aws

管理ガイド

Amazon WorkSpaces

Amazon WorkSpaces: 管理ガイド

Table of Contents

Amazon とは WorkSpaces

Amazon WorkSpaces では、仮想クラウドベースの Microsoft Windows、Amazon Linux、または Ubuntu Linux デスクトップをユーザー用にプロビジョニングできますWorkSpaces。これは、ハードウェアの調達とデプロイ、または複雑なソフトウェアのインストールの必要性 WorkSpaces を排除します。必要に応じてユーザーをすばやく追加または削除できます。ユーザーは、複数のデバイスまたはウェブブラウザから仮想デスクトップにアクセスできます。

詳細については、「Amazon WorkSpaces」を参照してください。

機能

- オペレーティングシステム (Windows、Amazon Linux、Ubuntu Linux) を選択し、さまざまなハードウェア構成、ソフトウェア構成、AWS リージョンから選択します。詳細については、「Amazon WorkSpaces バンドル」および「」を参照してくださいthe section called “カスタムイメージとバンドルを作成する”。
- プロトコルを選択します: PCoIP または WorkSpaces ストリーミングプロトコル (WSP)。詳細については、「Amazon のプロトコル WorkSpaces」を参照してください。
- に接続 WorkSpace し、中断した右側から集荷します。 WorkSpaces は永続的なデスクトップエクスペリエンスを提供します。
- WorkSpaces は、 の月単位または時間単位の請求の柔軟性を提供します WorkSpaces。詳細については、「 のWorkSpaces 料金」を参照してください。
- Windows デスクトップの場合、お持ちのライセンスとアプリケーションを導入できます。または、AWS Marketplace for Desktop Apps から購入することもできます。
- ユーザー用にスタンドアロンの マネージドディレクトリを作成するか、 WorkSpaces をオンプレミスのディレクトリに接続して、ユーザーが既存の認証情報を使用して社内リソースにシームレスにアクセスできるようにします。詳細については、「ディレクトリ」を参照してください。
- オンプレミスデスクトップの管理 WorkSpaces に使用するのと同じツールを使用して、 を管理します。
- Multi-Factor Authentication (MFA) を使用してセキュリティを強化します。
- AWS Key Management Service (AWS KMS) を使用して、残りのデータ、ディスク I/O、およびボリュームスナップショットを暗号化します。
- ユーザーが にアクセスできる IP アドレスを制御します WorkSpaces。

アーキテクチャ

Windows および Linux の場合 WorkSpaces、各 WorkSpace は Virtual Private Cloud (VPC) とディレクトリに関連付けられ、 およびユーザーの情報を保存および管理します WorkSpaces。詳細については、「the section called “VPC の要件”」を参照してください。ディレクトリは AWS Directory Service によって管理され、次のオプションが提供されます。Simple AD、AD Connector、または AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD とも呼ばれます)。詳細については、AWS Directory Service 管理ガイドを参照してください。

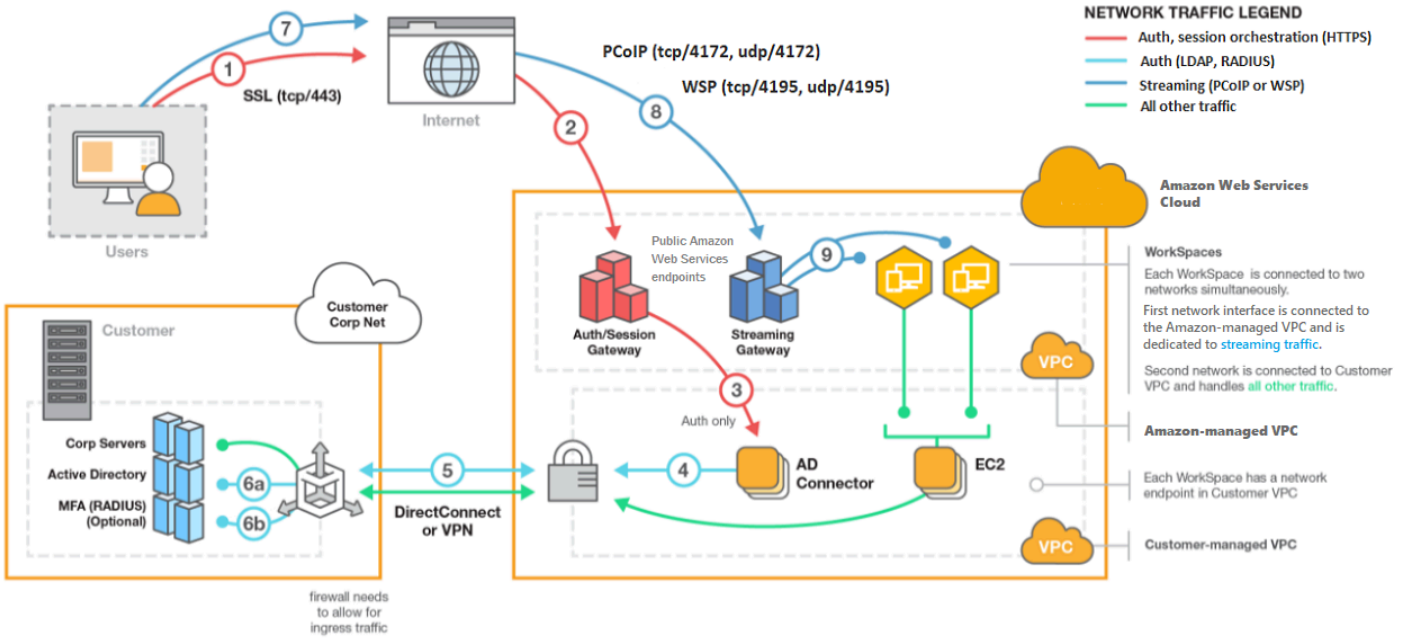
WorkSpaces は、Simple AD、AD Connector、または AWS Managed Microsoft AD ディレクトリを使用してユーザーを認証します。ユーザーは、サポートされているデバイスから、または Windows の場合は WorkSpacesウェブブラウザからクライアントアプリケーション WorkSpaces を使用してにアクセスし、ディレクトリの認証情報を使用してログインします。ログイン情報は認証ゲートウェイに送信され、認証ゲートウェイはトラフィックを の ディレクトリに転送します WorkSpace。ユーザーが認証されると、ストリーミングゲートウェイを介してトラフィックのストリーミングが開始されます。

クライアントアプリケーションは、すべての認証およびセッション関連情報に対して、ポート 443 でHTTPSを使用します。クライアントアプリケーションは、 へのピクセルストリーミングにポート 4172 (PCoIP) WorkSpace とポート 4195 (WSP) を使用し、ネットワークのヘルスチェックにポート 4172 と 4195 を使用します。詳細については、「クライアントアプリケーションのポート」を参照してください。

各 WorkSpace には、管理およびストリーミング用のネットワークインターフェイス (eth0) とプライマリネットワークインターフェイス (eth1) の 2 つの Elastic Network Interface が関連付けられています。プライマリネットワークインターフェイスでは、VPC によって提供された IP アドレスが、ディレクトリで使用されているのと同じサブネットから取得されます。これにより、 からのトラフィックがディレクトリに簡単に到達 WorkSpace できるようになります。VPC 内のリソースへのアクセスは、プライマリネットワークインターフェイスに割り当てられたセキュリティグループによって制御されます。詳細については、「ネットワークインターフェイス」を参照してください。

次の図は、 のアーキテクチャを示しています WorkSpaces。

Amazon WorkSpaces Architectural Diagram



へのアクセス WorkSpace

サポートされているオペレーティングシステムでサポートされているウェブブラウザを使用して、サポートされているデバイスの WorkSpaces クライアントアプリケーションを使用して に接続できます。

> **Note**
>
> ウェブブラウザを使用して Amazon Linux に接続することはできません WorkSpaces。

次のデバイス用のクライアントアプリケーションがあります。

- Windows コンピュータ
- macOS コンピュータ
- Ubuntu Linux 18.04 コンピュータ
- Chromebook
- iPad
- Android デバイス

- Fire タブレット
- ゼロクライアントデバイス (Teradici ゼロクライアントデバイスは PCoIP でのみサポートされます)

Windows、macOS、および Linux PCsでは、次のウェブブラウザを使用して Windows および Ubuntu Linux に接続できます WorkSpaces。

- Chrome 53 以降 (Windows および MacOS のみ)
- Firefox 49 以降

詳細については、「Amazon WorkSpaces ユーザーガイド」のWorkSpaces 「クライアント」を参照してください。

料金

にサインアップするとAWS、無料利用枠の WorkSpacesオファーを利用して WorkSpaces 、 を無料で使い始めることができます。詳細については、「 のWorkSpaces 料金」を参照してください。

では WorkSpaces、使用した分に対してのみ料金が発生します。バンドルと起動 WorkSpaces したの数に基づいて課金されます。の料金 WorkSpaces には、Simple AD と AD Connector の使用が含まれますが、 AWS Managed Microsoft AD の使用は含まれません。

WorkSpaces は、 の月額または時間単位の請求を提供します WorkSpaces。月額請求では、無制限の使用に対して固定料金を支払います。これは、 WorkSpaces フルタイムを使用するユーザーに最適です。時間単位の請求では、 ごとに少額の固定月額料金に加えて WorkSpace、 が実行され WorkSpace ている 1 時間ごとに低い時間料金が発生します。詳細については、「 のWorkSpaces 料金」を参照してください。

サポートされるリージョンの詳細については、「WorkSpaces の料金」をご参照ください。

開始方法

を作成するには WorkSpace、次のいずれかのチュートリアルを試してください。

- WorkSpaces Quick Setup を開始する
- AWS Managed Microsoft AD を使用して WorkSpace を起動する
- Simple AD を使用して WorkSpace を起動する

- AD Connector を使用して WorkSpace を起動する
- 信頼できるドメインを使用して WorkSpace を起動する

Amazon の詳細については、以下のリソースも参照してください WorkSpaces。

- クラウドでのデスクトップのプロビジョニング
- Amazon をデプロイするためのベストプラクティス WorkSpaces
- Amazon WorkSpaces リソース — ホワイトペーパー、ブログ投稿、ウェビナー、re:Invent セッションが含まれます。
- Amazon WorkSpaces FAQs

WorkSpaces Quick Setup を開始する

このチュートリアルでは、WorkSpaces と AWS Directory Service を使用して、仮想かつクラウドベースの Microsoft Windows、Amazon Linux、Ubuntu Linux デスクトップ (WorkSpace とも呼ばれます) をプロビジョニングする方法を学びます。

このチュートリアルでは、Quick Setup オプションを使用して WorkSpace を起動します。このオプションは、WorkSpace を起動したことがない場合にのみ使用できます。または「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

> **Note**
>
> Quick Setup は次の AWS リージョンでサポートされています。
>
> - 米国東部 (バージニア北部)
> - 米国西部 (オレゴン)
> - 欧州 (アイルランド)
> - アジアパシフィック (シンガポール)
> - アジアパシフィック (シドニー)
> - アジアパシフィック (東京)
>
> リージョンを変更するには、「リージョンの選択」を参照してください。

タスク

開始する前に

開始する前に、以下の前提条件を満たしていることを確認してください。

- WorkSpace を作成または管理するには、AWS アカウントが必要です。ユーザーは、WorkSpaces に接続して使用するためであれば AWS アカウントは必要としません。
- WorkSpaces はすべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、WorkSpaces のリージョンを選択します。サポートされるリージョンについては、AWS リージョン別の WorkSpaces の料金を参照してください。

また、次に進む前に、以下について確認して理解しておくことが有益です。

- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。詳細については、「Amazon WorkSpaces バンドル」および「Amazon WorkSpaces の料金」を参照してください。
- WorkSpace を起動するときは、バンドルで使用するプロトコル (PCoIP または WorkSpaces ストリーミングプロトコル [WSP]) を選択する必要があります。詳細については、「Amazon のプロトコル WorkSpaces」を参照してください
- 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の、ユーザーのプロファイル情報を指定する必要があります。パスワードを指定してプロファイルを完成させます。WorkSpace 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、「ディレクトリ」を参照してください

Quick Setup の機能

Quick Setup が、代わりに次のタスクを完了します。

- IAM ロールを作成して、WorkSpaces サービスが Elastic Network Interface を作成し、WorkSpaces ディレクトリの一覧を表示できるようにします。そのロールには、`workspaces_DefaultRole` という名前が付きます。
- 仮想プライベートクラウド (VPC) を作成します。代わりに既存の VPC を使用する場合は、の VPC を設定する WorkSpaces に記載されている要件を満たしていることを確認し、WorkSpaces を使用して仮想デスクトップを起動します。 に記載されているいずれかのチュートリアルの手順に従います。使用する Active Directory のタイプに対応するチュートリアルを選択します。
- VPC で Simple AD ディレクトリを設定し、Amazon WorkDocs に対して有効にします。この Simple AD ディレクトリは、ユーザーと WorkSpace 情報を格納するために使用されます。Quick

Setup で最初に作成される AWS アカウント は、管理者 AWS アカウント です。† ディレクトリには管理者アカウントもあります。詳細については、AWS Directory Service 管理ガイドの「作成されるもの」を参照してください。

- 指定された AWS アカウントを作成してディレクトリに追加します。
- WorkSpacesを作成します。各 WorkSpace には、インターネットアクセスを提供するためのパブリック IP アドレスが割り当てられます。実行モードは常時オンです。詳細については、「WorkSpace の実行モードを管理する」を参照してください
- 指定されたユーザーに招待 E メールを送信します。ユーザが招待メールを受信しない場合は、招待 E メールの送信 を参照してください。

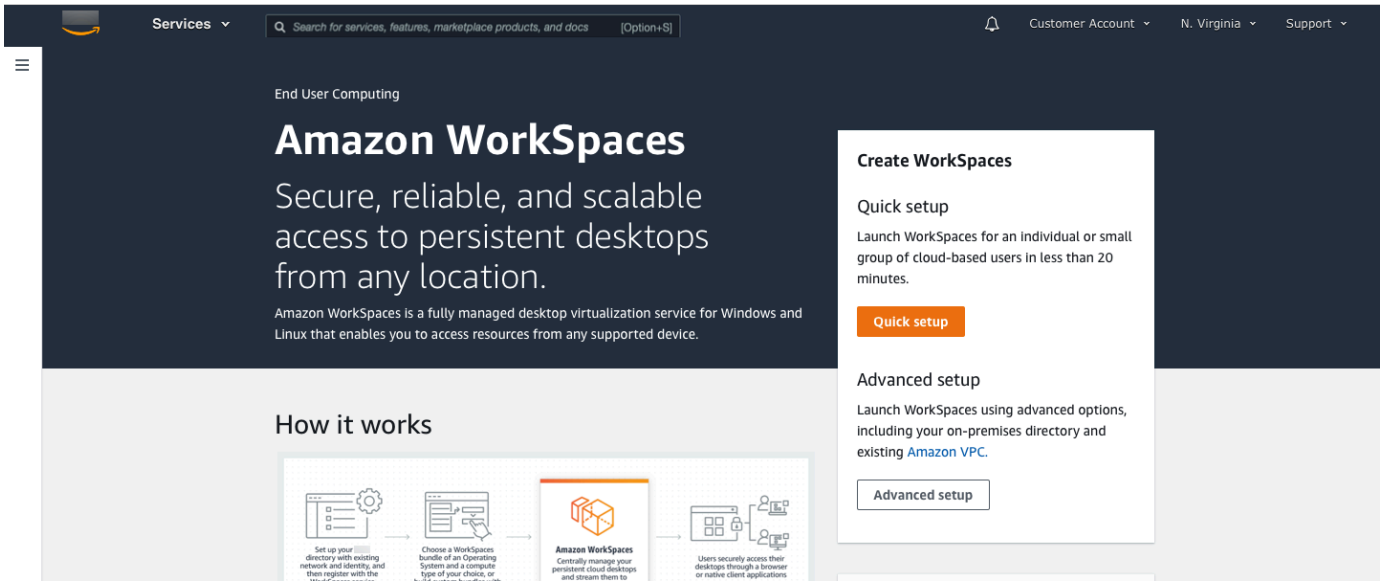
† Quick Setup で最初に作成される AWS アカウント は、管理者 AWS アカウント です。この AWS アカウントを WorkSpaces コンソールから更新することはできません。このアカウントの情報は、他の誰とも共有しないでください。WorkSpaces を使用するように他のユーザーを招待するには、これらのユーザー用の新しい AWS アカウントを作成します。

ステップ 1: WorkSpace の起動

Quick Setup を使用すると、最初の WorkSpace を数分で起動できます。

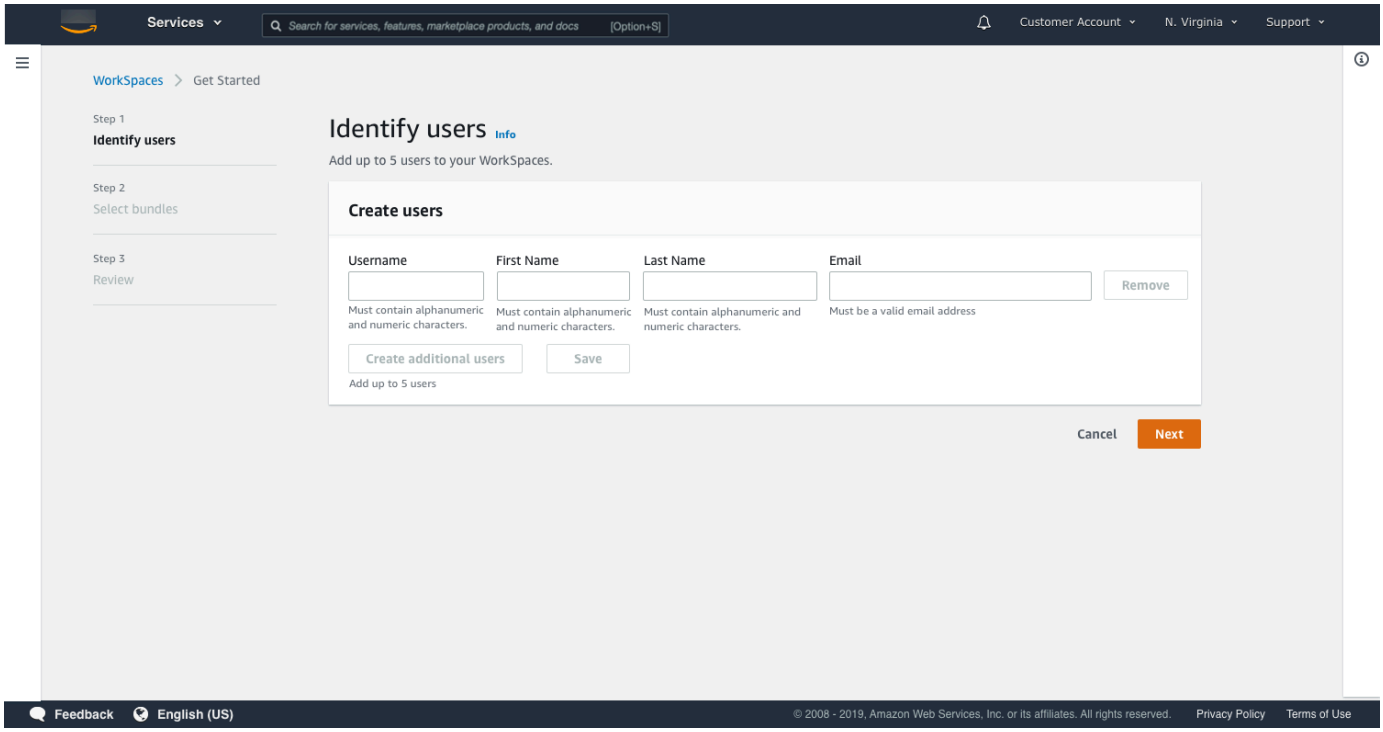
WorkSpace を起動するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. [Quick setup (クイック設定)] を選択します。このボタンが表示されない場合は、このリージョンで既に WorkSpace を起動しているか、Quick Setup をサポートするリージョンを使用していないかのいずれかです。この場合は、WorkSpaces を使用して仮想デスクトップを起動します。を参照してください。

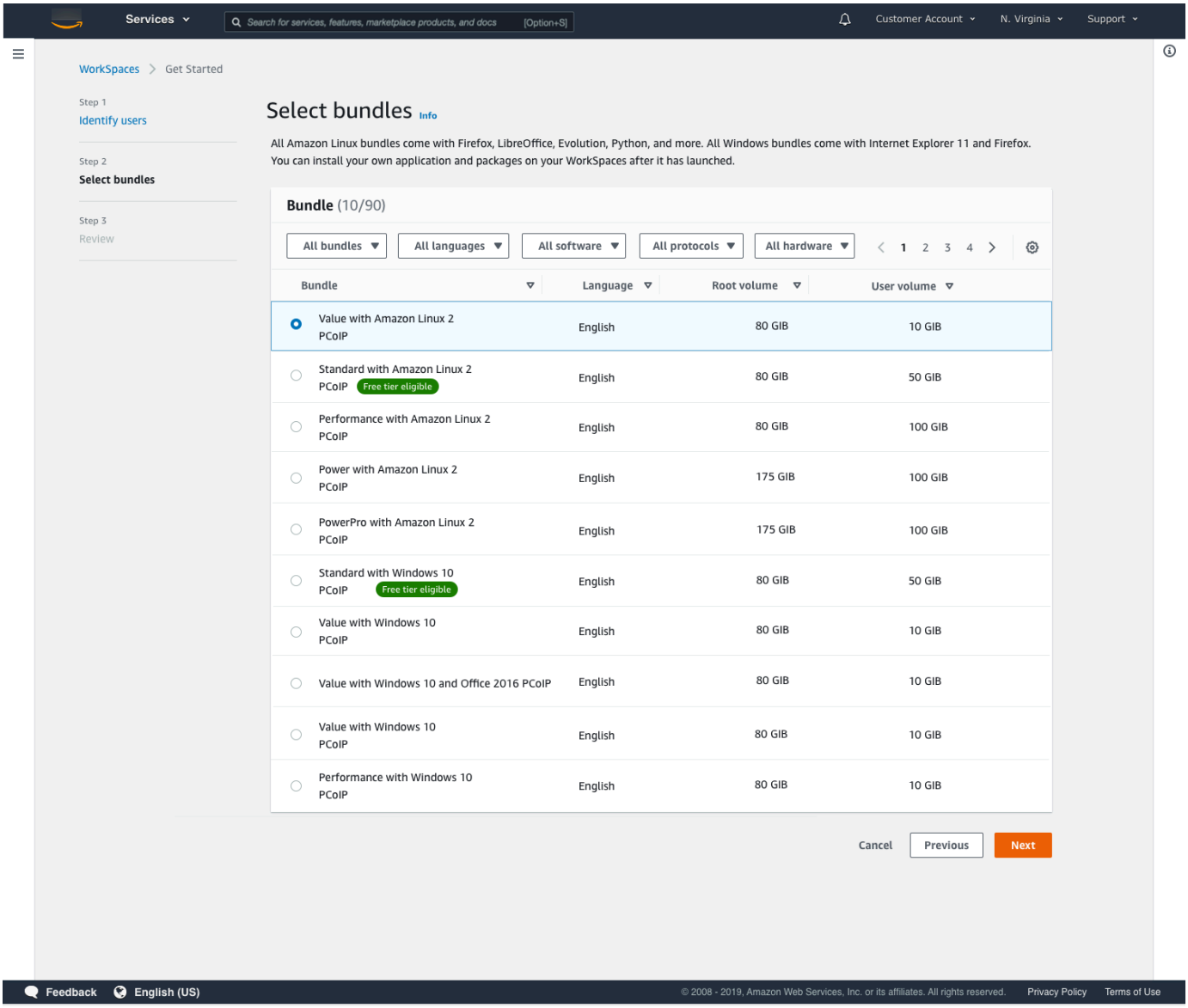


3. [Identify users] (ユーザーの識別) に [Username] (ユーザー名) と [First Name] (名前) を入力します。[Last Name] (姓) および [Emai] (E メール)。続いて、[Next] (次へ) を選択します。

