmazonWorkSpacesThinClientReadOnlyAccess

`AmazonWorkSpacesThinClientReadOnlyAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、WorkSpaces シンクライアントサービスとその依存関係へのフルアクセス許可を付与します。この管理ポリシーの詳細については、AWS 「 管理ポリシーリファレンスガイド」のAmazonWorkSpacesThinClientReadOnlyAccess」を参照してください。

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。

- `thinclient` (WorkSpaces シンクライアント) – すべての WorkSpaces シンクライアントアクションへの読み取り専用アクセスを許可します。
- `workspaces` (WorkSpaces) – WorkSpaces ディレクトリと接続エイリアスを記述するアクセス許可を付与します。これは、WorkSpaces リソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。
- `workspaces-web` (WorkSpaces Secure Browser) – WorkSpaces Secure Browser ポータルとユーザー設定を記述するアクセス許可を付与します。これは、WorkSpaces Secure Browserリソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。
- `appstream` (WorkSpaces アプリケーション) – WorkSpaces アプリケーションスタックを記述するアクセス許可を付与します。これは、WorkSpaces アプリケーションリソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。

JSON

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

```
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

AWS マネージドポリシー: AmazonWorkSpacesThinClientFullAccess

`AmazonWorkSpacesThinClientFullAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、WorkSpaces シンクライアントサービスとその依存関係へのフルアクセス許可を付与します。この管理ポリシーの詳細については、AWS 「 管理ポリシーリファレンスガイド」の[AmazonWorkSpacesThinClientFullAccess]」を参照してください。

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。

- `thinclient` (WorkSpaces シンクライアント) – すべての WorkSpaces シンクライアントアクションへのフルアクセスを許可します。
- `workspaces` (WorkSpaces) – WorkSpaces ディレクトリと接続エイリアスを記述するアクセス許可を付与します。これは、WorkSpaces リソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。
- `workspaces-web` (WorkSpaces Secure Browser) – WorkSpaces Secure Browser ポータルとユーザー設定を記述するアクセス許可を付与します。これは、WorkSpaces Secure Browserリソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。
- `appstream` (WorkSpaces アプリケーション) – WorkSpaces アプリケーションスタックを記述するアクセス許可を付与します。これは、WorkSpaces アプリケーションリソースが WorkSpaces シンクライアントと互換性があることを確認するために使用されます。また、WorkSpaces シンクライアント AWS コンソールでこれらのリソースを表示するためにも使用されます。
- `iam` – WorkSpaces シンクライアントがアカウントにサービスにリンクされたロールを作成できるようにします。このロールにより、WorkSpaces シンクライアントはユーザーに代わって CloudWatch にメトリクスを発行できます。

JSON

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

```
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowCreateServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition": {
```

```
        "StringEquals": {
          "iam:AWSServiceName": "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS マネージドポリシーへの WorkSpaces シンクライアントの更新

変更	説明	日付
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy – 削除されたポリシー	WorkSpaces シンクライアントが AmazonWorkSpacesThinClientMonitoringServiceRolePolicy セクションを削除しました。	2025 年 11 月 12 日
AmazonWorkSpacesThinClientFullAccess - ポリシーを更新 AmazonWorkSpacesThinClientMonitoringServiceRolePolicy - 新しいポリシー	WorkSpaces シンクライアントは、サービスにリンクされたロールを含めるようにポリシーを更新しました。	2025 年 8 月 26 日
AmazonWorkSpacesThinClientReadOnlyAccess - ポリシーを更新	WorkSpaces シンクライアントは、デバイスの詳細と WorkSpaces 接続エイリアスに対する制限された読み取りアクセス許可を含めるようにポリシーを更新しました。	2025 年 1 月 9 日
AmazonWorkSpacesThinClientFullAccess - ポリシーを更新	WorkSpaces シンクライアントは、WorkSpaces 接続エイリアスの読み取りアクセス許可の制限を含めるようにポリシーを更新しました。	2025 年 1 月 9 日

変更	説明	日付
AmazonWorkSpacesThinClientReadOnlyAccess - ポリシーを更新	WorkSpaces シンクライアントは、WorkSpaces アプリケーション、WorkSpaces Web、WorkSpaces の限定的な読み取りアクセス許可を含めるようにポリシーを更新しました。 WorkSpaces	2024 年 8 月 9 日
AmazonWorkSpacesThinClientFullAccess - 新しいポリシー	Amazon WorkSpaces シンクライアントへのフルアクセスと、必要な関連サービスへの制限付きアクセスを提供します。	2024 年 8 月 9 日
AmazonWorkSpacesThinClientReadOnlyAccess - 新しいポリシー	Amazon WorkSpaces シンクライアントとその依存関係への読み取り専用アクセスを提供します。	2024 年 7 月 19 日
WorkSpaces シンクライアントが変更の追跡を開始しました	WorkSpaces シンクライアントは、 AWS 管理ポリシーの変更の追跡を開始しました。	2024 年 7 月 19 日