> **Note**
>
> WorkSpaces を初めて使用する場合は、テスト目的でユーザを作成してみることをお勧めします。



4. [Bundles (バンドル)] で、該当するプロトコル (PCoIP または WSP) を使用するユーザーのバンドル (ハードウェアおよびソフトウェア) を選択します。Amazon WorkSpaces で利用できるさまざまなパブリックバンドルの詳細については、Amazon WorkSpaces バンドルを参照してください。



5. 情報を確認します。次に、[Create WorkSpace] (WorkSpace の作成) を選択します。
6. WorkSpace が起動するまでに約 20 分かかります。進行状況を監視するには、左側のナビゲーションペインに移動して [ディレクトリ] を選択します。ディレクトリが作成され、初期ステータスが `REQUESTED` と `CREATING` のディレクトリが表示されます。

   ディレクトリが作成され、ステータスが `ACTIVE` になったら、左側のナビゲーションペインで [WorkSpaces] を選択して、WorkSpace 起動プロセスの進行状況を監視できます。WorkSpace の最初のステータスは `PENDING` です。起動が完了すると、ステータスは `AVAILABLE` になり、各ユーザーに指定した E メールアドレスに招待状が送信されます。ユーザが招待メールを受信しない場合は、招待 E メールの送信 を参照してください。

ステップ 2: WorkSpace に接続する

招待メールを受け取ったら、選択したクライアントを使用して WorkSpace に接続できます。サインインすると、クライアントは WorkSpace デスクトップを表示します。

WorkSpace に接続するには

1. ユーザーの認証情報を設定していない場合は、招待メールのリンクを開き、指示に従います。WorkSpace に接続するために必要なパスワードを覚えておいてください。

   > **Note**
   >
   > パスワードは大文字と小文字が区別され、8〜64 文字の長さにする必要があります。パスワードには、小文字 (a〜z)、大文字 (A〜Z)、数字 (0〜9) の 3 つのカテゴリの少なくとも 1 つの文字と、セット ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ が含まれていなければなりません。

2. 各クライアントの要件の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントを確認し、次のいずれかの操作を行います。

   - プロンプトが表示されたら、クライアントアプリケーションの 1 つをダウンロードするか、Web Access を起動します。
   - プロンプトが表示されず、まだクライアントアプリケーションをインストールしていない場合は、https://clients.amazonworkspaces.com/ を開き、いずれかのクライアントアプリケーションをダウンロードするか、ウェブアクセスを起動します。

   > **Note**
   >
   > ウェブブラウザ (Web Access) を使用して Amazon Linux WorkSpaces に接続することはできません。

3. クライアントを起動し、招待 E メールから登録コードを入力して、[Register] を選択します。
4. サインインするように求められたら、サインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. （オプション）資格情報を保存するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

複数のモニターのセットアップや周辺機器の使用など、クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドのWorkSpaces クライアントおよび周辺機器のサポートを参照してください。

ステップ 3: クリーンアップする (オプション)

このチュートリアルで作成した WorkSpace を終了した場合は、削除することができます。詳細については、「the section called “WorkSpace の削除”」を参照してください

> **Note**
>
> Simple AD は、WorkSpaces で無料でご利用になれます。Simple AD ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> 空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD ディレクトリを削除した後に WorkSpaces を再度ご使用になる際は、いつでも新しいディレクトリを作成できます。

次のステップ

作成した WorkSpace は引き続きカスタマイズできます。たとえば、ソフトウェアをインストールして WorkSpace からカスタムバンドルを作成することができます。WorkSpaces および WorkSpaces ディレクトリに対してさまざまな管理タスクを実行することもできます。詳細については、次のドキュメントを参照してください。

- カスタム WorkSpaces イメージとバンドルを作成する
- の管理 WorkSpaces
- WorkSpaces のディレクトリを管理する

追加の WorkSpaces を作成するには、次のいずれかの操作を行います。

- Quick Setup で作成した VPC と Simple AD ディレクトリを引き続き使用する場合は、「Simple AD を使用して WorkSpace を起動する」チュートリアルの ステップ 2: WorkSpace の作成 セクションにあるステップに従い、追加ユーザー用の WorkSpaces を追加できます。

- 別の種類のディレクトリ、または既存の Active Directory を使用する必要がある場合は、WorkSpaces を使用して仮想デスクトップを起動します。 で関連チュートリアルを参照してください。

複数のモニターのセットアップや周辺機器の使用など、WorkSpaces クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントおよび周辺機器のサポートを参照してください。

WorkSpaces の詳細設定を開始する

このチュートリアルでは、WorkSpaces と AWS Directory Service を使用して、仮想かつクラウドベースの Microsoft Windows または Amazon Linux デスクトップ (WorkSpace とも呼ばれます) をプロビジョニングする方法を学びます。

このチュートリアルでは、詳細設定オプションを使用して WorkSpace を起動します。

> **Note**
>
> 詳細設定は WorkSpaces のすべてのリージョンでサポートされています。

タスク

- 開始する前に
- 詳細設定を使用して WorkSpace を起動する

開始する前に

開始する前に、WorkSpace の作成や管理に使用できる AWS アカウントがあることを確認してください。ユーザーは、WorkSpaces に接続して使用するためであれば AWS アカウントは必要ありません。

以下の概念を確認してから作業を進めてください。

- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。詳細については、「Amazon WorkSpace バンドル」を参照してください。
- WorkSpace を起動するときは、バンドルで使用するプロトコル (PCoIP または WorkSpaces ストリーミングプロトコル [WSP]) を選択する必要があります。詳細については、「Amazon のプロトコル WorkSpaces」を参照してください
- 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の、ユーザーのプロファイル情報を指定する必要があります。パスワードを指定してプロファイルを完成させます。WorkSpace 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、「ディレクトリ」を参照してください

詳細設定を使用して 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/ 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. ディレクトリの情報を確認し、[Create directory] (ディレクトリの作成) を選択します。

WorkSpaces のネットワーキングとアクセス

ネットワーク WorkSpace 管理者は、WorkSpaces のネットワーキングとアクセスについて以下のことを理解する必要があります。

目次

Amazon のプロトコル WorkSpaces

Amazon はPCoIP と WorkSpaces ストリーミングプロトコル (WSP) の 2 つのプロトコル WorkSpaces をサポートしています。選択するプロトコルは、ユーザーがアクセスするデバイスのタイプ WorkSpaces 、 上のオペレーティングシステム、ユーザーが直面する WorkSpacesネットワーク条件、ユーザーが双方向ビデオサポートを必要とするかどうかなど、いくつかの要因によって異なります。

要件

WSP WorkSpaces は、以下の最小要件でのみサポートされています。

ホストエージェントの要件:

- Windows ホストエージェントバージョン 2.0.0.312 以降
- Ubuntu ホストエージェントバージョン 2.1.0.501 以降
- Amazon Linux 2 ホストエージェントバージョン 2.0.0.596 以降

クライアント要件:

- Windows ネイティブクライアントバージョン 5.1.0.329 またはそれ以降
- macOS ネイティブクライアントバージョン 5.5.0 以降
- Web Access

WorkSpace クライアントバージョンとホストエージェントバージョンを確認する方法の詳細については、よくある質問を参照してください。

WSP を使用する場合

- エンドユーザーのネットワーク状態をサポートするために、損失/レイテンシーの許容値を高くする必要がある場合。例えば、世界中の距離 WorkSpaces にわたって にアクセスしたり、信頼できないネットワークを使用しているユーザーがいます。
- ユーザーがスマートカードで認証したり、セッション内でスマートカードを使用したりする必要がある場合。
- セッション内でウェブカメラサポート機能が必要な場合。
- Windows Server 2019 搭載 WorkSpaces バンドルで Web Access を使用する必要がある場合。
- Ubuntu を使用する必要がある場合 WorkSpaces。
- Windows 11 BYOL を使用する必要がある場合 WorkSpaces。
- Ubuntu GPU ベースのバンドル (Graphics.g4dn および GraphicsPro.g4dn) を使用する必要がある場合。
- ユーザーが YubiKey や Windows Hello などの WebAuthn 認証機関でセッション中の認証を必要とする場合。

PCoIP を使用すべき場合

- iPad または Android の Linux クライアントを使用する場合。
- Teradici ゼロクライアントデバイスを使用する場合。
- GPU ベースのバンドル (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または GraphicsPro) を使用する必要がある場合。
- スマートカード以外のユースケースに Linux バンドルを使用する必要がある場合。
- 中国 (寧夏) リージョン WorkSpaces で を使用する必要がある場合。

> **Note**
>
> - ディレクトリには、PCoIP と WSP を混在 WorkSpaces させることができます。
> - 2 つの WorkSpaces が別々のディレクトリにある WorkSpace 限り、ユーザーは PCoIP と WSP の両方を持つことができます。同じユーザーが WorkSpace 、同じディレクトリに PCoIP と WSP を持つことはできません。ユーザー用に複数の を作成する方法の詳細については、 WorkSpaces 「」を参照してくださいユーザー用に複数の WorkSpaces を作成する。
> - 2 つのプロトコル WorkSpace 間で を移行するには、 の再構築が必要な WorkSpaces 移行機能を使用します WorkSpace。詳細については、「の移行 WorkSpace」を参照してください。
> - WorkSpace が PCoIP バンドルで作成された場合は、ルートボリュームを保持したまま、再構築を必要とせずに 2 つのプロトコル間で移行するようにストリーミングプロトコルを変更できます。詳細については、「プロトコルの変更」を参照してください。
> - ビデオ会議を最大限に活用するには、電源または PowerPro バンドルのみを使用することをお勧めします。

の VPC を設定する WorkSpaces

WorkSpaces は Virtual Private Cloud (VPC) WorkSpaces で を起動します。

用の 2 つのプライベートサブネット WorkSpaces とパブリックサブネット内の NAT ゲートウェイを持つ VPC を作成できます。または、 用に 2 つのパブリックサブネットを持つ VPC を作成し WorkSpaces 、パブリック IP アドレスまたは Elastic IP アドレスを各 に関連付けることもできます WorkSpace。

VPC 設計上の考慮事項の詳細については、VPCs とネットワークのベストプラクティス」および WorkSpaces 「デプロイのベストプラクティス WorkSpaces - VPC 設計」を参照してください。

内容

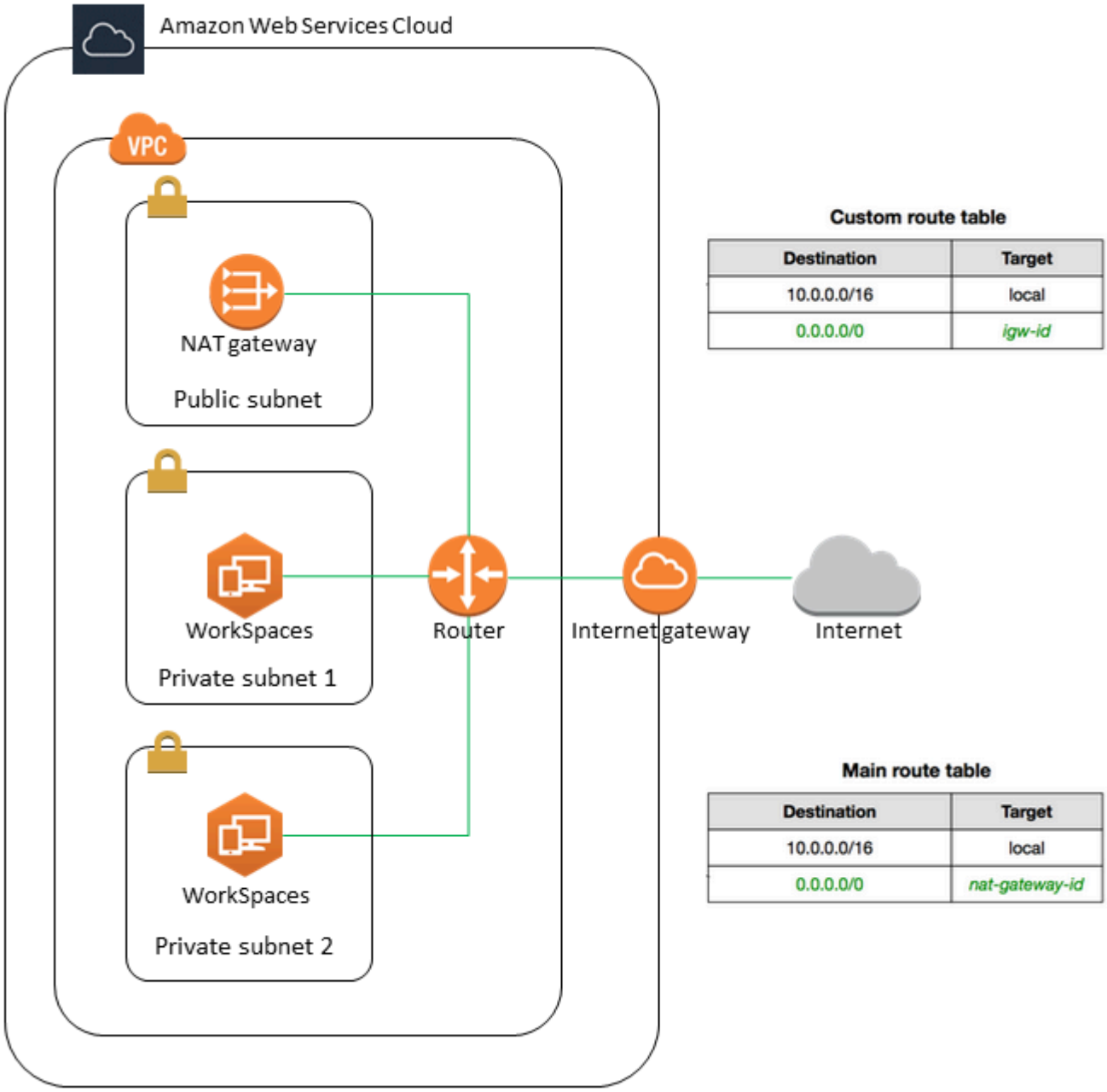
要件

VPC のサブネットは、 を起動するリージョン内の異なるアベイラビリティーゾーンに存在する必要があります WorkSpaces。アベイラビリティーゾーンとは、他のアベイラビリティーゾーンで発生した障害から切り離すために作られた場所です。個別のアベイラビリティーゾーンでインスタンスを起動することにより、1 つの場所で発生した障害からアプリケーションを保護できます。各サブネットが完全に 1 つのアベイラビリティーゾーン内に含まれている必要があり、1 つのサブネットが複数のゾーンに、またがることはできません。

> **Note**
>
> Amazon WorkSpaces は、サポートされている各リージョンのアベイラビリティーゾーンのサブセットで使用できます。に使用している VPC のサブネットに使用できるアベイラビリティーゾーンを確認するには WorkSpaces、「」を参照してくださいAmazon のアベイラビリティーゾーン WorkSpaces。

プライベートサブネットの VPC および NAT ゲートウェイを設定する

AWS Directory Service を使用して AWS Managed Microsoft または Simple AD を作成する場合は、1 つのパブリックサブネットと 2 つのプライベートサブネットを使用して VPC を設定することをお勧めします。プライベートサブネットで WorkSpaces を起動するようにディレクトリを設定します。プライベートサブネット WorkSpaces で へのインターネットアクセスを提供するには、パブリックサブネットで NAT ゲートウェイを設定します。



1 つのパブリックサブネットと、2 つのプライベートサブネットを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [Create VPC (VPC の作成)] を選択します。
3. Resources to create (作成するリソース) で、VPC only (VPC など) を選択します。
4. [名前タグの自動生成] に、VPC の名前を入力します。

5. サブネットを設定するには、次の操作を行います。

   a. [アベイラビリティーゾーンの数] で、ニーズに応じて [1] または [2] を選択します。
   b. [AZ のカスタマイズ] を展開し、アベイラビリティーゾーンを選択します。それ以外の場合は、 によって自動的に AWS 選択されます。適切な選択を行う方法については、「Amazon のアベイラビリティーゾーン WorkSpaces」を参照してください。
   c. [パブリックサブネットの数] で、アベイラビリティーゾーンごとに 1 つのパブリックサブネットがあることを確認します。
   d. [プライベートサブネットの数] で、アベイラビリティーゾーンごとに 1 つのプライベートサブネットがあることを確認します。
   e. 各サブネットの CIDR ブロックに入力します。詳細については、Amazon VPC ユーザーガイドの「サブネットのサイズ設定」を参照してください。
6. [NAT ゲートウェイ] には、[1 per AZ] (AZ あたり 1)を選択します。
7. [Create VPC (VPC の作成)] を選択します。

IPv6 CIDR ブロック

IPv6 CIDR ブロックを VPC とサブネットに関連付けることができます。ただし、サブネットで起動されたインスタンスに IPv6 アドレスを自動的に割り当てるようにサブネットを設定した場合、グラフィックスバンドルを使用することはできません。(ただし、Graphics.g4dn、 GraphicsPro.g4dn、および GraphicsPro バンドルを使用できます。) この制限は、IPv6 をサポートしない旧世代のインスタンスタイプのハードウェア制限から発生します。

この問題を回避するには、Graphics バンドルを起動する前に WorkSpaces サブネットで IPv6 アドレスの自動割り当て設定を一時的に無効にし、Graphics バンドルを起動した後にこの設定を再度有効に (必要に応じて) して、他のバンドルが目的の IP アドレスを受信できるようにします。

デフォルトでは、[auto-assign IPv6 addresses (IPv6 アドレスの自動割り当て)] 設定は無効になっています 。Amazon VPC コンソールからこの設定を確認するには、ナビゲーションペインで [Subnets] (サブネット) を選択します。サブネットを選択し、[アクション]、[自動割り当て IP 設定の変更] の順に選択します。

パブリックサブネットを持つ VPC を設定する

必要に応じて、2 つのパブリックサブネットを持つ VPC を作成できます。パブリックサブネット WorkSpaces で へのインターネットアクセスを提供するには、Elastic IP アドレスを自動または手動で各 に割り当てるようにディレクトリを設定します WorkSpace。

タスク

- ステップ 1: VPC を作成する
- ステップ 2: にパブリック IP アドレスを割り当てる WorkSpaces

ステップ 1: VPC を作成する

次のように、1 つのパブリックサブネットを持つVPCを作成します。

VPC を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. [Create VPC (VPC の作成)] を選択します。
3. Resources to create (作成するリソース) で、VPC only (VPC など) を選択します。
4. [名前タグの自動生成] に、VPC の名前を入力します。
5. サブネットを設定するには、次の操作を行います。
   a. [アベイラビリティゾーンの数] で、[2] を選択します。
   b. [AZ のカスタマイズ] を展開し、アベイラビリティーゾーンを選択します。それ以外の場合は、 によって自動的に AWS 選択されます。適切な選択を行う方法については、「Amazon のアベイラビリティーゾーン WorkSpaces」を参照してください。
   c. [Number of public subnets] (パブリックサブネットの数) で 2 を選択します。
   d. [Number of private subnets] (プライベートサブネットの数) には、[0] を選択します。
   e. パブリックサブネットごとに CIDR ブロックを入力します。詳細については、Amazon VPC ユーザーガイドの「サブネットのサイズ設定」を参照してください。
6. [Create VPC (VPC の作成)] を選択します。

IPv6 CIDR ブロック

IPv6 CIDR ブロックを VPC とサブネットに関連付けることができます。ただし、サブネットで起動されたインスタンスに IPv6 アドレスを自動的に割り当てるようにサブネットを設定した場合、グラフィックスバンドルを使用することはできません。(ただし、 GraphicsPro バンドルは使用できます。) この制限は、IPv6 をサポートしない旧世代のインスタンスタイプのハードウェア制限から発生します。

この問題を回避するには、Graphics バンドルを起動する前に WorkSpaces サブネットで IPv6 アドレスの自動割り当て設定を一時的に無効にし、Graphics バンドルの起動後にこの設定を再度有効にして (必要に応じて) 、他のバンドルが目的の IP アドレスを受け取るようにします。

デフォルトでは、[auto-assign IPv6 addresses (IPv6 アドレスの自動割り当て)] 設定は無効になっています 。Amazon VPC コンソールからこの設定を確認するには、ナビゲーションペインで [Subnets] (サブネット) を選択します。サブネットを選択し、[アクション]、[自動割り当て IP 設定の変更] の順に選択します。

ステップ 2: にパブリック IP アドレスを割り当てる WorkSpaces

パブリック IP アドレスは、 WorkSpaces 自動または手動で に割り当てることができます。自動割り当てを使用するには、the section called “自動パブリック IP アドレスを設定する” を参照してください。パブリック IP アドレスを手動で割り当てるには、以下の手順を使用します。

パブリック IP アドレスを手動で に割り当てるには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. の行を展開 WorkSpace し (矢印アイコンを選択) 、WorkSpace IP の値を書き留めます。これは、 のプライマリプライベート IP アドレスです WorkSpace。
4. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
5. ナビゲーションペインで Elastic IP を選択します。使用可能な Elastic IP アドレスがない場合は、[Allocate Elastic IP address] (Elastic IP アドレスの割り当て) を選択し、[Amazon's pool of IPv4 addresses] (Amazon の IPv4 アドレスプール) または [Customer owned pool of IPv4 addresses] (顧客所有の IPv4 アドレスのプール) を選択し、[Allocate] (割り当て) を選択します。新しい IP アドレスを書き留めます。
6. ナビゲーションペインで、[ネットワークインターフェイス] を選択します。
7. のネットワークインターフェイスを選択します WorkSpace。のネットワークインターフェイスを検索するには WorkSpace、検索ボックスに WorkSpace IP 値 (先ほど書き留めた値) を入力し、Enter キーを押します。WorkSpace IP 値は、ネットワークインターフェイスのプライマリプライベート IPv4 アドレスと一致します。ネットワークインターフェイスの VPC ID は VPC WorkSpaces の ID と一致することに注意してください。
8. [Actions]、[Manage IP Addresses] の順に選択します。[Assign new IP (新しい IP を割り当てる)] を選択し、[Yes, Update (はい、更新します)] を選択します。新しい IP アドレスを書き留めます。

9. [Actions]、[Associate Address] の順に選択します。
10. [Associate Elastic IP Address (Elastic IP アドレスを関連付ける)] ページで、[Address (アドレス)] から Elastic IP アドレスを選択します。[Associate to private IP address (プライベート IP アドレスに関連付ける)] で、新しいプライベート IP アドレスを指定し、[Associate Address (アドレスを関連付ける)] を選択します。