Amazon WorkSpaces シンクライアント ID とアクセスのトラブルシューティング

以下の情報を使用すると、WorkSpaces シンクライアントおよび IAM での作業中に直面する可能性がある一般的な問題の診断や修正に役立ちます。

トピック

- WorkSpaces シンクライアントでアクションを実行することを許可されていません
- アクセスキーを表示したい
- 管理者として、他の人が WorkSpaces シンクライアントにアクセスできるようする

- 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ことを許可されていません

がアクションを実行する権限がないと AWS マネジメントコンソール 通知した場合は、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 thinclient:*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:
 thinclient:ListDevices on resource: my-thin-client-device
```

この場合、Mateo は thinclient:*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を更新するよう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 を確認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ユーザーに付与できます 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、他の人が WorkSpaces シンクライアントにアクセスできるようする

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ユーザーまたはアプリケーションにアクセス許可を付与する必要があります。 AWS IAM アイデンティティセンター を使用してユーザーとアプリケーションを管理する場合は、アクセスレベルを定義するアクセス許可セットをユーザーまたはグループに割り当てます。アクセス許可セットは、ユーザーまたはアプリケーションに関連付けられている IAM ロールに自動的に IAM ポリシーを作成して割り当てます。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「アクセス許可セット」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していない場合は、アクセスを必要としてい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) を作成する必要があります。次に、WorkSpaces シンクライアントの適切な権限を付与するエンティティにポリシーをアタッチする必要があります。アクセス許可が付与されたら、ユーザーまたはアプリケーション開発者に認証情報を提供します。これらの認証情報を使用して AWSにアクセスします。IAM ユーザー、グループ、ポリシー、アクセス許可の作成の詳細については、「IAM ユーザーガイド」の「IAM アイデンティティ」と「IAM のポリシーとアクセス許可」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権限の付与」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は「Amazon WorkSpaces シンクライアントと IAM との連携方法」を参照してください。

- 所有 AWS アカウント している 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 している別の 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 を参照してください。
- 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使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」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 および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、および高度に冗長なネットワークで接続された複数の物理的に分離および分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。

WorkSpaces シンクライアントは、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能を提供します。

Amazon WorkSpaces シンクライアントの脆弱性分析と管理

設定と IT コントロールは、 AWS とお客様の間で責任を共有します。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 WorkSpaces アプリケーション、WorkSpaces Web とクロスインテグレーションします。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 WorkSpaces アプリケーションでの管理の更新
- Amazon WorkSpaces に関する更新管理
- 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、パフォーマンスを維持する上で重要な部分です。 には、WorkSpaces シンクライアントを監視し、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツール AWS が用意されています。

- 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 コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生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。

トピック

- AWS CloudTrailを使用した Amazon WorkSpaces シンクライアント API 呼び出しのログ記録
- CloudWatch メトリクスを使用して WorkSpaces シンクライアントをモニタリングする

AWS CloudTrailを使用した Amazon WorkSpaces シンクライアント API 呼び出しのログ記録

Amazon WorkSpaces シンクライアントは、ユーザーAWS CloudTrail、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 と統合されています AWS のサービス。CloudTrail は、WorkSpaces シンクライアントへのすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされたコールには、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。CloudTrail で収集された情報を使用して、WorkSpaces シンクライアントに対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト日時などの詳細を確認できます。

すべての Amazon WorkSpaces シンクライアントアクションは CloudTrail によってログに記録され、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`、`DeleteDevice`、`GetSoftwareSet` 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。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

CloudTrail は、アカウント AWS アカウント を作成すると でアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、 AWS リージョンで過去 90 日間に記録された 管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

追跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。を使用して作成された証跡はすべてマルチリージョン AWS マネジメントコンソール です。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。 AWS リージョン アカウントのすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレ

クタが制御します。CloudTrail Lake の詳細については、「 AWS CloudTrail ユーザーガイド」の「Working with AWS CloudTrail Lake」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail の WorkSpaces シンクライアントデータイベント

データイベントは、リソース上またはリソース内で実行されるリソースオペレーションに関する情報を提供します (エンドユーザーによるデバイスの登録など) 。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、CloudTrail はデータイベントをログ記録しません。CloudTrail [イベント履歴] にはデータイベントは記録されません。

追加の変更がイベントデータに適用されます。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail コンソール、または CloudTrail CloudTrail API オペレーションを使用して AWS CLI、WorkSpaces シンクライアントリソースタイプのデータイベントをログに記録できます。データイベントをログに記録する方法の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS マネジメントコンソールを使用したデータイベントのログ記録」および「AWS Command Line Interfaceを使用したデータイベントのログ記録」を参照してください。

次の表に、データイベントをログ記録できる WorkSpaces シンクライアントリソースタイプを示します。データイベントタイプ (コンソール) 列には、CloudTrail コンソールの [データイベントタイプ] リストから選択する値が表示されます。resources.type 値の列には `resources.type`値が表示され、 AWS CLI または CloudTrail APIs。CloudTrail に記録されたデータ API 列には、リソース タイプの CloudTrail にログ記録された API コールが表示されます。

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

eventName、readOnly、および resources.ARN フィールドでフィルタリングして、自分にとって重要なイベントのみをログに記録するように高度なイベントセレクタを設定できます。オブジェクトの詳細については、「AWS CloudTrail API リファレンス」の「AdvancedFieldSelector」を参照してください。

CloudTrail での WorkSpaces シンクライアント管理イベント

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

Amazon WorkSpaces シンクライアントは、すべての WorkSpaces シンクライアントコントロールプレーンオペレーションを管理イベントとして記録します。WorkSpaces シンクライアントが CloudTrail に記録する Amazon WorkSpaces シンクライアントコントロールプレーンオペレーションのリストについては、Amazon WorkSpaces シンクライアント API リファレンス」を参照してください。

WorkSpaces シンクライアントイベントの例

各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 API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

次の例は、RegisterDevice オペレーションを示す CloudTrail イベントを示しています。