Amazon のアベイラビリティーゾーン WorkSpaces

Amazon で使用する Virtual Private Cloud (VPC) を作成する場合 WorkSpaces、VPC のサブネットは、 を起動するリージョン内の異なるアベイラビリティーゾーンに存在する必要があります WorkSpaces。アベイラビリティーゾーンとは、他のアベイラビリティーゾーンで発生した障害から切り離すために作られた場所です。個別のアベイラビリティーゾーンでインスタンスを起動することにより、1 つの場所で発生した障害からアプリケーションを保護できます。各サブネットが完全に 1 つのアベイラビリティーゾーン内に含まれている必要があります。1 つのサブネットが複数のゾーンにまたがることはできません。

アベイラビリティーゾーンは、リージョンコードとそれに続く文字識別子によって表されます (us-east-1a など)。リソースがリージョンのアベイラビリティーゾーン全体に分散されるように、アベイラビリティーゾーンは各 AWS アカウントの名前に個別にマッピングされます。例えば、us-east-1a AWS アカウントのアベイラビリティーゾーンが別の AWS アカウントus-east-1aと同じ場所ではない場合があります。

アカウント間でアベイラビリティーゾーンを調整するには、アベイラビリティーゾーンの一意で一貫性のある識別子である AZ ID を使用する必要があります。例えば、 use1-az2はus-east-1リージョンの AZ ID であり、すべての AWS アカウントで同じ場所にあります。

AZ ID を表示すると、あるアカウントのリソースの場所を別のアカウントのリソースに対して決定できます。たとえば、AZ ID use1-az2 のアベイラビリティーゾーンにあるサブネットを別のアカウントと共有する場合、このサブネットは AZ ID が同じく use1-az2 であるアベイラビリティーゾーンのそのアカウントでも利用できます。各 VPC とサブネットの AZ ID は Amazon VPC コンソールに表示されます。

Amazon WorkSpaces は、サポートされている各リージョンのアベイラビリティーゾーンのサブセットでのみ使用できます。次の表に、各リージョンで使用できる AZ ID を示します。アカウント内のアベイラビリティーゾーンへの AZ ID のマッピングを確認するには、AWS RAM ユーザーガイドのリソースの AZ ID を参照してください。

リージョン名	リージョンコード	サポートされる AZ ID
米国東部 (バージニア北部)	us-east-1	use1-az2, use1-az4, use1-az6
米国西部 (オレゴン)	us-west-2	usw2-az1, usw2-az2, usw2-az3
アジアパシフィック (ムンバイ)	ap-south-1	aps1-az1, aps1-az2, aps1-az3
アジアパシフィック (ソウル)	ap-northeast-2	apne2-az1 , apne2-az3
アジアパシフィック (シンガポール)	ap-southeast-1	apse1-az1 , apse1-az2
アジアパシフィック (シドニー)	ap-southeast-2	apse2-az1 , apse2-az3
アジアパシフィック (東京)	ap-northeast-1	apne1-az1 , apne1-az4
カナダ (中部)	ca-central-1	cac1-az1, cac1-az2
欧州 (フランクフルト)	eu-central-1	euc1-az2, euc1-az3
欧州 (アイルランド)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
欧州 (ロンドン)	eu-west-2	euw2-az2, euw2-az3
南米 (サンパウロ)	sa-east-1	sae1-az1, sae1-az3
アフリカ (ケープタウン)	af-south-1	afs1-az1, afs1-az2, afs1-az3
イスラエル (テルアビブ)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (米国西部)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3

リージョン名	リージョンコード	サポートされる AZ ID
AWS GovCloud （米国東部）	us-gov-east-1	usge1-az1 , usge1-az2 , usge1-az3

アベイラビリティーゾーンと AZ IDsAmazon EC2 ユーザーガイド」の「リージョン、アベイラビリティーゾーン、ローカルゾーン」を参照してください。

の IP アドレスとポートの要件 WorkSpaces

に接続するには WorkSpaces、 WorkSpaces クライアントが接続されているネットワークで、さまざまな AWSのサービス (サブセットにグループ化) の IP アドレス範囲に対して特定のポートが開いている必要があります。これらのアドレス範囲は、AWS リージョンごとに異なります。これらと同じポートが、クライアントで実行されているファイアウォールで開かれている必要があります。異なるリージョンの AWS IP アドレス範囲の詳細については、「Amazon Web Services 全般のリファレンス」の「AWS IP アドレスの範囲」を参照してください。

アーキテクチャ図については、WorkSpaces 「アーキテクチャ」を参照してください。その他のアーキテクチャ図については、「Amazon をデプロイするためのベストプラクティス WorkSpaces」を参照してください。

クライアントアプリケーションのポート

WorkSpaces クライアントアプリケーションには、次のポートでのアウトバウンドアクセスが必要です。

ポート 53 (UDP)

このポートは、DNS サーバーにアクセスするために使用されます。クライアントがパブリックドメイン名を解決できるように、DNS サーバーの IP アドレスを公開している必要があります。ドメイン名の解決のために DNS サーバーを使用していない場合、このポート要件はオプションです。

ポート 443 (TCP)

このポートは、クライアントアプリケーションの更新、登録、認証に使用されます。デスクトップクライアントアプリケーションはポート 443 (HTTPS) トラフィックのプロキシサーバーの使用をサポートします。プロキシサーバーの使用を有効にするには、クライアントアプリケーション

を開き、[Advanced Settings] で、[Use Proxy Server] をオンにし、プロキシサーバーのアドレスとポートを指定して、[Save] を選択します。

このポートは、次の IP アドレス範囲に開放する必要があります。

- AMAZON リージョンの GLOBAL サブセット。
- WorkSpace があるリージョンのAMAZONサブセット。
- AMAZON リージョンの us-east-1 サブセット。
- AMAZON リージョンの us-west-2 サブセット。
- S3 リージョンの us-west-2 サブセット。

ポート 4172 (UDP と TCP)

このポートは、PCoIP WorkSpaces の WorkSpace デスクトップとヘルスチェックのストリーミングに使用されます。このポートは、PCoIP ゲートウェイと、 WorkSpace があるリージョンのヘルスチェックサーバーに対して開いている必要があります。詳細については、「ヘルスチェックサーバー と PCoIP ゲートウェイサーバー」を参照してください。

PCoIP WorkSpaces の場合、デスクトップクライアントアプリケーションはプロキシサーバーの使用も、UDP のポート 4172 トラフィック (デスクトップトラフィック用) の TLS 復号化および検査もサポートしていません。ポート 4172 に直接接続する必要があります。

ポート 4195 (UDP と TCP)

このポートは、ストリーミングプロトコル (WSP) の WorkSpace デスクトップとヘルスチェック WorkSpaces のストリーミングに使用されます WorkSpaces。このポートは、 WorkSpace があるリージョンの WSP Gateway IP アドレス範囲とヘルスチェックサーバーに対して開いている必要があります。詳細については、「ヘルスチェックサーバー と WSP ゲートウェイサーバー」を参照してください。

WSP の場合 WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) と macOS クライアントアプリケーション (バージョン 5.4 以降) はポート 4195 TCP トラフィックの HTTP プロキシサーバーの使用をサポートしますが、プロキシの使用は推奨されません。TLS の復号および検査はサポートしていません。詳細については、「Windows WorkSpaces 、Amazon Linux 、および Ubuntu のインターネットアクセス用のデバイスプロキシサーバー設定を構成する」を参照してください。 WorkSpaces WorkSpaces

> **Note**
>
> - ファイアウォールがステートフルフィルタリングを使用している場合、リターン通信用に一時ポート (ダイナミックポートとも呼ばれる) が自動的に解放されます。ファイアウォールがステートレスフィルタリングを使用する場合には、リターン通信用に一時ポートを明示的に開放する必要があります。開く必要のある一時ポート範囲は、構成によって異なります。
> - プロキシサーバー機能は UDP トラフィックではサポートされていません。プロキシサーバーを使用することを選択した場合、クライアントアプリケーションが Amazon WorkSpaces サービスに対して行う API コールもプロキシされます。API コールとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

Web Access のポート

WorkSpaces ウェブアクセスには、次のポートへのアウトバウンドアクセスが必要です。

ポート 53 (UDP)

このポートは、DNS サーバーにアクセスするために使用されます。クライアントがパブリックドメイン名を解決できるように、DNS サーバーの IP アドレスを公開している必要があります。ドメイン名の解決のために DNS サーバーを使用していない場合、このポート要件はオプションです。

ポート 80 (UDP と TCP)

このポートは `https://clients.amazonworkspaces.com` への最初の接続に使用され、その後に HTTPS に切り替えられます。これは、 WorkSpace があるリージョンのEC2サブセット内のすべての IP アドレス範囲に対して開いている必要があります。

ポート 443 (UDP と TCP)

このポートは、HTTPS を使用して登録および認証に使用されます。これは、 WorkSpace があるリージョンのEC2サブセット内のすべての IP アドレス範囲に対して開いている必要があります。

ポート 4195 (UDP と TCP)

WorkSpaces ストリーミングプロトコル (WSP) 用に WorkSpaces 設定された の場合、このポートは WorkSpaces デスクトップトラフィックのストリーミングに使用されます。このポートは、WSP ゲートウェイ IP アドレス範囲に開放する必要があります。詳細については、「WSP ゲートウェイサーバー」を参照してください。

WSP ウェブアクセスは、ポート 4195 の TCP トラフィックに対するプロキシサーバーの使用をサポートしていますが、お勧めしません。詳細については、「Windows WorkSpaces 、Amazon Linux 、および Ubuntu のインターネットアクセス用のデバイスプロキシサーバー設定を構成する」を参照してください。 WorkSpaces WorkSpaces

> **Note**
>
> ファイアウォールがステートフルフィルタリングを使用している場合、リターン通信用に一時ポート (ダイナミックポートとも呼ばれる) が自動的に解放されます。ファイアウォールがステートレスフィルタリングを使用する場合には、リターン通信用に一時ポートを明示的に開放する必要があります。解放する必要のある一時ポート範囲は、構成によって異なります。

通常、ウェブブラウザはトラフィックのストリーミングに使用する高範囲内のソースポートをランダムに選択します。 WorkSpaces Web Access は、ブラウザが選択するポートを制御できません。このポートへのリターントラフィックが許可されていることを確認する必要があります。

許可リストに追加するドメインと IP アドレス

WorkSpaces クライアントアプリケーションが WorkSpaces サービスにアクセスできるようにするには、クライアントがサービスにアクセスしようとしているネットワークの許可リストに次のドメインと IP アドレスを追加する必要があります。

許可リストに追加するドメインと IP アドレス

カテゴリ	ドメインまたは IP アドレス
キャプチャ	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	• https://d2td7dqidlhjx7.cloudfront.net/ • AWS GovCloud （ 米国西部) リージョン ： https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/WorkSpacesAppCastx64.xml
接続の確認	https://connectivity.amazonworkspaces.com/

カテゴリ	ドメインまたは IP アドレス
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com • https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • AWS GovCloud （ 米国西部) リージョン：

カテゴリ	ドメインまたは IP アドレス
	https://skylight-client-ds.us-gov-west-1.amazonaws.com • AWS GovCloud（米国東部) リージョンの場合： https://skylight-client-ds.us-gov-east-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • https://ws-client-service.eu-west-1.amazonaws.com • https://ws-client-service.eu-west-2.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com • AWS GovCloud（ 米国西部) リージョン：

カテゴリ	ドメインまたは IP アドレス
	https://ws-client-service.us-gov-west-1.amazonaws.com • AWS GovCloud（米国東部) リージョンの場合： https://ws-client-service.us-gov-east-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/*<region>*/*<directory ID>* MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • Legacy — https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> • 米国東部 (バージニア北部) — https://d2h1yryv1jxiq.cloudfront.net/ • 米国西部 (オレゴン) — https://d1fq42e1gi7rtq.cloudfront.net/ • アジアパシフィック (ムンバイ) — https://d1ctsk4u02kky7.cloudfront.net/ • アジアパシフィック (ソウル) — https://dyoj3cw6iktvg.cloudfront.net • アジアパシフィック (シンガポール) — https://d1525ef92caquk.cloudfront.net/ • アジアパシフィック (シドニー) — https://dodwxjr2amr8p.cloudfront.net/

カテゴリ	ドメインまたは IP アドレス
	• アジアパシフィック (東京) — https://d3v7kcib8ir2e1.cloudfront.net/ • カナダ (中部) — https://d1ebdk07rro1qy.cloudfront.net/ • 欧州 (フランクフルト) — https://d39q4y7cndearu.cloudfront.net/ • 欧州 (アイルランド) — https://d2127w6wvrc6l3.cloudfront.net/ • 欧州 (ロンドン) — https://df4ahgpxbxqy2.cloudfront.net/ • 南米 (サンパウロ) — https://d2nezqurrjvain.cloudfront.net/ • アフリカ (ケープタウン) — https://dr6ry0pwaoy23.cloudfront.net • イスラエル (テルアビブ) — https://d2kmf63k5sit88.cloudfront.net ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 米国東部 (バージニア北部) — https://d32i4gd7pg4909.cloudfront.net/ • 米国西部 (オレゴン) — https://d18af777lco7lp.cloudfront.net/ • アジアパシフィック (ムンバイ) — https://d78hovzzqqtsb.cloudfront.net/ • アジアパシフィック (ソウル) — https://dtyv4uwoh7ynt.cloudfront.net/

カテゴリ	ドメインまたは IP アドレス
	• アジアパシフィック (シンガポール) — https://d3qzmd7y07pz0i.cloudfront.net/ • アジアパシフィック (シドニー) — https://dwcpoxuuza83q.cloudfront.net/ • アジアパシフィック (東京) — https://d2c2t8mxjhq5z1.cloudfront.net/ • カナダ (中部) — https://d2wfbsypmqjmog.cloudfront.net/ • 欧州 (フランクフルト) — https://d1whcm49570jjw.cloudfront.net/ • 欧州 (アイルランド) — https://d3pgffbf39h4k4.cloudfront.net/ • 欧州 (ロンドン) — https://d16q6638mh01s7.cloudfront.net/ • 南米 (サンパウロ) — https://d2lh2qc5bdoq4b.cloudfront.net/ • アフリカ (ケープタウン) — https://di5ygl2cs0mrh.cloudfront.net/ • イスラエル (テルアビブ) — https://d1a3pnge9on3sx.cloudfront.net AWS GovCloud（米国西部) リージョン： • お客様のディレクトリ設定: https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID> • お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
	• ログインページのスタイル設定に使用される CSS ファイル: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript ログインページの ファイル : 該当しない AWS GovCloud （ 米国東部) リージョンの場合 : • お客様のディレクトリ設定: https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> • お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: https://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com • ログインページのスタイル設定に使用される CSS ファイル: https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • JavaScript ログインページの ファイル : 該当しない
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	ドメインまたは IP アドレス
セッション前のスマートカード認証エンドポイント	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin.amazonaws-us-gov.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン) AWS GovCloud（米国西部) および AWS GovCloud（米国東部) リージョン： https://login.us-gov-home.awsapps.com/directory/<directory id>/ (<directory id> はお客様のドメインです）

カテゴリ	ドメインまたは IP アドレス
WS ブローカー	ドメイン: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com • https://ws-broker-service.ap-south-1.amazonaws.com • https://ws-broker-service.ap-northeast-2.amazonaws.com • https://ws-broker-service.ap-southeast-1.amazonaws.com • https://ws-broker-service.ap-southeast-2.amazonaws.com • https://ws-broker-service.ap-northeast-1.amazonaws.com • https://ws-broker-service.ca-central-1.amazonaws.com • https://ws-broker-service.eu-central-1.amazonaws.com • https://ws-broker-service.eu-west-1.amazonaws.com • https://ws-broker-service.eu-west-2.amazonaws.com • https://ws-broker-service.sa-east-1.amazonaws.com • https://ws-broker-service.af-south-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
	• https://ws-broker-service.il-central-1.amazonaws.com • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
WorkSpaces SAML Single Sign-On (SSO) のエンドポイント	ドメイン: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-west-1.amazonaws.com/v1/report-heartbeat

カテゴリ	ドメインまたは IP アドレス
	• https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips.us-gov-east-1.amazonaws.com/v1/report-heartbeat

PCoIP の許可リストに追加するドメインと IP アドレス

カテゴリ	ドメインまたは IP アドレス
PCoIP Session Gateway (PSG)	PCoIP ゲートウェイサーバー
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
	• https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com

カテゴリ	ドメインまたは IP アドレス
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access は現在、アジアパシフィック (ムンバイ) リージョンではご利用いただけません。 • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Web Access は現在、アフリカ (ケープタウン) リージョンではご利用いただけません。 • Web Access は現在、イスラエル (テルアビブ) リージョンではご利用いただけません。

WorkSpaces ストリーミングプロトコル (WSP) の許可リストに追加するドメインと IP アドレス

カテゴリ	ドメインまたは IP アドレス
WSP セッションゲートウェイ (WSG)	WSP ゲートウェイサーバー
WSP のWeb Access TURN サーバー	WSP ゲートウェイサーバー

ヘルスチェックサーバー

WorkSpaces クライアントアプリケーションは、ポート 4172 および 4195 でヘルスチェックを実行します。これらのチェックでは、TCP または UDP トラフィックが WorkSpaces サーバーからクライアントアプリケーションにストリーミングされるかどうかを検証します。これらのチェックが正常に完了するには、ファイアウォールポリシーで、以下のリージョン別ヘルスチェックサーバーの IP アドレスへのアウトバウンドトラフィックを許可する必要があります。

リージョン	ヘルスチェックホスト名	IP アドレス
米国東部 (バージニア北部)	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
米国西部 (オレゴン)	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
アジアパシフィック (ムンバイ)	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
アジアパシフィック (ソウル)	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105

リージョン	ヘルスチェックホスト名	IP アドレス
		52.78.44.253 52.79.54.102
アジアパシフィック (シンガポール)	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
アジアパシフィック (シドニー)	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
アジアパシフィック (東京)	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
カナダ (中部)	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
欧州 (フランクフルト)	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
欧州 (アイルランド)	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224

リージョン	ヘルスチェックホスト名	IP アドレス
欧州 (ロンドン)	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
南米 (サンパウロ)	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
アフリカ (ケープタウン)	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
イスラエル (テルアビブ)	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43
AWS GovCloud （米国西部）	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88

リージョン	ヘルスチェックホスト名	IP アドレス
AWS GovCloud（米国東部）	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP ゲートウェイサーバー

WorkSpaces は PCoIP を使用して、ポート 4172 経由でクライアントにデスクトップセッションをストリーミングします。PCoIP ゲートウェイサーバーの場合、 は小さな範囲の Amazon EC2 パブリック IPv4 アドレス WorkSpaces を使用します。そのため、 WorkSpaces にアクセスするデバイスのファイアウォールポリシーを非常に細かく設定することができます。現時点では、 WorkSpaces クライアントは接続オプションとして IPv6 アドレスをサポートしていないことに注意してください。

リージョン	パブリック IP アドレス範囲
米国東部 (バージニア北部)	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
米国西部 (オレゴン)	35.80.88.0 - 35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255
アジアパシフィック (ムンバイ)	13.126.243.0 - 13.126.243.255
アジアパシフィック (ソウル)	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
アジアパシフィック (シンガポール)	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255

リージョン	パブリック IP アドレス範囲
	52.76.127.0 - 52.76.127.255
アジアパシフィック (シドニー)	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
アジアパシフィック (東京)	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
カナダ (中部)	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
欧州 (フランクフルト)	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
欧州 (アイルランド)	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
欧州 (ロンドン)	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
南米 (サンパウロ)	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255

リージョン	パブリック IP アドレス範囲
アフリカ (ケープタウン)	13.246.120.0 - 13.246.123.255
イスラエル (テルアビブ)	51.17.28.0-51.17.31.255
AWS GovCloud （米国西部）	52.61.193.0 - 52.61.193.255
AWS GovCloud （米国東部）	18.254.140.0 - 18.254.143.255

WSP ゲートウェイサーバー

> **Important**
>
> 2020 年 6 月から、 は WSP WorkSpaces のデスクトップセッションをポート 4172 ではなくポート 4195 経由でクライアントに WorkSpaces ストリーミングします。WSP を使用する場合は WorkSpaces、ポート 4195 がトラフィックに対して開かれていることを確認してください。

WorkSpaces は、WSP ゲートウェイサーバーに小さな範囲の Amazon EC2 パブリック IPv4 アドレスを使用します。そのため、 WorkSpaces にアクセスするデバイスのファイアウォールポリシーを非常に細かく設定することができます。現時点では、 WorkSpaces クライアントは接続オプションとして IPv6 アドレスをサポートしていないことに注意してください。

リージョン	パブリック IP アドレス範囲
米国東部 (バージニア北部)	• 3.227.4.0/22 • 44.209.84.0/22
米国西部 (オレゴン)	34.223.96.0/22
アジアパシフィック (ムンバイ)	65.1.156.0/22
アジアパシフィック (ソウル)	3.35.160.0/22
アジアパシフィック (シンガポール)	13.212.132.0/22

リージョン	パブリック IP アドレス範囲
アジアパシフィック (シドニー)	3.25.248.0/22
アジアパシフィック (東京)	3.114.164.0/22
カナダ (中部)	3.97.20.0/22
欧州 (フランクフルト)	18.192.216.0/22
欧州 (アイルランド)	3.248.176.0/22
欧州 (ロンドン)	18.134.68.0/22
南米 (サンパウロ)	15.228.64.0/22
アフリカ (ケープタウン)	13.246.108.0/22
イスラエル (テルアビブ)	51.17.72.0/22
AWS GovCloud （米国西部）	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud （米国東部）	18.254.148.0/22

WSP ゲートウェイドメイン名

次の表に、WSP WorkSpace ゲートウェイのドメイン名を示します。これらのドメインは、WorkSpaces クライアントアプリケーションが WorkSpace WSP サービスにアクセスできるようにするには、接続可能である必要があります。

リージョン	分野
米国東部 (バージニア北部)	*.prod.us-east-1.highlander.aws.a2z.com
米国西部 (オレゴン)	*.prod.us-west-2.highlander.aws.a2z.com
アジアパシフィック (ムンバイ)	*.prod.ap-south-1.highlander.aws.a2z.com

リージョン	分野
アジアパシフィック (ソウル)	*.prod.ap-northeast-2.highlander.aws.a2z.com
アジアパシフィック (シンガポール)	*.prod.ap-southeast-1.highlander.aws.a2z.com
アジアパシフィック (シドニー)	*.prod.ap-southeast-2.highlander.aws.a2z.com
アジアパシフィック (東京)	*.prod.ap-northeast-1.highlander.aws.a2z.com
カナダ (中部)	*.prod.ca-central-1.highlander.aws.a2z.com
欧州 (フランクフルト)	*.prod.eu-central-1.highlander.aws.a2z.com
欧州 (アイルランド)	*.prod.eu-west-1.highlander.aws.a2z.com
欧州 (ロンドン)	*.prod.eu-west-2.highlander.aws.a2z.com
南米 (サンパウロ)	*.prod.sa-east-1.highlander.aws.a2z.com
アフリカ (ケープタウン)	*.prod.af-south-1.highlander.aws.a2z.com
イスラエル (テルアビブ)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud （米国西部）	*.prod.us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud （米国東部）	*.prod.us-gov-east-1.highlander.aws.a2z.com