```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-06-19T17:13:44Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "RegisterDevice",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "dsn": "G1X11X11111111XX",
```

```
        "activationCode": "xxx1xxx1",
        "model": "AFTGAZL"
      },
      "responseElements": null,
      "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
      "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "eventCategory": "Data"
    }
```

次の例は、UpdateDeviceDetails オペレーションを示す CloudTrail イベントを示しています。

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "UpdateDeviceDetails",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
      "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
```

```
        }
      ],
      "eventType": "AwsServiceEvent",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "serviceEventDetails": {
        "settings": {
          "network": {
            "ethernet": {
              "addresses": [
                {
                  "gateway": "gateway",
                  "localIp": "localIp",
                  "type": "IPV4"
                }
              ],
              "connectionStatus": "NOT_CONNECTED"
            },
            "networkInterfaceInUse": "ETHERNET",
            "wifi": {
              "addresses": [
                {
                  "gateway": "gateway",
                  "localIp": "localIp",
                  "type": "IPV4"
                }
              ],
              "connectionStatus": "NOT_CONNECTED"
            }
          },
          "peripherals": {
            "bluetooth": {
              "enabledStatus": "ENABLED"
            },
            "keyboards": [
              {
                "name": "name",
                "type": "USB"
              }
            ],
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
```

```
            }
          ],
          "sound": {
            "microphones": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "BUILT_IN"
              }
            ],
            "speakers": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "BUILT_IN"
              }
            ]
          },
          "webcams": [
            {
              "name": "name",
              "selectionStatus": "SELECTED",
              "type": "USB"
            }
          ]
        },
        "powerAndSleep": {
          "sleepAfter": "FIFTEEN_MINUTES"
        }
      },
      "updatedAt": "2024-10-21T17:46:27.624Z"
    },
    "eventCategory": "Data"
  }
```


CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

CloudWatch メトリクスを使用して WorkSpaces シンクライアントをモニタリングする

WorkSpaces シンクライアントデバイスと Amazon CloudWatch は統合されているため、WorkSpaces シンクライアントデバイスから出力されるパフォーマンスメトリクスを収集して分析できます。これらのメトリクスは、CloudWatch コンソールまたは CloudWatch コマンドラインインターフェイスを使用して、あるいはプログラムによって CloudWatch API を使用してモニタリングできます。CloudWatch では、メトリックスの指定したしきい値に到達したときのアラームを設定することもできます。

CloudWatchとアラームの使用の詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

前提条件

前提条件はありません。WorkSpaces シンクライアントデバイスが環境に登録されると、デバイスメトリクスの出力が開始されます。

内容

WorkSpaces シンクライアントメトリクス

`AWS/WorkSpacesThinClient` 名前空間には、次のメトリクスが含まれます。

メトリクス	説明	ディメンション	統計	単位
DeviceSession	デバイスセッションに接続されているシンThinClientデバイスの数、またはセッションにないシンクライアントデバイスの数。	desktopType	平均、最小、最大、合計、サンプル数	カウント

メトリクス	説明	ディメンション	統計	単位
ConnectedDevices	現在オンラインの ThinClient デバイスの数。	該当なし	平均、最小、最大、合計、サンプル数	カウント
SoftwareSetVersion	特定のソフトウェアセットバージョンを実行している ThinClient デバイスの数。	softwareSetVersion	平均、最小、最大、合計、サンプル数	カウント
NetworkConnectionEthernet	現在イーサネット経由で接続されている ThinClient デバイスの数。	該当なし	平均、最小、最大、合計、サンプル数	カウント
NetworkConnectionWifi	現在 WiFi 経由で接続されている ThinClient デバイスの数。	該当なし	平均、最小、最大、合計、サンプル数	カウント