ネットワークインターフェイス

各 WorkSpace には、次のネットワークインターフェイスがあります。

- プライマリネットワークインターフェイス (eth1) は、VPC 内およびインターネット上のリソースへの接続を提供し、 WorkSpace を ディレクトリに結合するために使用されます。
- 管理ネットワークインターフェイス (eth0) は、セキュアな WorkSpaces 管理ネットワークに接続します。これは、 WorkSpaces クライアントへのデスクトップの WorkSpaceインタラクティブなストリーミングと、 WorkSpaces による の管理に使用されます WorkSpace。

WorkSpaces WorkSpaces は、 が作成されたリージョンに応じて、さまざまなアドレス範囲から管理ネットワークインターフェイスの IP アドレスを選択します。ディレクトリが登録されると、 は VPC CIDR と VPC 内のルートテーブルを WorkSpaces テストして、これらのアドレス範囲が競合するかどうかを確認します。リージョンで使用可能なすべてのアドレス範囲で競合が見つかった場合、エラーメッセージが表示され、ディレクトリは登録されません。ディレクトリが登録された後で VPC のルートテーブルを変更すると、競合が生じる可能性があります。

Warning

にアタッチされているネットワークインターフェイスを変更または削除しないでください WorkSpace。これを行うと、 WorkSpace にアクセスできなくなったり、インターネットアクセスが失われたりする可能性があります。例えば、ディレクトリレベルで Elastic IP アドレスの自動割り当てを有効にしている場合、起動時に (Amazon が提供するプールからの) Elastic IP アドレスが WorkSpaceに割り当てられます。ただし、所有している Elastic IP アドレスを に関連付けた後 WorkSpace、その Elastic IP アドレスと の関連付けを解除すると WorkSpace、 はパブリック IP アドレスを WorkSpace 失い、Amazon が提供するプールから新しいアドレスを自動的に取得しません。
Amazon が提供するプールからの新しいパブリック IP アドレスを に関連付けるには WorkSpace、 を再構築 WorkSpaceする必要があります。を再構築しない場合は WorkSpace、所有している別の Elastic IP アドレスを に関連付ける必要があります WorkSpace。

管理インターフェイスの IP 範囲

次の表は、管理ネットワークインターフェイスで使用される IP アドレス範囲の一覧です。

Note

- Bring Your Own License (BYOL) Windows を使用している場合 WorkSpaces、以下の表の IP アドレス範囲は適用されません。代わりに、PCoIP BYOL はすべてのAWSリージョンの管理インターフェイストラフィックに 54.239.224.0/20 IP アドレス範囲 WorkSpaces を使用します。WSP BYOL Windows の場合 WorkSpaces、54.239.224.0/20 と 10.0.0.0/8 の両方の IP アドレス範囲がすべての AWSリージョンに適用されます。(これらの IP アドレス範囲は、BYOL の管理トラフィック用に選択した /16 CIDR ブロックに加えて使用されます) WorkSpaces。

- パブリックバンドルから WorkSpaces 作成された WSP を使用している場合、次の表に示す PCoIP /WSP 範囲に加えて、すべてのAWSリージョンの管理インターフェイストラフィックに IP アドレス範囲 10.0.0.0/8 も適用されます。

リージョン	IP アドレス範囲
米国東部 (バージニア北部)	PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 WSP: 10.0.0.0/8
米国西部 (オレゴン)	PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、および 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (ムンバイ)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (ソウル)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (シンガポール)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (シドニー)	PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、および 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (東京)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
カナダ (中部)	PCoIP/WSP: 198.19.0.0/16

リージョン	IP アドレス範囲
	WSP: 10.0.0.0/8
欧州 (フランクフルト)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
欧州 (アイルランド)	PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、および 198.19.0.0/16 WSP: 10.0.0.0/8
欧州 (ロンドン)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
南米 (サンパウロ)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
アフリカ (ケープタウン)	PCoIP/WSP: 172.31.0.0/16 and 198.19.0.0/16 WSP: 10.0.0.0/8
イスラエル (テルアビブ)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
AWS GovCloud （米国西部）	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8 および 192.169.0.0/16
AWS GovCloud （米国東部）	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

管理インターフェイスポート

次のポートは、すべての の管理ネットワークインターフェイスで開いている必要があります WorkSpaces。

- ポート 4172 のインバウンド TCP。これは、PCoIP プロトコルでストリーミング接続を確立するために使用されます。
- ポート 4172 のインバウンド UDP。これは、PCoIP プロトコルでユーザー入力をストリーミングするために使用されます。
- ポート 4489 のインバウンド TCP。これはウェブクライアントを使用したアクセスに使用されます。
- ポート 8200 のインバウンド TCP。これは、 の管理と設定に使用されます WorkSpace。
- ポート 8201-8250 のインバウンド TCP。これらのポートは、ストリーミング接続の確立および WSP プロトコルでのユーザー入力のストリーミングに使用されます。
- ポート 8220 のインバウンド UDP。このポートは、ストリーミング接続の確立および WSP プロトコルでのユーザー入力のストリーミングに使用されます。
- ポート 8443 および 9997 のアウトバウンド TCP。これはウェブクライアントを使用したアクセスに使用されます。
- ポート 3478、4172、および 4195 のアウトバウンド UDP。これはウェブクライアントを使用したアクセスに使用されます。
- ポート 50002 および 55002 のアウトバウンド UDP。これはストリーミングに使用されます。ファイアウォールがステートフルフィルタリングを使用している場合、リターン通信用に一時ポート 50002 が自動的に開放されます。ファイアウォールがステートレスフィルタリングを使用する場合には、リターン通信用に一時ポート 49152 ~ 65535 を開放する必要があります。
- 管理インターフェイスの IP 範囲 で定義されているポート 80 のアウトバウンド TCP から、EC2 メタデータサービスにアクセスするための IP アドレス 169.254.169.254 へのアウトバウンド TCP。に割り当てられた HTTP プロキシでは、169.254.169.254 も除外 WorkSpaces する必要があります。
- パブリックバンドルに基づく WorkSpaces の Windows アクティベーション用の Microsoft KMS へのアクセスを許可する、ポート 1688 での IP アドレス 169.254.169.250 および 169.254.169.251 への送信 TCP。Bring Your Own License (BYOL) Windows を使用している場合は WorkSpaces、Windows アクティベーションのために独自の KMS サーバーへのアクセスを許可する必要があります。
- BYOL の Microsoft KMS for Office アクティベーションへのアクセスを許可する、ポート 1688 の IP アドレス 54.239.236.220 へのアウトバウンド TCP WorkSpaces。

  WorkSpaces いずれかのパブリックバンドルで Office を使用している場合、Microsoft KMS for Office アクティベーションの IP アドレスは異なります。IP アドレスを確認するには、 の管理インターフェイスの IP アドレスを見つけ WorkSpace、最後の 2 つのオクテットを に置き換えま

す64.250。例えば、管理インターフェイスの IP アドレスが 192.168.3.5 の場合、Microsoft KMS Office アクティベーションの IP アドレスは 192.168.64.250 です。

- WorkSpace ホストがプロキシサーバーを使用するように設定されている場合 WorkSpaces の、WSP の IP アドレス 127.0.0.2 へのアウトバウンド TCP。
- ループバックアドレス 127.0.01 から発信される通信。

通常の状況では、 WorkSpaces サービスはこれらのポートを に設定します WorkSpaces。これらのポートのいずれかをブロック WorkSpace するセキュリティまたはファイアウォールソフトウェアがにインストールされている場合、 WorkSpace が正しく機能しないか、到達できない可能性があります。

プライマリインターフェイスポート

ディレクトリのタイプに関係なく、すべての のプライマリネットワークインターフェイスで次のポートが開いている必要があります WorkSpaces。

- インターネット接続の場合、次のポートがすべての宛先へのアウトバウンドで、 WorkSpaces VPC からのインバウンドである必要があります。インターネットにアクセスできるようにする WorkSpaces には、これらのポリシーを のセキュリティグループに追加する必要があります。
  - TCP 80（HTTP）
  - TCP 443（HTTPS）
- ディレクトリコントローラーと通信するには、 WorkSpaces VPC とディレクトリコントローラーの間で次のポートが開いている必要があります。Simple AD ディレクトリの場合、AWS Directory Service によって作成されたセキュリティグループでは、これらのポートが正しく設定されます。AD Connector ディレクトリでは、VPC がそれらのポートを開くために、デフォルトのセキュリティグループの調整が必要になる場合があります。
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 認証
  - UDP 123 – NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 – SMB

- TCP/UDP 636 - LDAPS (TLS/SSL 経由の LDAP)
- TCP 1024-65535 - RPC 用ダイナミックポート

これらのポートのいずれかをブロック WorkSpace するセキュリティまたはファイアウォールソフトウェアが にインストールされている場合、 WorkSpace が正しく機能しないか、到達できない可能性があります。

リージョンごとの IP アドレスとポートの要件

米国東部 (バージニア北部)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.us-east-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-east-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 米国東部 (バージニア北部) — https://d32i4gd7pg4909.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.us-east-1.signin.aws
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)

カテゴリ	詳細
WS ブローカー	ドメイン: • https://ws-broker-service.us-east-1.amazonaws.com • https://ws-broker-service-fips.us-east-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: https://workspaces.us-east-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.us-east-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-iad.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255

カテゴリ	詳細
WSP ゲートウェイサーバーの IP アドレス範囲	• 3.227.4.0/22 • 44.209.84.0/22
WSP ゲートウェイドメイン名	*.prod.us-east-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP: 10.0.0.0/8

米国西部 (オレゴン)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.us-west-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-west-2.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID>

カテゴリ	詳細
	MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 米国西部 (オレゴン) — https://d18af777lco7lp.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.us-west-2.signin.aws
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com

カテゴリ	詳細
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.us-west-2.amazonaws.com • https://ws-broker-service-fips.us-west-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.us-west-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-pdx.amazonworkspaces.com
ヘルスチェック IP アドレス	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140

カテゴリ	詳細
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
WSP ゲートウェイサーバーの IP アドレス範囲	34.223.96.0/22
WSP ゲートウェイドメイン名	*.prod.us-west-2.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック (ムンバイ)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-south-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-south-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace :

カテゴリ	詳細
	• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • アジアパシフィック (ムンバイ) — https://d78hovzzqqtsb.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com

カテゴリ	詳細
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-south-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-south-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-south-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	Web Access は現在、アジアパシフィック (ムンバイ) リージョンではご利用いただけません。
ヘルスチェックホスト名	drp-bom.amazonworkspaces.com
ヘルスチェック IP アドレス	• 13.127.57.82 • 13.234.250.73
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	13.126.243.0 - 13.126.243.255
WSP ゲートウェイサーバーの IP アドレス範囲	65.1.156.0/22
WSP ゲートウェイドメイン名	*.prod.ap-south-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 192.168.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック (ソウル)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
デバイスメトリクス (1.0 以降および 2.0 以降の WorkSpaces クライアントアプリケーション用)	https://device-metrics-us-2.amazon.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-northeast-2.amazonaws.com
ディレクトリ設定	に ログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

カテゴリ	詳細
	お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • アジアパシフィック (ソウル) — https://dtyv4uwoh7ynt.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-northeast-2.amazonaws.com

カテゴリ	詳細
セッションブローカー（PCM）	ドメイン: • https://skylight-cm.ap-northeast-2.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.ap-northeast-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-icn.amazonworkspaces.com
ヘルスチェック IP アドレス	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
WSP ゲートウェイサーバーの IP アドレス範囲	3.35.160.0/22
WSP ゲートウェイドメイン名	*.prod.ap-northeast-2.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック（シンガポール）

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/

カテゴリ	詳細
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-southeast-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-southeast-1.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (シンガポール) — https://d3qzmd7y07pz0i.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-southeast-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-southeast-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-southeast-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.ap-southeast-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-sin.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
WSP ゲートウェイサーバーの IP アドレス範囲	13.212.132.0/22

カテゴリ	詳細
WSP ゲートウェイドメイン名	*.prod.ap-southeast-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック (シドニー)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-southeast-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-southeast-2.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • アジアパシフィック (シドニー) — https://dwcpoxuuza83q.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.ap-southeast-2.signin.aws
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)

カテゴリ	詳細
WS ブローカー	ドメイン: • https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-southeast-2.amazonaws.com
セッションブローカー（PCM）	ドメイン: • https://skylight-cm.ap-southeast-2.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.ap-southeast-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-syd.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.24.11.127 • 13.237.232.125
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
WSP ゲートウェイサーバーの IP アドレス範囲	3.25.248.0/22
WSP ゲートウェイドメイン名	*.prod.ap-southeast-2.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、および 198.19.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック（東京）

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-northeast-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-northeast-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック:

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • アジアパシフィック (東京) — https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.ap-northeast-1.signin.aws
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-northeast-1.amazonaws.com

カテゴリ	詳細
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-northeast-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.ap-northeast-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-nrt.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.178.102.247 • 54.64.174.128
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
WSP ゲートウェイサーバーの IP アドレス範囲	3.114.164.0/22
WSP ゲートウェイドメイン名	*.prod.ap-northeast-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

カナダ (中部)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/

カテゴリ	詳細
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ca-central-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ca-central-1.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • カナダ (中部) — https://d2wfbsypmqjmog.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ca-central-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ca-central-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ca-central-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.ca-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-yul.amazonworkspaces.com
ヘルスチェック IP アドレス	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
WSP ゲートウェイサーバーの IP アドレス範囲	3.97.20.0/22

カテゴリ	詳細
WSP ゲートウェイドメイン名	*.prod.ca-central-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

欧州 (フランクフルト)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.eu-central-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.eu-central-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 欧州 (フランクフルト) — https://d1whcm49570jjw.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-central-1.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.eu-central-1.amazonaws.com
セッションブローカー（PCM）	ドメイン: • https://skylight-cm.eu-central-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.eu-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-fra.amazonworkspaces.com
ヘルスチェック IP アドレス	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
WSP ゲートウェイサーバーの IP アドレス範囲	18.192.216.0/22
WSP ゲートウェイドメイン名	*.prod.eu-central-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 198.19.0.0/16 • WSP: 10.0.0.0/8

欧州 (アイルランド)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.eu-west-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.eu-west-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック:

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 欧州 (アイルランド) — https://d3pgffbf39h4k4.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.eu-west-1.signin.aws
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.eu-west-1.amazonaws.com

カテゴリ	詳細
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.eu-west-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.eu-west-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-dub.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
WSP ゲートウェイサーバーの IP アドレス範囲	3.248.176.0/22
WSP ゲートウェイドメイン名	*.prod.eu-west-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、および 198.19.0.0/16 • WSP: 10.0.0.0/8

欧州 (ロンドン)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/

カテゴリ	詳細
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.eu-west-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.eu-west-2.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 欧州 (ロンドン) — https://d16q6638mh01s7.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-west-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.eu-west-2.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.eu-west-2.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.eu-west-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-lhr.amazonworkspaces.com
ヘルスチェック IP アドレス	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
WSP ゲートウェイサーバーの IP アドレス範囲	18.134.68.0/22

カテゴリ	詳細
WSP ゲートウェイドメイン名	*.prod.eu-west-2.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8

南米 (サンパウロ)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.sa-east-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.sa-east-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 南米 (サンパウロ) — https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.sa-east-1.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.sa-east-1.amazonaws.com
セッションブローカー（PCM）	ドメイン: • https://skylight-cm.sa-east-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.sa-east-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-gru.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
WSP ゲートウェイサーバーの IP アドレス範囲	15.228.64.0/22
WSP ゲートウェイドメイン名	*.prod.sa-east-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8

アフリカ (ケープタウン)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.af-south-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.af-south-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック:

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • アフリカ (ケープタウン); — https://di5ygl2cs0mrh.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.af-south-1.amazonaws.com

カテゴリ	詳細
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.af-south-1.amazonaws.com
ヘルスチェックホスト名	drp-cpt.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 13.246.120.0 - 13.246.123.255
WSP ゲートウェイサーバーの IP アドレス範囲	15.228.64.0/22
WSP ゲートウェイドメイン名	*.prod.af-south-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• 172.31.0.0/16 and 198.19.0.0/16 • WSP: 10.0.0.0/8

イスラエル (テルアビブ)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン:

カテゴリ	詳細
	https://skylight-client-ds.il-central-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.il-central-1.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • ログインページのスタイル設定に使用される CSS ファイル: • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • イスラエル (テルアビブ) —
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.il-central-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.il-central-1.amazonaws.com
PCoIP のウェブアクセス TURN サーバー	サーバー: • turn:*.il-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-tlv.amazonworkspaces.com
ヘルスチェック IP アドレス	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 51.17.28.0-51.17.31.255
WSP ゲートウェイサーバーの IP アドレス範囲	51.17.72.0/22
WSP ゲートウェイドメイン名	*.prod.il-central-1.highlander.aws.a2z.com

カテゴリ	詳細
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud（米国西部) リージョン

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: hhttps://skylight-client-ds.us-gov-west-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-gov-west-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<directory ID> ログインページのスタイル設定に使用されるCSS ファイル: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript ログインページの ファイル : • 該当しない
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.signin.amazonaws-us-gov.com
登録の依存関係 (ウェブアクセスおよびTeradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (<directory id> はお客様のドメインです)

カテゴリ	詳細
WS ブローカー	ドメイン: • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com
セッションブローカー（PCM）	ドメイン: • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com
ヘルスチェックホスト名	drp-pdt.amazonworkspaces.com
ヘルスチェック IP アドレス	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 52.61.193.0 - 52.61.193.255

カテゴリ	詳細
WSP ゲートウェイサーバーの IP アドレス範囲	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
WSP ゲートウェイドメイン名	*.prod.us-gov-west-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8 および 192.169.0.0/16

AWS GovCloud（ 米国東部) リージョン

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://s3.amazonaws.com/workspaces-client-updates/prod/osu/windows/WorkSpacesAppCast.xml
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: hhttps://skylight-client-ds.us-gov-east-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-gov-east-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントから顧客ディレクトリへの認証 WorkSpace：

カテゴリ	詳細
	• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<directory ID> ログインページのスタイル設定に使用される CSS ファイル: • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript ログインページの ファイル : • 該当しない
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.signin.amazonaws-us-gov.com

カテゴリ	詳細
登録の依存関係 (ウェブアクセスおよび Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (<directory id> はお客様のドメインです)
WS ブローカー	ドメイン: • https://ws-broker-service.us-gov-east-1.amazonaws.com • https://ws-broker-service-fips.us-gov-east-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.us-gov-east-1.amazonaws.com • https://workspaces-fips.us-gov-east-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-gov-east-1.amazonaws.com • https://skylight-cm-fips.us-gov-east-1.amazonaws.com
ヘルスチェックホスト名	drp-osu.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.253.251.70 • 18.254.0.118
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.254.140.0 - 18.254.143.255
WSP ゲートウェイサーバーの IP アドレス範囲	18.254.148.0/22

カテゴリ	詳細
WSP ゲートウェイドメイン名	*.prod.us-gov-east-1.highlander.aws.a2z.com
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8

Amazon WorkSpaces クライアントネットワークの要件

WorkSpaces ユーザーは、サポートされているデバイスのクライアントアプリケーションを使用して WorkSpaces に接続することができます。また、ウェブブラウザを使用して、このアクセス形式をサポートする WorkSpaces に接続することができます。ウェブブラウザのアクセスをサポートする WorkSpaces のリストについては、「ウェブアクセスはどの Amazon WorkSpaces バンドルでサポートされていますか?」を参照してください。クライアントアクセス、Web アクセス、およびユーザーエクスペリエンスで。

> **Note**
>
> ウェブブラウザを使用して Amazon Linux WorkSpaces に接続することはできません。

> **Important**
>
> 2020 年 10 月 1 日以降、お客様は Amazon WorkSpaces Web Access クライアントを使用して Windows 7 カスタム WorkSpaces または Windows 7 自分のライセンス使用 (BYOL) WorkSpaces に接続できなくなります。

ユーザーに WorkSpaces の優れた体験を提供するために、クライアントデバイスが以下のネットワーク要件を満たしていることを確認します。

- クライアントデバイスには、ブロードバンドインターネット接続が必要です。480p ビデオウィンドウを視聴する同時ユーザーあたり 1 Mbps 以上を計画することをお勧めします。ビデオ解像度に対するユーザー品質の要件によっては、より多くの帯域幅が必要になる場合があります。
- クライアントデバイスが接続されているネットワーク、およびクライアントデバイスのファイアウォールに、さまざまな AWS サービスの IP アドレス範囲に対して開かれている特定のポートが

存在している必要があります。詳細については、「の IP アドレスとポートの要件 WorkSpaces」を参照してください。

- PCoIP のパフォーマンスを最大限に高めるには、クライアントネットワークから WorkSpaces があるリージョンまでのラウンドトリップ時間 (RTT) が 100ms 未満でなければなりません。RTT が 100 ミリ秒から 200 ミリ秒の間にある場合、ユーザーは WorkSpace にアクセスできますが、パフォーマンスに影響します。RTT が 200 ミリ秒 ~ 375 ミリ秒の間にある場合、パフォーマンスは低下します。RTT が 375 ミリ秒を超えると、WorkSpaces クライアント接続は終了します。

  WorkSpaces Streaming Protocol (WSP) の最高のパフォーマンスのためには、クライアントのネットワークから WorkSpaces があるリージョンまでの RTT が 250 ミリ秒未満でなければなりません。RTT が 250 ミリ秒から 400 ミリ秒の間にある場合、ユーザーは WorkSpace にアクセスできますが、パフォーマンスは低下します。

  自分の場所からさまざまな AWS リージョンへの RTT を確認するには、Amazon WorkSpaces 接続ヘルスチェックを使用します。
- WSP でウェブカメラを使用する場合、アップロードの帯域幅には最低 1 秒あたり 1.7 メガビットの確保が推奨されます。
- ユーザーが仮想プライベートネットワーク (VPN) 経由で WorkSpace にアクセスする場合は、少なくとも 1200 バイトの最大送信単位 (MTU) をサポートする接続が必用です。

  > **Note**
  >
  > Virtual Private Cloud (VPC) に接続された VPN を介して WorkSpaces にアクセスすることはできません。VPN を使用して WorkSpaces にアクセスするには、の IP アドレスとポートの要件 WorkSpaces で説明されているように、(VPN のパブリック IP アドレス経由の) インターネット接続が必要です。

- クライアントには、サービスと Amazon Simple Storage Service (Amazon S3) がホストする WorkSpaces リソースへの HTTPS アクセスが必要です。クライアントは、アプリケーションレベルのプロキシリダイレクトをサポートしていません。ユーザーが登録を完了して Workspace にアクセスできるようにするには、HTTPS アクセスが必要です。
- PCoIP ゼロクライアントデバイスからのアクセスを許可するには、WorkSpaces の PCoIP プロトコルバンドルを使用する必要があります。また、Teradici でネットワークタイムプロトコル (NTP) を有効にする必要があります。詳細については、「WorkSpaces の PCoIP ゼロクライアントをセットアップする」を参照してください。
- 3.0 以降のクライアントの場合、Amazon WorkDocs で Single Sign-On (SSO) を使用している場合は、AWS Directory Service 管理ガイドの Single Sign-On の手順に従う必要があります。

次の方法で、クライアントデバイスがネットワーキング要件を満たしていることを確認できます。

3.0 以上のクライアントのネットワーク要件を確認するには

1. WorkSpaces クライアントを開きます。クライアントを初めて開いた場合は、招待メールで受け取った登録コードを入力するよう求められます。
2. 使用しているクライアントに応じて、以下のいずれかを実行します。

使用しているクライアント	操作
Windows または Linux クライアント	クライアントアプリケーションの右上にある [Network (ネットワーク)] アイコン を選択します。
macOS クライアント	[Connections (接続)]、[Network (ネットワーク)] の順に選択します。

   クライアントアプリケーションによって、ネットワーク接続、ポート、ラウンドトリップ時間がテストされ、これらのテストの結果がレポートされます。
3. [Network (ネットワーク)] ダイアログボックスを閉じて、サインインページに戻ります。

1.0 以上および 2.0 以上のクライアントのネットワーク要件を確認するには

1. WorkSpaces クライアントを開きます。クライアントを初めて開いた場合は、招待メールで受け取った登録コードを入力するよう求められます。
2. クライアントアプリケーションの右下隅にある [Network (ネットワーク)] を選択します。クライアントアプリケーションによって、ネットワーク接続、ポート、ラウンドトリップ時間がテストされ、これらのテストの結果がレポートされます。
3. [Dismiss] を選択してサインインページに戻ります。

信頼できるデバイス WorkSpaces へのアクセスを制限する

デフォルトでは、ユーザーはインターネットに接続されているサポートされている WorkSpaces 任意のデバイスから にアクセスできます。会社が企業データへのアクセスを信頼できるデバイス (マ

ネージドデバイスとも呼ばれます) に制限している場合、有効な証明書を持つ信頼できるデバイス WorkSpaces へのアクセスを制限できます。

この機能を有効にすると、 は証明書ベースの認証 WorkSpaces を使用して、デバイスが信頼されているかどうかを判断します。 WorkSpaces クライアントアプリケーションは、デバイスが信頼されていることを検証できない場合、ログインまたはデバイスからの再接続をブロックします。

各ディレクトリにで、最大 2 つのルート証明書をインポートできます。2 つのルート証明書をインポートすると、 は両方をクライアントに WorkSpaces 提示し、クライアントはいずれかのルート証明書に連鎖する最初の有効な一致証明書を見つけます。

Supported Clients (サポートされるクライアント)

- Android、Android または Android 対応の Chrome OS システム
- macOS
- Windows

Important

この機能は次のクライアントではサポートされていません。

- WorkSpaces Linux または iPad 用の クライアントアプリケーション
- サードパーティークライアント (Teradici PCoIP、RDP クライアント、リモートデスクトップアプリケーションを含みますが、これらに限定されません)。

Note

特定のクライアントに対してアクセスを有効にする場合は、不要な他のデバイスタイプのアクセスをブロックしてください。これを行う方法の詳細については、以下のステップ 3.7 を参照してください。

ステップ 1: 証明書を作成する

この機能には、内部認証局 (CA) によって生成されるルート証明書と、ルート証明書に連鎖するクライアント証明書の 2 種類の証明書が必要です。

要件

- ルート証明書は、Base64 でエンコードされた CRT、CERT、または PEM 形式の証明書ファイルである必要があります。
- ルート証明書は、次の正規表現パターンを満たす必要があります。つまり、最後の行の横にあるすべてのエンコードされた行は、正確に 64 文字でなければなりません: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`。
- デバイス証明書には共通名が含まれている必要があります。
- デバイス証明書には、`Key Usage: Digital Signature` および`Enhanced Key Usage: Client Authentication` の拡張機能が含まれている必要があります。
- デバイス証明書から信頼されたルート認証局へのチェーン内の、すべての証明書をクライアントデバイスにインストールする必要があります。
- 証明書チェーンでサポートされている最大長は 4 です。
- WorkSpaces は現在、クライアント証明書の証明書失効リスト (CRL) やオンライン証明書ステータスプロトコル (OCSP) などのデバイス失効メカニズムをサポートしていません。
- 強力な暗号化アルゴリズムを使用します。SHA256 (RSA)、SHA256 (ECDSA)、SHA384 (ECDSA)、SHA512 (ECDSA) をお勧めします。
- macOS の場合、デバイス証明書がシステムキーチェーンにある場合は、 WorkSpaces クライアントアプリケーションがそれらの証明書にアクセスすることを許可することをお勧めします。それ以外の場合は、ユーザーがログインまたは再接続するときに、キーチェーンの資格情報を入力する必要があります。

ステップ 2: クライアント証明書を信頼されたデバイスにデプロイする

ユーザーの信頼されたデバイスで、デバイス証明書から信頼されたルート証明書認証へのチェーン内の、すべての証明書を含む証明書バンドルをインストールする必要があります。任意のソリューションを使用して、一連のクライアントデバイスに証明書をインストールすることができます。たとえば、SCCM（System Center Configuration Manager）や MDM（Mobile Device Management）などです。SCCM と MDM は、オプションでセキュリティ体制評価を実行して、デバイスが にアクセスするための企業ポリシーを満たしているかどうかを判断できることに注意してください WorkSpaces。

WorkSpaces クライアントアプリケーションは、次のように証明書を検索します。

- Android - [設定] に移動し、[セキュリティと位置情報]、[認証情報]、[SD カードからインストール] の順に選択します。
- Android 対応 Chrome OS システム - Android の [設定] を開き、[セキュリティと位置情報]、[認証情報]、[SD カードからインストール] の順に選択します。
- macOS - キーチェーンでクライアント証明書を検索します。
- Windows - ユーザーストアとルート証明書ストアでクライアント証明書を探します。

ステップ 3: 制限を設定する

信頼されたデバイスにクライアント証明書をデプロイした後で、ディレクトリレベルでの制限付きアクセスを有効にすることができます。これには、ユーザーが にログインできるようにする前に、 WorkSpaces クライアントアプリケーションがデバイスで証明書を検証する必要があります WorkSpace。

制限を設定するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Access Control Options] を展開します。
5. 「各デバイスタイプ」で、 にアクセスできるデバイスを指定し WorkSpaces、「信頼できるデバイス」を選択します。
6. 最大 2 つのルート証明書をインポートします。各ルート証明書について、次の操作を行います。

   a. [Import] (インポート) を選択します。

   b. 証明書の本文をフォームにコピーします。

   c. [Import] (インポート) を選択します。
7. 他のタイプのデバイスが にアクセスできるかどうかを指定します WorkSpaces。

   a. [Other Platforms] セクションまで下にスクロールします。デフォルトでは、 WorkSpaces Linux クライアントは無効になっており、ユーザーは WorkSpaces iOS デバイス、Android デバイス、ウェブアクセス、Chromebook、PCoIP ゼロクライアントデバイスから にアクセスできます。

   b. 有効にするデバイスタイプを選択し、無効にするデバイスタイプをクリアします。

c. 選択したすべてのデバイスタイプからのアクセスをブロックするには、[Block] を選択します。

8. [Update and Exit] を選択します。

WorkSpaces と SAML 2.0 の統合

SAML 2.0 をデスクトップセッションの認証のために WorkSpaces と統合すると、ユーザーはデフォルトのウェブブラウザから既存の SAML 2.0 ID プロバイダー (IdP) 認証情報と認証方法を使用できるようになります。IdP を使用して WorkSpaces へのユーザーの認証を行うと、多要素認証やコンテキストに応じたアクセスポリシーなどの IdP 機能を採用することで、WorkSpaces を保護することができます。

認証ワークフロー

以下のセクションでは、WorkSpaces クライアントアプリケーション、WorkSpaces Web Access、および SAML 2.0 ID プロバイダー (IdP) によって開始される認証ワークフローについて説明します。

- フローが IdP によって開始されるとき。たとえば、ユーザーが IdP ユーザーポータルのアプリケーションをウェブブラウザで選択したときです。
- フローが WorkSpaces クライアントによって開始されるとき。たとえば、ユーザーがクライアントを開いてサインインしたときです。
- フローが WorkSpaces Web Access によって開始されるとき。たとえば、ユーザーがブラウザで Web Access を開いてサインインしたときです。

これらの例では、ユーザーは「`user@example.com`」と入力して IdP にサインインします。IdP には、WorkSpaces ディレクトリ用に設定された SAML 2.0 サービスプロバイダーアプリケーションがあり、ユーザーは WorkSpaces SAML 2.0 アプリケーションに対して承認されています。ユーザーは、SAML 2.0 認証が有効になっているディレクトリにユーザー名 `user` の WorkSpace を作成します。さらに、ユーザーはデバイスに WorkSpaces クライアントアプリケーションをインストールするか、ウェブブラウザで Web Access を使用します。

クライアントアプリケーションを使用したID プロバイダー (IdP) 主導フロー

IdP 主導のフローでは、ユーザーは WorkSpaces 登録コードを入力せずに、デバイスに WorkSpaces クライアントアプリケーションを自動的に登録できます。ユーザーは、IdP 主導のフローを使用して

自身の WorkSpaces に対してサインインしません。WorkSpaces 認証は、クライアントアプリケーションから開始する必要があります。

1. ユーザーはウェブブラウザを使用して、IdP にサインインします。
2. IdP にサインインした後、ユーザーは IdP ユーザーポータルから WorkSpaces アプリケーションを選択します。
3. ユーザーはブラウザでこのページにリダイレクトされ、WorkSpaces クライアントアプリケーションが自動的に開きます。

4. WorkSpaces クライアントアプリケーションが登録されました。ユーザーは、[Continue to sign in to WorkSpaces] (WorkSpaces へのサインインを続ける) をクリックして続行できます。

ウェブアクセスを使用した ID プロバイダー (IdP) 主導フロー

IdP 主導のウェブアクセスフローでは、ユーザーは WorkSpaces 登録コードを入力せずに、ウェブブラウザに WorkSpaces を自動的に登録できます。ユーザーは、IdP 主導のフローを使用して自身の WorkSpaces に対してサインインしません。WorkSpaces 認証は、ウェブアクセスから開始する必要があります。

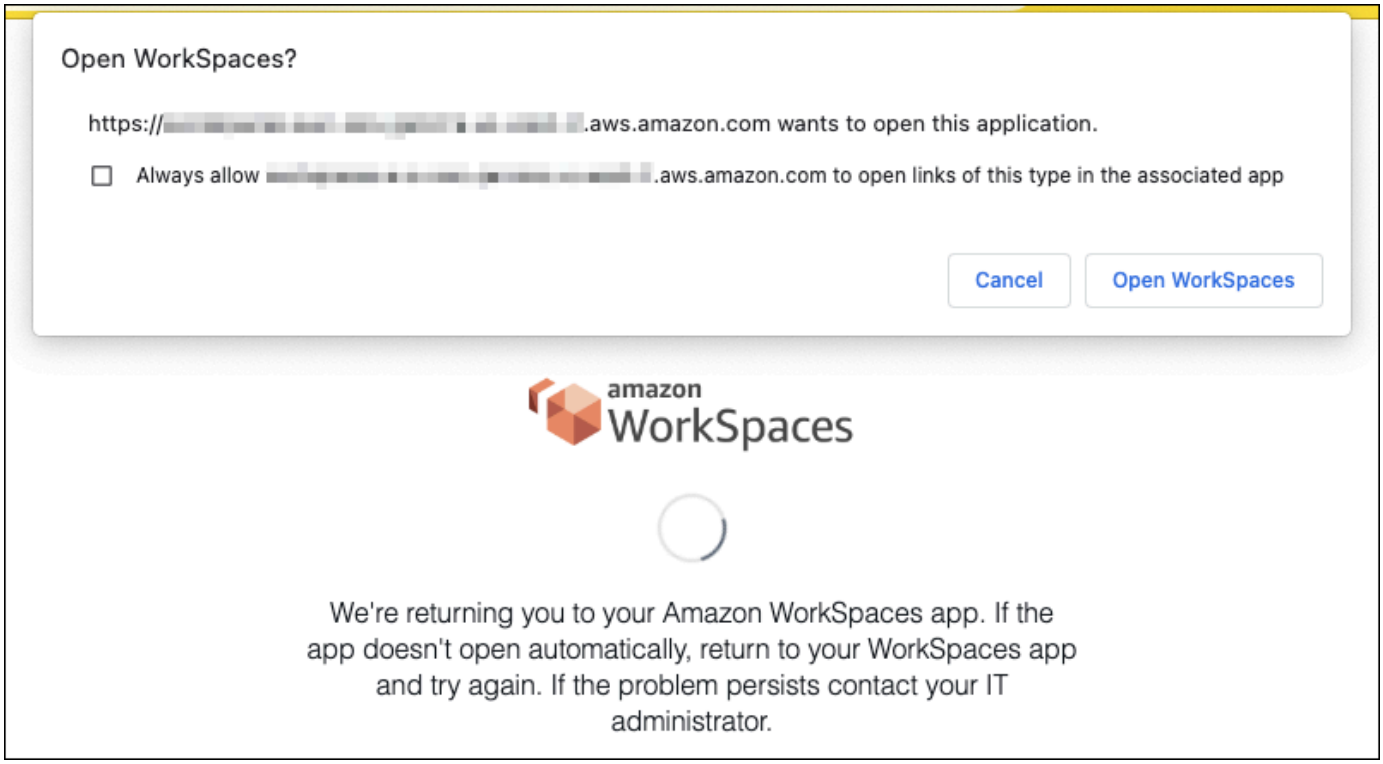
1. ユーザーはウェブブラウザを使用して、IdP にサインインします。
2. IdP にサインインした後、ユーザーは IdP ユーザーポータルから WorkSpaces アプリケーションを選択します。
3. ユーザーはブラウザでこのページにリダイレクトされます。WorkSpaces を開くには、[Amazon WorkSpaces in the browser] (ブラウザでの Amazon WorkSpaces) を選択します。

4. WorkSpaces クライアントアプリケーションが登録されました。ユーザーは、WorkSpaces Web Access からサインインを続行できます。

WorkSpaces クライアント主導フロー

クライアント主導のフローでは、ユーザーは IdP にサインインした後に WorkSpaces にサインインできます。

1. ユーザーが WorkSpaces クライアントアプリケーションを起動し (まだ実行されていない場合)、[WorkSpaces へのサインインを続行] をクリックします。
2. ユーザーはデフォルトのウェブブラウザにリダイレクトされ、IdP にサインインします。ユーザーがブラウザで既に IdP にサインインしている場合、再度サインインする必要はなく、このステップをスキップします。
3. IdP にサインインすると、ユーザーはポップアップにリダイレクトされます。プロンプトに従うと、ウェブブラウザーがクライアントアプリケーションを開くことができます。



4. ユーザーは WorkSpaces クライアントアプリケーションにリダイレクトされ、WorkSpace へのサインインが完了します。WorkSpaces のユーザー名は、IdP SAML 2.0 アサーションから自動的に入力されます。証明書ベースの認証 (CBA) を使用すると、ユーザーは自動的にサインインされます。
5. ユーザーは自分の WorkSpace にサインインしています。

WorkSpaces Web Access 主導のフロー

WorkSpaces Web Access 主導のフローでは、ユーザーは IdP にサインインした後に WorkSpaces にサインインできます。

1. ユーザーは WorkSpaces Web アクセスを起動して、[サインイン] を選択します。
2. 同じブラウザータブで、ユーザーは IdP ポータルにリダイレクトされます。ユーザーがブラウザで既に IdP にサインインしている場合、再度サインインする必要はなく、このステップをスキップできます。
3. IdP にサインインすると、ユーザーはブラウザでこのページにリダイレクトされ、[Log in to WorkSpaces] (WorkSpaces にログインする) をクリックします。
4. ユーザーは WorkSpaces クライアントアプリケーションにリダイレクトされ、WorkSpace へのサインインが完了します。WorkSpaces のユーザー名は、IdP SAML 2.0 アサーションから自動

的に入力されます。証明書ベースの認証 (CBA) を使用すると、ユーザーは自動的にサインインされます。

5. ユーザーは自分の WorkSpace にサインインしています。

SAML 2.0 の設定

SAML 2.0 を使用して ID フェデレーションを設定することで、SAML 2.0 ID プロバイダー (IdP) の認証情報と認証方法を使用して、ユーザーのクライアント WorkSpaces アプリケーション登録と WorkSpaces へのサインインを有効にします。SAML 2.0 を使用した ID フェデレーションを設定するには、IAM ロールとリレーステート URL を使用して、IdP を設定し、 AWSを有効にします。これにより、フェデレーティッドユーザーに WorkSpaces ディレクトリへのアクセス許可が付与されます。リレーステートは、 WorkSpaces に正常にサインインした後にユーザーが転送されるディレクトリエンドポイントです AWS。

内容

要件

- SAML 2.0 認証は、以下のリージョンで使用できます。
  - 米国東部 (バージニア北部) リージョン
  - 米国西部 (オレゴン) リージョン
  - アフリカ (ケープタウン) リージョン
  - アジアパシフィック (ムンバイ) リージョン
  - Asia Pacific (Seoul) Region

  - アジアパシフィック (シンガポール) リージョン
  - アジアパシフィック (シドニー) リージョン
  - アジアパシフィック (東京) リージョン
  - カナダ (中部) リージョン
  - Europe (Frankfurt) Region
  - 欧州 (アイルランド) リージョン
  - 欧州 (ロンドン) リージョン
  - 南米 (サンパウロ) リージョン
  - イスラエル (テルアビブ) リージョン
  - AWS GovCloud （ 米国西部 ）
  - AWS GovCloud （ 米国東部 ）
- で SAML 2.0 認証を使用するには WorkSpaces、IdP はディープリンクターゲットリソースまたはリレーステートエンドポイント URL を持つ未承諾の IdP 開始 SSO をサポートする必要があります。の例 IdPs には、ADFS、Azure AD、 Single Sign-On、Okta PingFederate、 などがありますPingOne。詳細については、IdP のユーザードキュメントを参照してください。
- SAML 2.0 認証は Simple AD を使用して WorkSpaces 起動された で機能しますが、Simple AD は SAML 2.0 と統合されないため、これは推奨されません IdPs。
- SAML 2.0 認証は、次の WorkSpaces クライアントでサポートされています。SAML 2.0 認証は、他のクライアントバージョンではサポートされていません。Amazon WorkSpaces Client Downloads を開いて最新バージョンを確認します。
  - WorkSpaces Windows クライアントアプリケーションのバージョン 5.1.0.3029 以降
  - macOS クライアントバージョン 5.x 以降
  - Ubuntu 22.04 バージョン 2024.1 以降、Ubuntu 20.04 バージョン 24.1 以降の Linux クライアント
  - Web Access

  フォールバック WorkSpaces が有効になっていない限り、他のクライアントバージョンは SAML 2.0 認証が有効になっている に接続できません。詳細については、WorkSpaces 「 ディレクトリで SAML 2.0 認証を有効にする」を参照してください。

ADFS、Azure AD、 Single Sign-On、Okta、 OneLogin PingFederate for Enterprise WorkSpaces を使用して SAML 2.0 を と統合する step-by-step 手順については、「Amazon WorkSpaces SAML 認証実装ガイド PingOne 」を参照してください。

前提条件

WorkSpaces ディレクトリへの SAML 2.0 ID プロバイダー (IdP) 接続を設定する前に、次の前提条件を満たしてください。

1. WorkSpaces ディレクトリで使用される Microsoft Active Directory のユーザー ID を統合するように IdP を設定します。を持つユーザーの場合 WorkSpace、ユーザーが IdP WorkSpaces を使用して にサインインするには、Active Directory ユーザーの sAMAccountName 属性と E メール属性、および SAML クレーム値が一致する必要があります。Active Directory を IdP と統合する方法の詳細については、IdP のドキュメントを参照してください。
2. AWSとの信頼関係を確立するために IdP を設定します。
   - AWS フェデレーションの設定の詳細については、「サードパーティーの SAML ソリューションプロバイダーと の統合 AWS」を参照してください。関連する例には、 AWS マネジメントコンソールにアクセスするための IdP と AWS IAM の統合が含まれます。
   - IdP を使用して、組織を IdP として定義するフェデレーションメタデータドキュメントを生成し、ダウンロードします。署名されたこの XML ドキュメントは、証明書利用者の信頼を確立するために使用されます。後で IAM コンソールからアクセスできる場所にこのファイルを保存します。
3. WorkSpaces マネジメントコンソール WorkSpaces を使用して、 のディレクトリを作成または登録します。詳細については、「 のディレクトリを管理する WorkSpaces」を参照してください。の SAML 2.0 認証 WorkSpaces は、次のディレクトリタイプでサポートされています。
   - AD Connector
   - AWS Managed Microsoft AD
4. サポートされているディレクトリタイプを使用して IdP にサインインできる WorkSpace ユーザーの を作成します。は、 WorkSpaces マネジメントコンソール、、 AWS CLIまたは WorkSpaces API WorkSpace を使用して作成できます。詳細については、「 を使用して仮想デスクトップを起動する WorkSpaces」を参照してください。

ステップ 1: AWS IAM で SAML ID プロバイダーを作成する

まず、 AWS IAM で SAML IdP を作成します。この IdP は、組織内の IdP ソフトウェアによって生成されたメタデータドキュメントを使用して、組織の IdP とAWS 信頼の関係を定義します。詳細については、「SAML ID プロバイダーの作成と管理 (アマゾン ウェブ サービス管理コンソール)」を参照してください。 (米国西部) および AWS GovCloud （ AWS GovCloud 米国東部) IdPs での SAML の使用については、AWS 「 Identity and Access Management」を参照してください。

ステップ 2: SAML 2.0 フェデレーション IAM ロールを作成する

次に、SAML 2.0 フェデレーション IAM ロールを作成します。この手順では、IAM と組織の IdP 間に、IdP をフェデレーションの信頼されるエンティティと識別する信頼関係を確立します。

SAML IdP への IAM ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles] (ロール) を選択してから、[Create role] (ロールを作成する) を選択します。
3. [ロールタイプ] で [SAML 2.0 フェデレーション] を選択します。
4. [SAML Provider] (SAML プロバイダー) で、作成した SAML IdP を選択します。

   > **Important**
   >
   > 2 つの SAML 2.0 アクセスメソッド ([プログラムによるアクセスのみを許可する] または [プログラムによるアクセスと Amazon Web Services マネジメントコンソールによるアクセスを許可する]) のいずれも選択しないでください。

5. [属性] で 、[SAML:sub_type] を選択します。
6. [Value] (値) に「`persistent`」と入力します。この値は、persistent の値の SAML サブジェクトタイプアサーションを含む SAML ユーザーストリーミングリクエストへのロールアクセスを制限します。SAML:sub_type が persistent の場合、IdP は特定のユーザーからのすべての SAML リクエストで同じ一意の値を NameID 要素に送信します。SAML:sub_type アサーションの詳細については、「 への API アクセスに AWSSAML ベースのフェデレーションを使用する」の「SAML ベースのフェデレーションでユーザーを一意に識別する」セクションを参照してください。
7. 正しい信頼されたエンティティおよび条件を確認して SAML 2.0 の信頼情報を確かめたら、[Next: Permissions] (次: アクセス許可) を選択します。
8. [アクセス権限ポリシーをアタッチする] ページで、[Next: Tags] を選択します。
9. (オプション) 追加する各タグのキーと値を入力します。詳細については、「IAM ユーザーとロールのタグ付け」を参照してください。
10. 終了したら、[Next: Review] を選択します。後でこのロールにインラインポリシーを作成して埋め込みます。