WorkSpaces シンクライアントメトリクスのディメンション

ディメンション	説明
desktopType	デバイスで現在セッション中のデスクトップタイプでメトリクスデータをフィルタリングします。ユーザーがデスクトップにログインしていて、デバイスがスリープしていない場合、デバイスはセッション内です。デバイスがセッション内である場合、ディメンション値は WorkSpaces WorkSpacesSecureBrowser 、AppStream など、使用されるデスクトップタイプになります。デバイスがセッ

ディメンション	説明
	ション内にない場合、ディメンション値は NotInSession になります。
softwareSetVersion	デバイスにインストールされているソフトウェアセットのバージョンでメトリクスデータをフィルタリングします。X.Y.Z のディメンションの形式。例: 1.4.2。

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 CloudFormation プロビジョニングして設定します。

を使用すると 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一貫して繰り返しセットアップできます。リソースを一度記述し、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します。

WorkSpaces シンクライアントと 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および設定するには、 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 形式のテキストファイルです。これらのテンプレートは、 CloudFormation スタックで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、CloudFormation デザイナーを使用して 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「CloudFormation Designer 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 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 CloudFormation

詳細については 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
- 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 シンクライアント間の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 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、パブリック IP アドレスがなくても WorkSpaces シンクライアントにアクセスできます。

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 の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管理型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 Guide (AWS PrivateLink ガイド)」の「Access an AWS のサービス using an interface VPC endpoint (インターフェイス VPC エンドポイントを使用して にアクセスする)」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てすべての API アクションの呼び出しをサポートしています。

WorkSpaces シンクライアント用のインターフェイスエンドポイントの作成

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` と指定します。

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、インターフェイスエンドポイントにカスタムエンドポイントポリシーをアタッチします。

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用の 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。インターフェイスエンドポイントにアタッチされると、このポリシーは、すべてのリソースですべてのプリンシパルに、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権を付与します。

```
{
   "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
AWS マネージドポリシー: AmazonWorkSpacesThinClientMonitoringServiceRolePolicy	Amazon WorkSpaces シンクライアントが AmazonWorkSpacesThinClientMonitoringServiceRolePolicy セクションを削除しました。	2025 年 11 月 12 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientMonitoringServiceRolePolicy AWS マネージドポリシー: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 管理ポリシーが追加されました。 Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientFullAccess マネージドポリシーバージョン 3 が追加されました。	2025 年 8 月 26 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientFullAccess マネージドポリシーバージョン 2 が追加されました。	2025 年 1 月 9 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientReadOnlyAccess マネージドポ	2025 年 1 月 9 日

変更	説明	日付
	リシーバージョン 3 が追加されました。	
AWS CloudTrail を使用した Amazon WorkSpaces シンクライアント API コールのログ記録 デバイス設定 Amazon WorkSpaces シンクライアントの保管時のデータ暗号化	データイベントの新しいセクションを追加しました。 デバイス設定の新しいセクションを追加しました。 保管時のデータ暗号化に関する セクションの KMS 情報を更新しました。	2024 年 10 月 28 日
ビジネス継続性	ビジネス継続性とディザスタリカバリに関する新しいセクションを追加しました。	2024 年 9 月 6 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientFullAccess 管理ポリシーが追加されました。	2024 年 8 月 9 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientReadOnlyAccess マネージドポリシーバージョン 2 が追加されました。	2024 年 8 月 9 日
WorkSpaces シンクライアント用の WorkSpaces Personal の設定	新しい WorkSpaces Personal の を更新しました。	2024 年 8 月 7 日

変更	説明	日付
WorkSpaces シンクライアントの WorkSpaces プールの設定	新しい WorkSpaces Pools の新しいセクションを追加しました。	2024 年 8 月 7 日
AWS マネージドポリシー: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces シンクライアントに AmazonWorkSpacesThinClientReadOnlyAccess 管理ポリシーが追加されました。	2024 年 7 月 19 日
AWS Amazon WorkSpaces シンクライアントの マネージドポリシー	Amazon WorkSpaces シンクライアントが変更の追跡を開始しました。	2024 年 7 月 19 日
Amazon WorkSpaces シンクライアント用の WorkSpaces の設定 Amazon WorkSpaces	オペレーティングシステムのリストを更新しました。	2024 年 2 月 12 日
Amazon WorkSpaces シンクライアント用の WorkSpaces アプリケーションの設定 Amazon WorkSpaces	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。