11. [Role name] (ロール名) に、このロールの目的を識別できる名前を入力します。なぜなら複数エンティティがロールを参照している可能性があります。ロールが作成された後のロールの名前の編集はできません。
12. (オプション) [Role description] (ロールの説明) に、新しいロールの説明を入力します。
13. ロールの詳細を確認し、[ロールの作成] を選択します。
14. sts:TagSession permission を新しい IAM ロールの信頼ポリシーに追加します。詳細については、「AWS STSでのセッションタグの受け渡し」を参照してください。新しい IAM ロールの詳細ページで、[Trust relationships] (信頼関係) タブを選択してから、[Edit trust relationship] (信頼関係の編集) を選択します。信頼関係ポリシーの編集エディタが開いたら、次のように sts:TagSession* アクセス許可を追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

IDENTITY-PROVIDER をステップ 1 で作成した SAML IdP の名前で置き換えます。次に、[Update Trust Policy] (信頼ポリシーの更新) を選択します。

ステップ 3: IAM ロールにインラインポリシーを埋め込む

次に、作成したロールにインライン IAM ポリシーを埋め込みます。インラインポリシーを埋め込むと、ポリシーのアクセス許可が、間違ったプリンシパルエンティティにアタッチされることを回避できます。インラインポリシーは、フェデレーティッドユーザーに WorkSpaces ディレクトリへのアクセスを提供します。

> **Important**
>
> ソース IP AWS に基づいて へのアクセスを管理する IAM ポリシーは、`workspaces:Stream`アクションではサポートされていません。の IP アクセスコントロールを管理するには WorkSpaces、IP アクセスコントロールグループ を使用します。さらに、SAML 2.0 認証を使用する場合、SAML 2.0 IdP から利用可能な IP アクセスコントロールポリシーを使用できます。

1. 作成した IAM ロールの詳細で、[Permissions] (アクセス許可) タブを選択し、必要なアクセス許可を、ロールのアクセス許可ポリシーに追加します。[Create policy wizard] (ポリシーの作成ウィザード) が起動します。
2. [ポリシーの作成] で、[JSON] タブを選択します。
3. 次の JSON ポリシーを JSON ウィンドウにコピーして貼り付けます。次に、 AWS リージョンコード、アカウント ID、ディレクトリ ID を入力してリソースを変更します。次のポリシーでは、 `"Action": "workspaces:Stream"`は WorkSpaces 、 ディレクトリ内のデスクトップセッションに接続するためのアクセス許可を WorkSpaces ユーザーに付与するアクションです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
```

```
            }
        }
    ]
}
```

をディレクトリが存在する AWS リージョンREGION-CODEに置き換えます WorkSpaces。を、 WorkSpaces マネジメントコンソールにある WorkSpaces ディレクトリ ID DIRECTORY-IDに置き換えます。 AWS GovCloud （ 米国西部) または AWS GovCloud （ 米国東部) のリソースの場合、ARN には の形式を使用しますarn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID。

4. 完了したら、[ポリシーの確認] をクリックします。構文エラーがある場合は、「ポリシーの検証」によってレポートされます。

ステップ 4: SAML 2.0 ID プロバイダーを設定する

次に、SAML 2.0 IdP に応じて、https://signin.aws.amazon.com/static/saml-metadata.xml のsaml-metadata.xmlファイルを IdP にアップロードして、サービスプロバイダー AWS として信頼するように IdP を手動で更新する必要がある場合があります。このステップは、IdP のメタデータを更新します。一部の では IdPs、更新が既に設定されている場合があります。この場合は、次のステップに進みます。

IdP でこの更新がまだ設定されていない場合には、IdP から提供されるドキュメントでメタデータを更新する方法に関する情報を確認します。プロバイダーによっては、URL を入力し、また IdP によってファイルを取得してインストールするオプションが提供されます。また、URL からファイルをダウンロードし、ローカルファイルとして指定する必要があるプロバイダーもあります。

> **Important**
>
> 現時点では、IdP のユーザーに IdP で設定したアプリケーションへのアクセス WorkSpaces を許可することもできます IdP 。ディレクトリの WorkSpaces アプリケーションへのアクセスが許可されているユーザーには、自動的に WorkSpace が作成されません。同様に、が WorkSpace 作成されたユーザーは、 WorkSpaces アプリケーションへのアクセスを自動的に許可されません。SAML 2.0 認証を使用して に WorkSpace 正常に接続するには、ユーザーが IdP によって承認され、 が作成され WorkSpaceている必要があります。

ステップ 5: SAML 認証レスポンスのアサーションを作成する

次に、IdP が認証レスポンスで SAML 属性 AWS として に送信する情報を設定します。IdP によっては、既に設定されています。その場合、「ステップ 6: フェデレーションのリレーステートを設定する」へ進んでください。

この情報がまだ IdP で設定されていない場合は、次の操作を実行します。

- SAML Subject NameID (SAML サブジェクト名 ID) – 署名するユーザーの一意の識別子。値は WorkSpaces ユーザー名と一致する必要があり、通常は Active Directory ユーザーの sAMAccountName 属性です。
- SAML Subject Type (SAML サブジェクトタイプ) (値を `persistent` に設定) – 値を `persistent` に設定すると、特定のユーザーからのすべての SAML リクエストの `NameID` 要素に同じ一意の値を IdP が送信することを確保できます。ステップ 2: SAML 2.0 フェデレーション IAM ロールを作成するで説明されているように、SAML sub_type が `persistent` に設定されている SAML リクエストのみを許可する条件が IAM ポリシーに含まれていることを確認します。
- **`Attribute`** 要素 (**`Name`** 属性が **`https://aws.amazon.com/SAML/Attributes/Role`** に設定) – この要素には、IdP によってマッピングされたユーザーの IAM ロールと SAML IdP を一覧表示する 1 つ以上の `AttributeValue` 要素が含まれます。このロールと IdP は、カンマ区切りの ARN のペアとして指定されます。予期される値の例は `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME` です。
- **`Attribute Name`** 属性が に設定された 要素 **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** – この要素には、SSO 用に発行された AWS 一時的な認証情報の識別子を提供する `AttributeValue`要素が 1 つ含まれています。`AttributeValue` 要素の値は 2 ~ 64 文字とし、英数字、アンダースコア、および _ . : / = + - @ のみを含めることができます。スペースを含めることはできません。値は通常、E メールアドレスまたはユーザープリンシパル名 (UPN) です。ユーザーの表示名のように、スペースを含む値とすることはできません。
- **`Attribute`** 要素 (**`Name`** 属性を **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** に設定) – この要素には、ユーザーの E メールアドレスを指定する `AttributeValue` 要素が含まれます。値は、 WorkSpaces ディレクトリで定義されている WorkSpaces ユーザーの E メールアドレスと一致する必要があります。タグ値には、文字、数字、スペース、および特殊文字 (_ . : / = + - @) の組み合わせを含めることができます。詳細については、IAM ユーザーガイドの「IAM および AWS STSでのタグ付けの規則」を参照してください。
- **`Attribute`** 要素 (**`Name`** 属性を **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** に設定) (オプション) — この要素には、サインインして

いるユーザーの Active Directory `userPrincipalName` を指定する `AttributeValue` 要素が 1 つ含まれています。値は `username@domain.com` の形式で指定する必要があります。このパラメータは、証明書ベースの認証で、エンドユーザー証明書のサブジェクト代替名として使用します。詳細については、「証明書ベースの認証」を参照してください。

- **`Attribute` 要素 (`Name` 属性を `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid` に設定) (オプション)** — この要素には、サインインしているユーザーの Active Directory セキュリティ識別子 (SID) を指定する `AttributeValue` 要素が 1 つ含まれています。このパラメータを証明書ベースの認証で使用すると、Active Directory ユーザーへの強力なマッピングが可能になります。詳細については、「証明書ベースの認証」を参照してください。
- **`Attribute` 要素 (`Name` 属性を `https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName` に設定) (オプション)** — この要素には、代替ユーザー名形式を指定する `AttributeValue` 要素が 1 つ含まれています。 WorkSpaces クライアントを使用して`username@corp.example.com`ログインするために `corp\username`、、 などのユーザー名形式を必要とするユースケースがある場合は`corp.example.com\username`、この属性を使用します。タグのキーと値には、文字、数字、スペース、特殊文字 (_ : / . + = @ -) の任意の組み合わせを使用できます。詳細については、IAM ユーザーガイドの「IAM および AWS STSでのタグ付けの規則」を参照してください。`corp\username` または `corp.example.com\username` の形式を使用する場合は、SAML アサーションの \ を / に置き換えてください。
- **`AttributeName` 属性が** https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain **(オプション) に設定された 要素** – この要素には、サインインするユーザーの Active Directory DNS 完全修飾ドメイン名 (FQDN) を提供する `AttributeValue` 要素が 1 つ含まれています。このパラメータは、ユーザーの Active Directory `userPrincipalName` に代替サフィックスが含まれている場合に、証明書ベースの認証で使用されます。値は、サブドメインを含め、`domain.com` で指定する必要があります。
- **`Attribute Name` 属性が** https://aws.amazon.com/SAML/Attributes/SessionDuration **(オプション) に設定されている 要素** – この要素には、ユーザーのフェデレーティッドストリーミングセッションが再認証が必要になるまでアクティブのままになる最大時間を指定する `AttributeValue` 要素が 1 つ含まれています。デフォルト値は 3600 秒 (60 分) です。SAML IdP の詳細については、「SAML `SessionDurationAttribute`」を参照してください。

> **Note**
>
> `SessionDuration` はオプションの属性ですが、これを SAML レスポンスに含めることをお勧めします。この属性を指定しない場合、セッション期間はデフォルト値の 3600 秒

(60 分) に設定されます。 WorkSpaces デスクトップセッションは、セッション期間が終了すると切断されます。

これらの要素を設定する方法については、「IAM ユーザーガイド」の「認証レスポンスの SAML アサーションを設定する」を参照してください。IdP の特定の設定要件に関する詳細は、IdP のドキュメントを参照してください。

ステップ 6: フェデレーションのリレーステートを設定する

次に、IdP を使用して、 WorkSpaces ディレクトリリレーステート URL を指すようにフェデレーションのリレーステートを設定します。による認証が成功すると AWS、ユーザーは WorkSpaces ディレクトリエンドポイントに誘導され、SAML 認証レスポンスでリレーステートとして定義されます。

リレーステート URL は次の形式です。

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

ディレクトリ登録コードと、 WorkSpaces ディレクトリが配置されているリージョンに関連付けられたリレーステートエンドポイントからリレーステート URL を構築します。登録コードは WorkSpaces マネジメントコンソールにあります。

必要に応じて、 のクロスリージョンリダイレクトを使用している場合 WorkSpaces、登録コードをプライマリリージョンとフェイルオーバーリージョンのディレクトリに関連付けられた完全修飾ドメイン名 (FQDN) に置き換えることができます。詳細については、「Amazon のクロスリージョンリダイレクト WorkSpaces」を参照してください。クロスリージョンリダイレクトと SAML 2.0 認証を使用する場合、プライマリディレクトリとフェイルオーバーディレクトリの両方を SAML 2.0 認証に対して有効にし、各リージョンに関連付けられたリレーステートエンドポイントを使用して IdP で個別に設定する必要があります。これにより、ユーザーがサインインする前に WorkSpaces クライアントアプリケーションを登録するときに FQDN が正しく設定され、フェイルオーバーイベント中にユーザーが認証できるようになります。

次の表に、 WorkSpaces SAML 2.0 認証が利用可能なリージョンのリレーステートエンドポイントを示します。

WorkSpaces SAML 2.0 認証が利用可能なリージョン

リージョン	リレーステートのエンドポイント
米国東部 (バージニア北部) リージョン	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
米国西部 (オレゴン) リージョン	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
アフリカ (ケープタウン) リージョン	workspaces.euc-sso.af-south-1.aws.amazon.com
アジアパシフィック (ムンバイ) リージョン	workspaces.euc-sso.ap-south-1.aws.amazon.com
アジアパシフィック (ソウル) リージョン	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
アジアパシフィック (シンガポール) リージョン	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
アジアパシフィック (シドニー) リージョン	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
アジアパシフィック (東京) リージョン	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
カナダ (中部) リージョン	workspaces.euc-sso.ca-central-1.aws.amazon.com
欧州 (フランクフルト) リージョン	workspaces.euc-sso.eu-central-1.aws.amazon.com

リージョン	リレーステートのエンドポイント
欧州 (アイルランド) リージョン	workspaces.euc-sso.eu-west-1.aws.amazon.com
欧州 (ロンドン) リージョン	workspaces.euc-sso.eu-west-2.aws.amazon.com
南米 (サンパウロ) リージョン	workspaces.euc-sso.sa-east-1.aws.amazon.com
イスラエル (テルアビブ) リージョン	workspaces.euc-sso.il-central-1.aws.amazon.com
AWS GovCloud （米国西部）	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** 詳細については、(米国) ユーザーガイドの「Amazon WorkSpaces」を参照してください。 AWS GovCloud
AWS GovCloud （米国東部）	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** 詳細については、(米国) ユーザーガイドの「Amazon WorkSpaces」を参照してください。 AWS GovCloud

ステップ 7: WorkSpaces ディレクトリで SAML 2.0 との統合を有効にする

WorkSpaces コンソールを使用して、 WorkSpaces ディレクトリで SAML 2.0 認証を有効にできます。

SAML 2.0 との統合を有効にするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. のディレクトリ ID を選択します WorkSpaces。
4. [Authentication] (認証) で、[Edit] (編集) を選択します。
5. [Edit SAML 2.0 Identity Provider] (SAML 2.0 ID プロバイダーの編集) を選択します。
6. [Enable SAML 2.0 authentication] (SAML 2.0 認証の有効化) チェックボックスをオンにします。
7. [User Access URL] (ユーザーアクセス URL) と [IdP deep link parameter name] (IdP ディープリンクパラメータ名) には、ステップ 1 で設定した IdP とアプリケーションに該当する値を入力します。IdP ディープリンクパラメータ名のデフォルト値は、このパラメータを省略すると RelayState「」です。次の表に、アプリケーションの ID プロバイダー別に固有のユーザーアクセス URL とパラメータ名を示します。

   許可リストに追加するドメインと IP アドレス

ID プロバイダー	パラメータ	ユーザーアクセス URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity`

ID プロバイダー	パラメータ	ユーザーアクセス URL
		.com/saml2/sp/<app_id>/sso
Okta	RelayState	https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/<app-id>
Auth0	RelayState	https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>
PingFederate	TargetResource	https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>
PingOne エンタープライズ向け	TargetResource	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>

ユーザーアクセス URL は、通常、未承諾の IdP を起点とする SSO のプロバイダーによって定義されます。ユーザーはこの URL をウェブブラウザに入力して、SAML アプリケーションに直接フェデレートできます。IdP のユーザーアクセス URL とパラメータ値をテストするには、[Test] (テスト) を選択します。現在のブラウザまたは別のブラウザのプライベートウィンド

ウにテスト URL をコピーして貼り付け、現在の AWS 管理コンソールセッションを中断することなく SAML 2.0 ログオンをテストします。IdP 開始フローが開いたら、 WorkSpaces クライアントを登録できます。詳細については、「Identity provider (IdP)-initiated flow」(ID プロバイダー (IdP) を起点とするフロー) を参照してください。

8. [Allow clients that do not support SAML 2.0 to login] (SAML 2.0 をサポートしていないクライアントにログインを許可する) チェックボックスをオンまたはオフにして、フォールバック設定を管理します。この設定を有効にすると、SAML 2.0 をサポートしていないクライアントタイプまたはバージョン WorkSpaces の使用、またはユーザーが最新のクライアントバージョンへのアップグレードに時間が必要な場合は、引き続き へのアクセスをユーザーに許可できます。

> **Note**
>
> この設定により、ユーザーは SAML 2.0 ではなく、古いクライアントバージョンを使用したディレクトリ認証を通じてログインできます。

9. ウェブクライアントで SAML を使用するには、Web Access を有効にします。詳細については、「Amazon WorkSpaces Web Access の有効化と設定」を参照してください。

> **Note**
>
> SAML を使用する PCoIP は Web Access ではサポートされていません。

10. [保存] を選択します。これで、SAML 2.0 統合で WorkSpaces ディレクトリが有効になりました。IdP 開始フローとクライアントアプリケーション開始フローを使用して、 WorkSpaces クライアントアプリケーションを登録し、 にサインインできます WorkSpaces。

証明書ベースの認証

で証明書ベースの認証を使用して WorkSpaces 、Active Directory ドメインパスワードのユーザープロンプトを削除できます。Active Directory ドメインで証明書ベースの認証を使用すると、以下のことを行うことができます。

- SAML 2.0 ID プロバイダーに依頼してユーザーを認証し、Active Directory 内のユーザーと一致する SAML アサーションを提供する。
- ユーザープロンプトの回数を減らして、シングルサインオンでログオンできるようにする。
- SAML 2.0 ID プロバイダーを使用して、パスワードなしの認証フローを有効にする。

証明書ベースの認証では、 AWS アカウントの AWS Private CA リソースを使用します。 は、ルート CA と下位 CAs を含むプライベート認証機関 (CA) 階層の作成 AWS Private CA を有効にします。を使用すると AWS Private CA、独自の CA 階層を作成し、内部ユーザーを認証するための証明書を発行できます。詳細については、『AWS Private Certificate Authority ユーザーガイド』を参照してください。

証明書ベースの認証 AWS Private CA に を使用する場合、 WorkSpaces はセッション認証中にユーザーの証明書を自動的にリクエストします。ユーザーは、証明書によりプロビジョニングされた仮想スマートカードを使用して Active Directory に対して認証されます。

証明書ベースの認証は、最新の WorkSpaces Web Access、Windows、macOS クライアントアプリケーションを使用する Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) バンドルでサポートされています。Amazon WorkSpaces Client のダウンロードを開いて最新バージョンを検索します。

- Windows クライアントバージョン 5.5.0 以降
- macOS クライアントバージョン 5.6.0 以降

Amazon での証明書ベースの認証の設定の詳細については WorkSpaces、「Amazon の証明書ベースの認証を設定する方法 WorkSpaces」および AppStream 「2.0 および WorkSpaces での証明書ベースの認証の規制の厳しい環境での証明書ベースの認証に関する考慮事項の設計」を参照してください。

前提条件

証明書ベースの認証を有効にする前に、次の手順を実行してください。

1. 証明書ベースの認証を使用するように SAML 2.0 統合で WorkSpaces ディレクトリを設定します。詳細については、WorkSpaces「SAML 2.0 との統合」を参照してください。
2. SAML アサーションの `userPrincipalName` 属性を設定します。詳細については、「SAML 認証レスポンスのアサーションを作成する」を参照してください。
3. SAML アサーションの `ObjectSid` 属性を設定します。これは、Active Directory ユーザーへの強力なマッピングを行うためのオプションです。この属性が SAML_Subject `NameID` で指定したユーザーの Active Directory セキュリティ識別子 (SID) と一致しない場合、証明書ベースの認証は失敗します。詳細については、「SAML 認証レスポンスのアサーションを作成する」を参照してください。
4. SAML 2.0 設定で使用される IAM ロール信頼ポリシーに sts:TagSession アクセス許可がまだ存在しない場合は、追加します。このアクセス許可は、証明書ベースの認証を使用するために必要で

す。詳細については、「SAML 2.0 フェデレーション IAM ロールを作成する」を参照してください。

5. Active Directory で設定 AWS Private CA されていない場合は、 を使用してプライベート認証機関 (CA) を作成します。 AWS Private CA は証明書ベースの認証を使用する必要があります。詳細については、AWS Private CA 「デプロイの計画」を参照し、ガイダンスに従って証明書ベースの認証用に CA を設定します。証明書ベースの認証のユースケースでは、次の AWS Private CA 設定が最も一般的です。

   a. CA タイプオプション:

      i. 使用期間が短い証明書 CA 使用モード (証明書ベースの認証用のエンドユーザー証明書を発行するためだけに CA を使用する場合に推奨)

      ii. ルート CA を含む単一レベルの階層 (既存の CA 階層と統合する場合は下位 CA を選択することも可能)

   b. 主要なアルゴリズムオプション: RSA 2048

   c. サブジェクト識別名オプション: 複数のオプションを自由に組み合わせて、Active Directory の信頼されたルート認証局ストア内の CA を識別します。

   d. 証明書失効オプション: CRL ディストリビューション

   > **Note**
   >
   > 証明書ベースの認証には、デスクトップとドメインコントローラーからアクセスできるオンライン CRL ディストリビューションポイントが必要です。これには、プライベート CA CRL エントリ用に設定された Amazon S3 バケットへの認証されていないアクセス、または CloudFrontパブリックアクセスをブロックしている場合は S3 バケットにアクセスできるディストリビューションが必要です。これらのオプションの詳細については、「証明書失効リスト (CRL) を計画する」を参照してください。

6. プライベート CA に `euc-private-ca` という名前でキーをタグ付けし、EUC 証明書ベースの認証で使用する CA を指定します。このキーには値が必要ありません。詳細については、「プライベート CA のタグの管理」を参照してください。

7. 証明書ベースの認証では、ログオンに仮想スマートカードを使用します。Active Directory で「サードパーティの証明機関でスマートカードログオンを有効にするためのガイドライン」に従って、次の手順を実行します。

   - ドメインコントローラー証明書を使用して、スマートカードユーザーを認証するようにドメインコントローラーを設定します。Active Directory 証明書サービスのエンタープライズ CA が Active Directory に設定されている場合、ドメインコントローラーに証明書が自動的に登録さ

れ、スマートカードによるログオンが可能になります。Active Directory 証明書サービスがない場合は、「サードパーティ CA からのドメインコントローラー証明書の要件」を参照してください。ドメインコントローラー証明書は AWS Private CAで作成できます。その場合は、使用期間の短い証明書用に設定されたプライベート CA を使用しないでください。

> **Note**
>
> を使用している場合は AWS Managed Microsoft AD、ドメインコントローラー証明書の要件を満たすように EC2 インスタンスで Certificate Services を設定できます。Active Directory Certificate Services で設定された の AWS Managed Microsoft AD デプロイ例AWS Launch Wizardについては、「」を参照してください。 AWS プライベート CA は Active Directory Certificate Services CA の下位として設定することも、 を使用するときに独自のルートとして設定することもできます AWS Managed Microsoft AD。AWS Managed Microsoft AD および Active Directory Certificate Services の追加設定タスクは、コントローラー VPC セキュリティグループから Certificate Services を実行している EC2 インスタンスへのアウトバウンドルールを作成して、TCP ポート 135 および 49152-65535 で証明書の自動登録を有効にすることです。さらに、実行中の EC2 インスタンスは、ドメインインスタンス (ドメインコントローラーを含む) からのインバウンドアクセスを同じポートで許可する必要があります。のセキュリティグループの検索の詳細については、「VPC サブネットとセキュリティグループを設定する AWS Managed Microsoft AD 」を参照してください。

- AWS Private CA コンソールまたは SDK または CLI を使用して CA を選択し、CA 証明書で CA プライベート証明書をエクスポートします。詳細については「プライベート証明書のエクスポート」を参照してください。
- CA をアクティブディレクトリに公開します。ドメインコントローラーまたはドメインに参加しているマシンにログオンします。CA プライベート証明書を任意の `<path>\<file>` にコピーし、ドメイン管理者として次のコマンドを実行します。または、グループポリシーと Microsoft PKI Health Tool (PKIView) ツールを使用して CA を公開することもできます。詳細については、「設定手順」を参照してください。

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

コマンドが正常に完了したことを確認したら、プライベート証明書ファイルを削除します。Active Directory のレプリケーション設定によっては、CA がドメインコントローラーとデスクトップインスタンスに公開されるまでに数分かかる場合があります。

> **Note**
>
> - Active Directory は、デスクトップがドメインに参加している WorkSpaces ときに、信頼されたルート認証機関とエンタープライズ NTAuth ストアに CA を自動的に配布する必要があります。
> - 証明書の強力な強制で証明書ベースの認証をサポートするには、Active Directory ドメインコントローラーを互換モードにする必要があります。詳細については、Microsoft サポートドキュメントのKB5014754 — Windows ドメインコントローラーでの証明書ベースの認証の変更」を参照してください。 AWS Managed Microsoft AD を使用している場合は、「ディレクトリのセキュリティ設定の構成」を参照してください。

証明書ベースの認証を有効にする

証明書ベースの認証を有効にするには、次の手順を実行します。

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. のディレクトリ ID を選択します WorkSpaces。
4. [Authentication] (認証) で [Edit] (編集) をクリックします。
5. [Edit Certificate-Based Authentication] (証明書ベースの認証を編集) をクリックします。
6. [Enable Certificate-Based Authentication] (証明書ベースの認証を有効にする) チェックボックスをオンにします。
7. プライベート CA ARN がリストに関連付けられていることを確認します。プライベート CA は、同じ AWS アカウントと に存在し AWS リージョン、リストに表示する euc-private-ca という権限を持つキーでタグ付けされている必要があります。
8. [Save Changes] (変更の保存) をクリックします。これで証明書ベースの認証が有効になりました。
9. Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) バンドルを再起動して、変更を有効にします。詳細については、「 の再起動 WorkSpace」を参照してください。
10. 再起動後、ユーザーがサポートされているクライアントを使用して SAML 2.0 経由で認証すると、ドメインパスワードの入力を求めるプロンプトが表示されなくなります。

> **Note**
>
> 証明書ベースの認証が にサインインするように有効になっている場合 WorkSpaces、ディレクトリで有効になっていても、ユーザーは多要素認証 (MFA) を求められません。証明書ベースの認証を使用するときに、SAML 2.0 ID プロバイダーを通じて MFA を有効にすることができます。 AWS Directory Service MFA の詳細については、「多要素認証 (AD Connector)」または「 の多要素認証を有効にする AWS Managed Microsoft AD」を参照してください。

証明書ベースの認証の管理

CA 証明書

一般的な設定の場合、プライベート CA 証明書の有効期間は 10 年です。証明書の有効期限が切れた CA を置き換えたり、新しい有効期間で CA を再発行したりする方法の詳細については、「プライベート CA ライフサイクルの管理」を参照してください。

エンドユーザー証明書

証明書ベースの認証 AWS Private CA のために によって発行されたエンドユーザー WorkSpaces 証明書は、更新や取り消しを必要としません。これらの証明書は有効期間が短くなります。WorkSpaces は 24 時間ごとに新しい証明書を自動的に発行します。これらのエンドユーザー証明書の有効期間は、一般的な AWS Private CA CRL ディストリビューションよりも短くなります。そのため、エンドユーザー証明書を取り消さなくても、CRL に表示されなくなります。

監査レポート

プライベート CA が発行または取り消したすべての証明書を一覧表示する監査報告書を作成できます。詳細については、「プライベート CA での監査レポートの使用」を参照してください。

ログ記録とモニタリング

を使用してAWS CloudTrail、 AWS Private CA による への API コールを記録できます WorkSpaces。詳細については、「 の使用 CloudTrail」を参照してください。CloudTrail イベント履歴では、`EcmAssumeRoleSession`ユーザー名によって WorkSpaces作成された`IssueCertificate`イベントソースから `GetCertificate`および `acm-pca.amazonaws.com` イベント名を表示できます。これらのイベントは、EUC 証明書ベースの認証リクエストごとに記録されます。

クロスアカウント PCA 共有を有効にする

プライベート CA クロスアカウント共有を使用すると、集中型 CA を使用するアクセス許可を他のアカウントに付与できるため、すべてのアカウントでプライベート CA が不要になります。CA は、AWS Resource Access Manager を使用してアクセス許可を管理することで、証明書を生成して発行できます。プライベート CA クロスアカウント共有は、同じ AWS リージョン内の WorkSpaces 証明書ベースの認証 (CBA) で使用できます。

WorkSpaces CBA で共有 Private CA リソースを使用するには

1. 一元化された AWS アカウントで CBA のプライベート CA を設定します。詳細については、「証明書ベースの認証」を参照してください。
2. 「RAM を使用して ACM プライベート CA クロス AWS アカウント を共有する方法」の手順に従って、 WorkSpaces リソースが CBA を利用するリソースアカウントとプライベート CA を共有します。 AWS証明書を作成するには、ステップ 3 を完了する必要はありません。Private CA を個々の AWS アカウントと共有することも、 AWS Organizations を通じて共有することもできます。個々のアカウントと共有するには、Resource Access Manager (RAM) コンソールまたは APIs を使用して、リソースアカウントで共有プライベート CA を受け入れる必要があります。共有を設定するときは、リソースアカウントの Private CA の RAM リソース共有が `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` マネージドアクセス許可テンプレートを使用していることを確認します。このテンプレートは、CBA 証明書の発行時に WorkSpaces サービスロールが使用する PCA テンプレートと一致します。
3. 共有が成功すると、リソースアカウントの Private CA コンソールを使用して、共有 Private CA を表示できるようになります。
4. API または CLI を使用して、プライベート CA ARN を WorkSpaces ディレクトリプロパティの CBA に関連付けます。現時点では、 WorkSpaces コンソールは共有プライベート CA ARNs の選択をサポートしていません。CLI コマンドの例：

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

認証にスマートカードを使用する

Windows および Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) バンドルでは、認証に共通アクセスカード (CAC) および個人識別検証 (PIV) スマートカードを使用できます。

Amazon は、セッション前認証とセッション内認証の両方でスマートカードの使用 WorkSpaces をサポートしています。セッション前認証とは、ユーザーが にログインしている間に実行されるスマートカード認証を指します WorkSpaces。セッション内認証とは、ログイン後に実行される認証をいいます。

例えば、ユーザーは、ウェブブラウザやアプリケーションを操作しながら、セッション内認証にスマートカードを使用できます。また、管理アクセス許可が必要な操作にスマートカードを使用することもできます。例えば、ユーザーが Linux に対する管理アクセス許可を持っている場合 WorkSpace、 `sudo`および `sudo -i` コマンドの実行時にスマートカードを使用して自分自身を認証できます。

コンテンツ

要件

- セッション前認証には、Active Directory Connector (AD Connector) ディレクトリが必要です。AD Connector は、証明書ベースの相互 Transport Layer Security (相互 TLS) 認証を使用し、ハードウェアまたはソフトウェアベースのスマートカード証明書を使用して Active Directory に対してユーザーを認証します。AD Connector およびオンプレミスのディレクトリを設定する方法の詳細については、ディレクトリ設定 を参照してください。
- Windows または Linux でスマートカードを使用するには WorkSpace、ユーザーは Amazon WorkSpaces Windows クライアントバージョン 3.1.1 以降または WorkSpaces macOS クライアントバージョン 3.1.5 以降を使用する必要があります。Windows および macOS クライアントでのスマートカードの使用の詳細については、「Amazon WorkSpaces ユーザーガイド」の「スマートカードのサポート」を参照してください。

- ルート CA 証明書およびスマートカード証明書は、特定の要件を満たしている必要があります。詳細については、 AWS Directory Service 管理ガイドの「スマートカードで使用する AD Connector で mTLS 認証を有効にする」および Microsoft のドキュメントの「証明書の要件」を参照してください。

  これらの要件に加えて、Amazon へのスマートカード認証に使用されるユーザー証明書には、次の属性を含める WorkSpaces 必要があります。

  - 証明書の userPrincipalName (SAN) フィールドにある AD ユーザーの subjectAltName (UPN)。ユーザーのデフォルト UPN のスマートカード証明書を発行することをお勧めします。
  - クライアント認証 (1.3.6.1.5.5.7.3.2) 拡張キー使用法 (EKU) 属性。
  - スマートカードログオン (1.3.6.1.4.1.311.20.2.2) EKU 属性。
- セッション前認証では、証明書失効チェックにオンライン証明書状態プロトコル (OCSP) は必須です。セッション内認証では、OCSP を使用することをお勧めしますが、必須ではありません。

制限事項

- 現在、スマートカード認証では、 WorkSpaces Windows クライアントアプリケーションバージョン 3.1.1 以降と macOS クライアントアプリケーションバージョン 3.1.5 以降のみがサポートされています。
- WorkSpaces Windows クライアントアプリケーション 3.1.1 以降では、クライアントが 64 ビットバージョンの Windows で実行されている場合にのみスマートカードがサポートされます。
- Ubuntu は現在、スマートカード認証をサポート WorkSpaces していません。
- 現在、スマートカード認証では、AD Connector ディレクトリのみがサポートされています。
- セッション内認証は、WSP がサポートされているすべてのリージョンで利用可能です。セッション前認証は、以下のリージョンで使用できます。
  - アジアパシフィック (シドニー) リージョン
  - アジアパシフィック (東京) リージョン
  - 欧州 (アイルランド) リージョン
  - AWS GovCloud （ 米国東部) リージョン
  - AWS GovCloud （ 米国西部) リージョン
  - 米国東部 (バージニア北部) リージョン
  - 米国西部 (オレゴン) リージョン

- Linux または Windows でのセッション内認証およびセッション前認証の場合 WorkSpaces、現在許可されるスマートカードは 1 つだけです。
- 現在、セッション前認証において、スマートカード認証とサインイン認証の両方を同じディレクトリで有効にすることはサポートされていません。
- 現時点では、CAC カードと PIV カードのみがサポートされています。他のタイプのハードウェアまたはソフトウェアベースのスマートカードも機能する可能性がありますが、WSP での使用は完全にはテストされていません。

ディレクトリ設定

スマートカード認証を有効にするには、AD Connector ディレクトリおよびオンプレミスのディレクトリを次の方法で設定する必要があります。

AD Connector ディレクトリの設定

開始する前に、AWS Directory Service 管理ガイドの AD Connector の前提条件の説明に従って AD Connector ディレクトリが設定されていることを確認します。特に、ファイアウォールで必要なポートを開いていることを確認してください。

AD Connector ディレクトリの設定を完了するには、AWS Directory Service 管理ガイドの「スマートカードで使用する AD Connector で mTLS 認証を有効にする」の手順に従います。

> **Note**
>
> スマートカード認証が正しく機能するためには、Kerberos の制約付き委任 (KCD) が必要です。KCD では、AD Connector サービスアカウントのユーザー名部分がAccountName 、同じユーザーの sAM と一致する必要があります。sAM AccountName は 20 文字を超えることはできません。

オンプレミスのディレクトリの設定

AD Connector ディレクトリを設定するだけでなく、オンプレミスのディレクトリのドメインコントローラーに発行される証明書に「KDC 認証」拡張キー使用法 (EKU) が設定されていることも確認する必要があります。これを行うには、Active Directory Domain Services (AD DS) のデフォルトの Kerberos 認証証明書テンプレートを使用します。ドメインコントローラー証明書テンプレートまたはドメインコントローラー認証証明書テンプレートには、スマートカード認証に必要な設定が含まれていないため、これらのテンプレートを使用しないでください。

Windows 用のスマートカードを有効にする WorkSpaces

Windows でスマートカード認証を有効にする方法の一般的なガイダンスについては、Microsoft のドキュメントの「サードパーティの証明機関でスマートカードログオンを有効にするためのガイドライン」をご参照ください。

Windows ロック画面を検出してセッションを切断するには

画面がロックされているときにスマートカードセッション前認証が有効になってい WorkSpaces る Windows をユーザーがロック解除できるようにするには、ユーザーのセッションで Windows ロック画面検出を有効にします。Windows ロック画面が検出されると、 WorkSpace セッションは切断され、ユーザーはスマートカードを使用して WorkSpaces クライアントから再接続できます。

グループポリシー設定を使用して、Windows ロック画面が検出されたときに、セッションの切断を有効にできます。詳細については、「WSP の画面ロックの場合のセッションの切断を有効化/無効化する」を参照してください。

セッション内認証またはセッション前認証を有効にするには

デフォルトでは、Windows WorkSpaces はセッション前認証またはセッション内認証にスマートカードの使用をサポートしていません。必要に応じて、グループポリシー設定 WorkSpaces を使用して Windows のセッション内認証とセッション前認証を有効にできます。詳細については、「WSP のスマートカードリダイレクトを有効化/無効化する」を参照してください。

セッション前認証を使用するには、グループポリシー設定の更新に加えて、AD Connector ディレクトリ設定からセッション前認証を有効にする必要があります。詳細については、AWS Directory Service 管理ガイドの「スマートカードで使用する AD Connector で mTLS 認証を有効にする」を参照してください。

ユーザーがブラウザでスマートカードを使用できるようにするには

ユーザーが Chrome をブラウザとして使用している場合、スマートカードを使用するために特別な設定は必要ありません。

ユーザーが Firefox をブラウザとして使用している場合は、グループポリシーを通じて Firefox でスマートカードを使用できるように設定できます。これらの Firefox グループポリシーテンプレートは、 で使用できます GitHub。

例えば、PKCS #11 をサポートするために、Windows 用 OpenSC の 64 ビットバージョンをインストールし、次のグループポリシー設定を使用できます。ここで、*NAME_OF_DEVICE* は PKCS #11 の

識別に使用する任意の値 (OpenSC など)、*PATH_TO_LIBRARY_FOR_DEVICE* は PKCS #11 モジュールへのパスです。このパスは、.DLL 拡張子の付いたライブラリ (`C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll` など) をポイントする必要があります。

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

OpenSC を使用している場合は、pkcs11 プログラムを実行して OpenSC `pkcs11-register.exe` モジュールを Firefox にロードすることもできます。このプログラムを実行するには、`C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` のファイルをダブルクリックするか、コマンドプロンプトウィンドウを開き、次のコマンドを実行します。

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

OpenSC pkcs11 モジュールが Firefox にロードされたことを確認するには、次の操作を行います。

1. Firefox が既に実行されている場合は、Firefox を終了します。
2. Firefox を開きます。右上のメニューボタン

   を選択し、[Options] (オプション) を選択します。
3. [about:preferences] ページの左側のナビゲーションペインで、[Privacy & Security] (プライバシーとセキュリティ) を選択します。
4. [Certificates] (証明書) で、[Security Devices] (セキュリティデバイス) を選択します。
5. [Device Manager] (デバイスマネージャー) ダイアログボックスで、左側のナビゲーションに OpenSC スマートカードフレームワーク (0.21) が表示され、選択すると次の値が表示されます。

   モジュール: `OpenSC smartcard framework (0.21)`

   パス: `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

トラブルシューティング

スマートカードのトラブルシューティングについては、Microsoft のドキュメントの「証明書と構成に関する問題」をご参照ください。

問題を引き起こす可能性のある一般的な問題は次のとおりです。

- 証明書へのスロットのマッピングが正しくありません。
- ユーザーと一致する複数の証明書がスマートカードにあること。証明書は、以下の基準を使用して照合されます。
  - 証明書のルート CA。
  - 証明書の <KU> フィールドおよび <EKU> フィールド。
  - 証明書のサブジェクトの UPN。
- キーの使用に <EKU>msScLogin が含まれる複数の証明書を有していること。

一般的に、スマートカード認証のために、スマートカードの最初のスロットにマッピングされた証明書を 1 つだけ使用することがベストプラクティスです。

スマートカード上の証明書およびキーを管理するためのツール (証明書およびキーの削除または再マッピングなど) は、製造元によって異なる場合があります。詳細については、スマートカードの製造元から提供されているドキュメントをご参照ください。

Linux 用のスマートカードを有効にする WorkSpaces

> **Note**
>
> 現在、WSP WorkSpaces の Linux には以下の制限があります。
>
> - クリップボード、オーディオ入力、ビデオ入力、およびタイムゾーンのリダイレクトはサポートされていません。
> - マルチモニターはサポートされていません。
> - WSP で Linux に接続するには、 WorkSpaces Windows WorkSpaces クライアントアプリケーションを使用する必要があります。

Linux でスマートカードを使用できるようにするには WorkSpaces、 WorkSpace イメージに PEM 形式のルート CA 証明書ファイルを含める必要があります。

ルート CA 証明書を取得するには

ルート CA 証明書は、いくつかの方法で取得できます。

- サードパーティーの証明機関によって運用されるルート CA 証明書を使用できます。
- ウェブ登録サイト (http://*ip_address*/certsrv または http://*fqdn*/certsrv) を使用して、独自のルート CA 証明書をエクスポートできます。ここで、*ip_address* および *fqdn* はルート証明書 CA サーバーの IP アドレスおよび完全修飾ドメイン名 (FQDN) です。ウェブ登録サイトの使用の詳細については、Microsoft のドキュメントの「ルート証明機関の証明書をエクスポートする方法」をご参照ください。
- 次の手順を使用して、Active Directory 証明書サービス (AD CS) を実行しているルート CA 証明書サーバーからルート CA 証明書をエクスポートできます。AD CS のインストールの詳細については、Microsoft のドキュメントの「証明機関をインストールする」をご参照ください。

  1. 管理者アカウントを使用してルート CA サーバーにログインします。
  2. Windows の [Start] (スタート) メニューから、コマンドプロンプトウィンドウ ([Start] (スタート) > [Windows System] (Windows システム) > [Command Prompt] (コマンドプロンプト)) を開きます。
  3. 次のコマンドを使用して、ルート CA 証明書を新しいファイルにエクスポートします。ここで、*rootca*.cer は新しいファイルの名前です。

     ```
     certutil -ca.cert rootca.cer
     ```

     certutil の実行の詳細については、Microsoft のドキュメントの「certutil」をご参照ください。
  4. 次の OpenSSL コマンドを使用して、エクスポートされたルート CA 証明書を DER 形式から PEM 形式に変換します。ここで、*rootca* は証明書の名前です。OpenSSL の詳細については、www.openssl.org をご参照ください。

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

Linux にルート CA 証明書を追加するには WorkSpaces

お客様がスマートカードを有効にするのをサポートするために、この enable_smartcard スクリプトを当社の Amazon Linux WSP バンドルに追加しました。このスクリプトは以下のアクションを実行します。

- ルート CA 証明書をネットワークセキュリティサービス (NSS) データベースにインポートします。
- PAM (Pluggable Authentication Module) 認証用の pam_pkcs11 モジュールをインストールします。
- プロビジョニングpkinit中の WorkSpace の有効化を含むデフォルト設定を実行します。

次の手順では、 enable_smartcardスクリプトを使用して Linux にルート CA 証明書を追加 WorkSpaces し、Linux のスマートカードを有効にする方法について説明します WorkSpaces。

1. WSP プロトコルを有効に WorkSpace して新しい Linux を作成します。Amazon WorkSpaces コンソール WorkSpace のバンドルの選択ページで を起動するときは、プロトコルに WSP を選択し、Amazon Linux 2 パブリックバンドルのいずれかを選択してください。
2. 新しい で WorkSpace、次のコマンドを root として実行します。ここで、 *pem-path*は PEM 形式のルート CA 証明書ファイルへのパスです。

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path
   ```

   > **Note**
   >
   > Linux では、スマートカードの証明書が などのユーザーのデフォルトのユーザープリンシパル名 (UPN) に対して発行されていることを WorkSpaces 前提としています。ここで*sAMAccountName*@*domain*、 *domain*は完全修飾ドメイン名 (FQDN) です。
   > 代替 UPN サフィックスを使用するには、run /usr/lib/skylight/enable_smartcard --help をご参照ください。代替 UPN サフィックスのマッピングは、各ユーザーに固有です。したがって、そのマッピングは各ユーザーの で個別に実行する必要があります WorkSpace。

3. (オプション) デフォルトでは、Linux でスマートカード認証を使用するようにすべてのサービスが有効になっています WorkSpaces。特定のサービスについてのみスマートカード認証を使用できるようにするには、/etc/pam.d/system-auth を編集する必要があります。必要に応じて、auth の pam_succeed_if.so 行のコメントを解除し、サービスのリストを編集します。

   auth 行のコメントを解除した後、あるサービスについてスマートカード認証を使用できるようにするには、その行をリストに追加する必要があります。あるサービスににについてパスワード認証のみを使用するには、リストからそのサービスを削除する必要があります。

4. に追加のカスタマイズを実行します WorkSpace。例えば、システム全体のポリシーを追加して、ユーザーが Firefox でスマートカードを使用できるようにします。(Chrome ユーザーは、クライアントでスマートカードを有効にする必要があります。 詳細については、「Amazon ユーザーガイド」の「スマートカードのサポート」を参照してください。) WorkSpaces
5. からカスタム WorkSpace イメージとバンドルを作成します WorkSpace。
6. 新しいカスタムバンドルを使用して、ユーザーの WorkSpaces を起動します。

ユーザーが Firefox でスマートカードを使用できるようにするには

Linux WorkSpace イメージに SecurityDevices ポリシーを追加することで、ユーザーが Firefox でスマートカードを使用できるようにすることができます。システム全体のポリシーを Firefox に追加する方法の詳細については、「」の「Mozilla ポリシーテンプレート」を参照してください GitHub。

1. WorkSpace イメージの作成に WorkSpace 使用している で、 `policies.json`という名前の新しいファイルを作成します`/usr/lib64/firefox/distribution/`。
2. JSON ファイルに次の SecurityDevices ポリシーを追加します。ここで、*`NAME_OF_DEVICE`*は`pkcs`モジュールを識別するために使用する任意の値です。例えば、`"OpenSC"` などの値を使用できます。

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
        }
    }
}
```

トラブルシューティング

トラブルシューティングのために、`pkcs11-tools` ユーティリティを追加することをお勧めします。このユーティリティを使用すると、次のアクションを実行できます。

- 各スマートカードを一覧表示します。
- 各スマートカードのスロットを一覧表示します。
- 各スマートカードの証明書を一覧表示します。

問題を引き起こす可能性のある一般的な問題は次のとおりです。

- 証明書へのスロットのマッピングが正しくありません。
- ユーザーと一致する複数の証明書がスマートカードにあること。証明書は、以下の基準を使用して照合されます。
  - 証明書のルート CA。
  - 証明書の <KU> フィールドおよび <EKU> フィールド。
  - 証明書のサブジェクトの UPN。
- キーの使用に <EKU>msScLogin が含まれる複数の証明書を有していること。

一般的に、スマートカード認証のために、スマートカードの最初のスロットにマッピングされた証明書を 1 つだけ使用することがベストプラクティスです。

スマートカード上の証明書およびキーを管理するためのツール (証明書およびキーの削除または再マッピングなど) は、製造元によって異なる場合があります。スマートカードの操作に使用できるその他のツールは次のとおりです。

- opensc-explorer
- opensc-tool
- pkcs11_inspect
- pkcs11_listcerts
- pkcs15-tool

デバッグログを有効にするには

pam_pkcs11 および pam-krb5 の設定のトラブルシューティングを行うには、デバッグのログを有効にします。

1. /etc/pam.d/system-auth-ac ファイルで、auth アクションを編集し、nodebug の pam_pksc11.so パラメータを debug に変更します。
2. /etc/pam_pkcs11/pam_pkcs11.conf ファイルで、debug = false; を debug = true; に変更します。debug オプションは、各マッパーモジュールに個別に適用されるので、pam_pkcs11 セクションの直下と適切なマッパーセクション (デフォルトでは、これは mapper generic) の両方で変更する必要がある場合があります。
3. /etc/pam.d/system-auth-ac ファイルで、auth アクションを編集し、debug または debug_sensitive パラメータを pam_krb5.so に追加します。

デバッグのログを有効にすると、システムはアクティブな端末に直接 pam_pkcs11 デバッグメッセージを出力します。pam_krb5 からのメッセージは /var/log/secure でログインされます。

スマートカード証明書がマップされるユーザー名を確認するには、次の pklogin_finder コマンドを使用します。

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

プロンプトが表示されたら、スマートカードの PIN を入力します。pklogin_finder は、スマートカード証明書のユーザー名を stdout に *NETBIOS**username* 形式で出力します。このユーザー名は WorkSpace ユーザー名と一致する必要があります。

Active Directory Domain Services (AD DS) では、NetBIOS ドメイン名は Windows 2000 より前のドメイン名です。通常 (ただし、常にではありません)、NetBIOS ドメイン名はドメインネームシステム (DNS) ドメイン名のサブドメインです。例えば、DNS ドメイン名が example.com の場合、NetBIOS ドメイン名は通常 EXAMPLE です。DNS ドメイン名が corp.example.com の場合、NetBIOS ドメイン名は通常 CORP です。

例えば、mmajor ドメイン内のユーザー corp.example.com の場合、pklogin_finder からの出力は CORP\mmajor です。

> **Note**
>
> メッセージ "ERROR:pam_pkcs11.c:504: verify_certificate() failed" を受け取った場合、このメッセージは、pam_pkcs11 がユーザー名の条件に一致する証明書をスマートカード上に見つけたものの、マシンで認識されるルート CA 証明書に連鎖していないことを示します。この場合、pam_pkcs11 は上記のメッセージを出力し、次の証明書を試します。認証を許可するのは、ユーザー名と一致し、かつ、認識されたルート CA 証明書まで連鎖する証明書が見つかった場合だけです。

pam_krb5 設定をトラブルシューティングするには、次のコマンドを使用して、デバッグモードで手動で kinit を起動できます。

```
KRB5_TRACE=/dev/stdout kinit -V
```

このコマンドは、Kerberos Ticket Granting Ticket (TGT) を正常に取得するはずです。失敗する場合は、正しい Kerberos プリンシパル名をコマンドに明示的に追加してみてください。例えば、ドメイン mmajor 内のユーザー corp.example.com の場合は、次のコマンドを使用します。

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

このコマンドが成功した場合、 WorkSpace ユーザー名から Kerberos プリンシパル名へのマッピングに問題がある可能性が最も高くなります。[appdefaults]/pam/mappings ファイル内の /etc/krb5.conf セクションを確認してください。

このコマンドが成功せず、パスワードベースの kinit コマンドが成功した場合は、pkinit_ ファイル内の /etc/krb5.conf に関連する設定を確認してください。例えば、スマートカードに複数の証明書が含まれている場合は、pkinit_cert_match に変更を加える必要がある場合があります。

からのインターネットアクセスを提供する WorkSpace

オペレーティングシステムに更新をインストールしてアプリケーションをデプロイするには、 がインターネットにアクセスできる WorkSpaces 必要があります。次のいずれかのオプションを使用して、Virtual Private Cloud (VPC) WorkSpaces の がインターネットにアクセスできるようにします。

オプション

- プライベートサブネット WorkSpaces で を起動し、VPC のパブリックサブネットで NAT ゲートウェイを設定します。
- をパブリックサブネット WorkSpaces で起動し、 にパブリック IP アドレスを自動または手動で割り当てます WorkSpaces。

これらのオプションの詳細については、の VPC を設定する WorkSpaces の対応するセクションを参照してください。

これらのオプションのいずれかを使用して、 のセキュリティグループ WorkSpacesがすべての宛先 () へのポート 80 (HTTP) および 443 (HTTPS) でのアウトバウンドトラフィックを許可していることを確認する必要があります0.0.0.0/0。

Amazon Linux Extras Library

Amazon Linux リポジトリを使用している場合は、Amazon Linux がインターネットにアクセスできる WorkSpaces か、このリポジトリとメイン Amazon Linux リポジトリへの VPC エンドポイントを設定する必要があります。詳細については、Amazon S3 のエンドポイントの例: Amazon Linux AMI リポジトリへのアクセスの有効化のセクションを参照してください。Amazon Linux AMI リポジトリは、各リージョン内の Amazon S3 バケットです。VPC 内のインスタンスが、エンドポイント経由

でリポジトリにアクセスできるようにする場合、それらのバケットへのアクセスを有効にするエンドポイントポリシーを作成します。次のポリシーでは、Amazon Linux リポジトリへのアクセスが許可されます。

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

のセキュリティグループ WorkSpaces

にディレクトリを登録すると WorkSpaces、2 つのセキュリティグループが作成されます。1 つはディレクトリコントローラー用、もう 1 つはディレクトリ WorkSpaces 内の 用です。ディレクトリコントローラーのセキュリティグループの名前は、ディレクトリ識別子の後に _controllers が続きます (たとえば、d-12345678e1_controllers)。のセキュリティグループには、ディレクトリ識別子の後に _workspacesMembers が続く名前 (d-123456fc11_workspacesMembers など) WorkSpaces があります。

> **Warning**
>
> _controllers と _workspacesMembers セキュリティグループを変更、削除、またはデタッチすることは避けてください。これらのセキュリティグループを変更または削除する場合は注意が必要です。これらのグループを再作成したり、変更または削除した後に追加し直したりすることはできないからです。詳細は、「Linux インスタンス用の Amazon EC2 セキュリティグループ」または「Windows インスタンス用 Amazon EC2 セキュリティグループ」を参照してください。

デフォルトの WorkSpaces セキュリティグループをディレクトリに追加できます。新しいセキュリティグループを WorkSpaces ディレクトリに関連付けると、起動 WorkSpaces した新しい または再構築 WorkSpaces した既存の に新しいセキュリティグループが割り当てられます。このトピックで後述するように、 を再構築 WorkSpaces せずに、この新しいデフォルトのセキュリティグループを既存の に追加することもできます。

複数のセキュリティグループを WorkSpaces ディレクトリに関連付けると、各セキュリティグループのルールが効果的に集約され、1 つのルールセットが作成されます。セキュリティグループルールをできるだけ凝縮することをお勧めします。

VPC セキュリティグループの詳細については、Amazon VPC ユーザーガイドの VPC のセキュリティグループを参照してください。

セキュリティグループを WorkSpaces ディレクトリに追加するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Security Group] を展開して、セキュリティグループを選択します。
5. [Update and Exit] を選択します。

既存の にセキュリティグループを再構築 WorkSpace せずに追加するには、 の Elastic Network Interface (ENI) に新しいセキュリティグループを割り当てます WorkSpace。

既存の にセキュリティグループを追加するには WorkSpace

1. 更新 WorkSpace する必要がある各 の IP アドレスを見つけます。
   a. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
   b. 各 を展開 WorkSpace し、その WorkSpace IP アドレスを記録します。
2. それぞれの ENI を検索 WorkSpace し、セキュリティグループの割り当てを更新します。
   a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
   b. [ネットワークとセキュリティ] で、[ネットワークインターフェイス] を選択します。
   c. ステップ 1 で記録した最初の IP アドレスを検索します。
   d. IP アドレスに関連付けられている ENI を選択し、[アクション]、[セキュリティグループの変更] の順に選択します。

e. 新しいセキュリティグループを選択し、[保存] を選択します。

f. 必要に応じて、他の に対してこのプロセスを繰り返します WorkSpaces。

WorkSpaces の IP アクセスコントロールグループ

Amazon WorkSpaces では、WorkSpaces にアクセスできる IP アドレスを制御できます。IP アドレスに基づくコントロールグループを使用すると、信頼できる IP アドレスのグループを定義および管理し、信頼できるネットワークに接続しているときにだけ WorkSpaces にアクセスできるようにすることができます。

IP アクセスアクセスコントロールグループは、ユーザーが自分の WorkSpaces にアクセスできる IP アドレスを制御する仮想ファイアウォールとして機能します。CIDR アドレス範囲を指定するには、IP アクセスコントロールグループにルールを追加し、グループをディレクトリに関連付けます。各 IP アクセスコントロールグループを1 つまたは複数のディレクトリに関連付けることができます。AWS アカウントあたり最大 100 の IP アクセスコントロールグループをリージョンごとに作成できます。ただし、1 つのディレクトリに関連付けることができるのは、最大 25 の IP アクセスコントロールグループのみです。

デフォルトの IP アクセスコントロールグループが各ディレクトリに関連付けられています。このデフォルトのグループには、ユーザーがどこからでも自分の WorkSpaces にアクセスできるようにするデフォルトのルールが含まれています。ディレクトリのデフォルトの IP アクセスコントロールグループを変更することはできません。IP アクセスコントロールグループをディレクトリに関連付けない場合は、デフォルトのグループが使用されます。IP アクセスコントロールグループをディレクトリに関連付けると、デフォルトの IP アクセスコントロールグループの関連付けが解除されます。

信頼できるネットワークのパブリック IP アドレスと IP アドレスの範囲を指定するには、IP アクセスコントロールグループにルールを追加します。ユーザーが NAT ゲートウェイまたは VPN 経由で WorkSpaces にアクセスする場合は、NAT ゲートウェイまたは VPN のパブリック IP アドレスからのトラフィックを許可するルールを作成する必要があります。

> **Note**
>
> - IP アクセスコントロールグループでは、NAT 用に動的 IP アドレスを使用することはできません。NAT を使用している場合は、動的 IP アドレスではなく静的 IP アドレスを使用するように設定します。WorkSpaces セッションの間、NAT がすべての UDP トラフィックを同じ静的 IP アドレス経由でルーティングするようにします。

- IP アクセス制御グループは、ユーザーが WorkSpaces にストリーミングセッションを接続できる IP アドレスを制御します。ユーザーは、Amazon WorkSpaces パブリック API を使用して、任意の IP アドレスから再起動、再構築、シャットダウンなどの機能を実行できます。

この機能は、Web Access、PCoIP ゼロクライアント、ならびに macOS、iPad、Windows、Chromebook、および Android 用のクライアントアプリケーションで使用できます。

IP アクセスコントロールグループを作成する

IP アクセスコントロールグループは、次のように作成できます。各 IP アクセスコントロールグループには、最大 10 個のルールを含めることができます。

IP アクセスコントロールグループを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. [IP グループの作成] を選択します。
4. [IP グループの作成] ダイアログボックスで、グループ名と説明を入力し、[作成] を選択します。
5. グループを選択してから、[編集] を選択します。
6. 各 IP アドレスで、[Add Rule (ルールの追加)] を選択します。[Source (送信元)] に IP アドレスまたは IP アドレスの範囲を入力します。[説明] に説明を入力します。ルールの追加を完了したら、[保存] を選択します。

IP アクセスコントロールグループをディレクトリに関連付ける

IP アクセスコントロールグループをディレクトリに関連付けることで、信頼できるネットワークからのみ WorkSpaces にアクセスできるようにすることができます。

ルールを持たない IP アクセスコントロールグループをディレクトリに関連付けると、すべての WorkSpaces へのすべてのアクセスがブロックされます。

IP アクセスコントロールグループをディレクトリに関連付けるには

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

2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [IP アクセスコントロールグループ] を展開し、1 つ以上の IP アクセスコントロールグループを選択します。
5. [Update and Exit] を選択します。

IP アクセスコントロールグループをコピーする

既存の IP アクセスコントロールグループを新しい IP アクセスコントロールグループを作成するためのベースとして使用できます。

既存の IP アクセスコントロールグループから新しいグループを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. グループを選択して、[アクション]、[コピーして新規作成] の順に選択します。
4. [IP グループのコピー] ダイアログボックスで、新しいグループの名前と説明を入力し、[グループのコピー] を選択します。
5. (オプション) 元のグループからコピーしたルールを変更するには、新しいグループを選択し、[編集] を選択します。必要に応じてルールを追加、更新、または削除します。[保存] を選択します。

IP アクセスコントロールグループを削除する

IP アクセスコントロールグループからいつでもルールを削除できます。WorkSpace への接続を許可するために使用されたルールを削除すると、そのユーザーは WorkSpace から切断されます。

IP アクセスコントロールグループを削除する前に、任意のディレクトリから関連付けを解除する必要があります。

IP アクセスコントロールグループを削除するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. IP アクセスコントロールグループに関連付けられている各ディレクトリで、ディレクトリを選択し、[アクション]、[更新の詳細] の順に選択します。[IP アクセスコントロールグループ] を展

開し、IP アクセスコントロールグループのチェックボックスをオフにして、[更新と終了] を選択します。

4. ナビゲーションペインで [IP アクセスコントロール] を選択します。
5. グループを選択し、[アクション]、[IP グループの削除] を選択します。

WorkSpaces の PCoIP ゼロクライアントをセットアップする

PCoIP ゼロクライアントは、PCoIP プロトコルを使用する WorkSpaces バンドルと互換性があります。

ゼロクライアントデバイスにファームウェアバージョン 6.0.0 以降がある場合、ユーザーは各自の WorkSpaces に直接接続できます。ユーザーが、ゼロクライアントデバイスを使用して WorkSpaces に直接接続する場合には、WorkSpaces ディレクトリに Multi-Factor Authentication (MFA) を使用することをお勧めします。ディレクトリに MFA を使用する方法については、次のドキュメントを参照してください。

- AWS Managed Microsoft AD — AWS Directory Service管理ガイドの AWS Managed Microsoft AD の多要素認証を有効にする
- AD Connector — AWS Directory Service 管理ガイドの AD Connector の多要素認証を有効にするおよび 多要素認証 (AD Connector)
- 信頼されたドメイン — AWS Directory Service 管理ガイドの AWS Managed Microsoft AD の多要素認証を有効にする
- Simple AD — 多要素認証は、Simple AD では使用できません。

2021 年 4 月 13 日以降、バージョンが 4.6.0 ~ 6.0.0 のゼロクライアントデバイスファームウェアでは、PCoIP Connection Manager の使用がサポートされなくなりました。バージョンが 6.0.0 以降ではないゼロクライアントファームウェアをご使用のお客様は、https://www.teradici.com/desktop-access の Desktop Access サブスクリプションを通じて最新のファームウェアをご入手いただけます。

> **Important**
>
> - Teradici PCoIP Administrative Web Interface (AWI) または Teradici PCoIP Management Console (MC) で、必ずネットワークタイムプロトコル (NTP) を有効にします。NTP ホストの DNS 名には **`pool.ntp.org`** を使用し、NTP ホストポートを 123 に設定します。NTP が有効になっていない場合、PCoIP ゼロクライアントユーザーに、「指定された

証明書はタイムスタンプのため無効です」などの証明書の失敗エラーが表示されることがあります。

- PCoIP エージェントのバージョン 20.10.4 以降、Amazon WorkSpaces は、Windows レジストリを介して USB リダイレクトをデフォルトで無効にします。このレジストリ設定は、ユーザーが PCoIP ゼロクライアントデバイスを使用して WorkSpaces に接続する場合の USB 周辺機器の動作に影響します。詳細については、「PCoIP ゼロクライアントで USB プリンタと他の USB 周辺機器が動作しない」を参照してください。

PCoIP ゼロクライアントデバイスをセットアップし、接続する方法については、Amazon WorkSpaces ユーザーガイドの PCoIP ゼロクライアントを参照してください。承認された PCoIP ゼロクライアントデバイスのリストについては、Teradici ウェブサイトの「PCoIP Zero Clients」をご参照ください。

Chromebook 用の Android のセットアップ

バージョン 2.4.13 は、Amazon WorkSpaces Chromebook クライアントアプリケーションの最終リリースです。 Google は Chrome Apps のサポートを段階的に廃止するため、 WorkSpaces Chromebook クライアントアプリケーションにはそれ以上の更新はなく、その使用はサポートされていません。

Android アプリケーションのインストールをサポートする Chromebook の場合は、代わりに WorkSpaces Android クライアントアプリケーションを使用することをお勧めします。

ユーザーが Amazon Android クライアントアプリケーションをインストールする前に、2019 年より前にリリースされた一部の Chromebook で WorkSpaces Android アプリケーションをインストールできるようにする必要があります。詳細については、「Chrome OS Systems Supporting Android Apps」を参照してください。

ユーザーの Chromebook で Android アプリをインストールできるようにリモート管理する方法については、「Set up Android on Chrome devices」を参照してください。

Amazon WorkSpaces Web Access の有効化と設定

ほとんどの WorkSpaces バンドルは Amazon WorkSpaces Web Access をサポートしています。ウェブブラウザアクセスをサポートする のリストについては、「どの Amazon WorkSpaces バンドル WorkSpaces がウェブアクセスをサポートしていますか？」を参照してください。クライアントアクセス、Web アクセス、およびユーザーエクスペリエンスで。

Note

- WSP for Windows と Ubuntu によるウェブアクセス WorkSpaces は、 WorkSpaces WSP が利用可能なすべてのリージョンでサポートされています。Amazon Linux 用 WSP WorkSpaces は、 AWS GovCloud （ 米国西部) でのみ使用できます。
- ストリーミング品質とユーザーエクスペリエンスを最大限に高め WorkSpaces るには、WSP で Web Access を使用することを強くお勧めします。PCoIP WorkSpaces で Web Access を使用する場合の制限は次のとおりです。
  - PCoIP によるウェブアクセスは、、アジアパシフィック (ムンバイ） AWS GovCloud (US) Regions、アフリカ (ケープタウン ）、イスラエル (テルアビブ) ではサポートされていません。
  - PCoIP によるウェブアクセスは Windows でのみサポートされ WorkSpaces、Amazon Linux ではサポートされません WorkSpaces。
  - ウェブアクセスは、PCoIP プロトコル WorkSpaces を使用している一部の Windows 10 では使用できません。PCoIP WorkSpaces が Windows Server 2019 または 2022 で動作している場合、ウェブアクセスは使用できません。
- ウェブブラウザを使用して GPU 対応 に接続することはできません WorkSpaces。
- VPN で macOS を使用し、Firefox ウェブブラウザを使用している場合、ウェブブラウザは WorkSpaces Web Access を使用した PCoIP WorkSpaces のストリーミングをサポートしません。これは Firefox の WebRTC プロトコル実装における制限によるものです。

Important

2020 年 10 月 1 日以降、お客様は Amazon WorkSpaces Web Access クライアントを使用して Windows 7 カスタム WorkSpaces または Windows 7 Bring Your Own License (BYOL) に接続できなくなります WorkSpaces。

ステップ 1: へのウェブアクセスを有効にする WorkSpaces

へのウェブアクセス WorkSpaces は、ディレクトリレベルで制御します。ユーザーが Web Access クライアント経由でアクセス WorkSpaces できるようにする を含むディレクトリごとに、次の手順を実行します。

へのウェブアクセスを有効にするには WorkSpaces

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [Directory ID] (ディレクトリ ID) 列で、Web Access を有効にするディレクトリのディレクトリ ID を選択します。
4. [Directory Details] (ディレクトリの詳細) ページで、[Other platforms] (その他のプラットフォーム) セクションまでスクロールし、[Edit] (編集) を選択します。
5. [Web Access] を選択します。
6. [保存] を選択します。

> **Note**
>
> Web Access を有効にしたら、 を再起動して WorkSpace 変更を適用します。

ステップ 2: Web Access 用のポートへのインバウンドおよびアウトバウンドアクセスを設定する

Amazon WorkSpaces Web Access では、特定のポートに対してインバウンドおよびアウトバウンドのアクセスが必要です。詳細については、「Web Access のポート」を参照してください。

ステップ 3: グループポリシーとセキュリティポリシーの設定を構成してユーザーがログオンできるようにする

Amazon WorkSpaces は、ユーザーが Web Access クライアントから正常にログオンできるように、特定のログオン画面設定に依存しています。

Web Access ユーザーが にログオンできるようにするには WorkSpaces、グループポリシー設定と 3 つのセキュリティポリシー設定を設定する必要があります。これらの設定が正しく設定されていない場合、ユーザーが にログオンしようとすると、ログオン時間が長くなり、画面が黒くなることがあります WorkSpaces。これらの設定を構成するには、次の手順に従います。

グループポリシーオブジェクト (GPOsを使用して、Windows WorkSpaces または Windows ディレクトリの一部であるユーザーを管理するための設定を適用できます WorkSpaces 。 WorkSpaces コンピュータオブジェクトの組織単位と WorkSpaces ユーザーオブジェクトの組織単位を作成することをお勧めします。

Active Directory 管理ツールを使用して GPO を操作する方法の詳細については、AWS Directory Service 管理ガイドの Active Directory 管理ツールのインストールを参照してください。

WorkSpaces ログオンエージェントでユーザーを切り替えるには

ほとんどの場合、ユーザーが にログオンしようとすると WorkSpace、ユーザー名フィールドにそのユーザーの名前が事前に入力されます。ただし、管理者がメンテナンスタスクを実行する WorkSpace ために への RDP 接続を確立した場合、代わりにユーザー名フィールドに管理者の名前が入力されます。

この問題を回避するには、グループポリシー設定の [Hide entry points for Fast User Switching] を無効にします。この設定を無効にすると、 WorkSpaces ログオンエージェントはユーザーの切り替えボタンを使用してユーザー名フィールドに正しい名前を入力できます。

1. グループポリシー管理ツール (gpmc.msc) を開き、 に使用するディレクトリのドメインまたはドメインコントローラーレベルで GPO に移動して選択します WorkSpaces。 (ドメインに WorkSpaces グループポリシー管理テンプレートがインストールされている場合は、WorkSpaces マシンアカウントに WorkSpaces GPO を使用できます。)
2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Policies]、[Administrative Templates]、[System]、[Logon] の順に選択します。
4. [Hide entry points for Fast User Switching] 設定を開きます。
5. [Hide entry points for Fast User Switching] ダイアログボックスで、[無効]、[OK] の順に選択します。

最後にログオンしたユーザー名を非表示にするには

デフォルトでは、[Switch User] ボタンではなく、最後にログオンしたユーザーのリストが表示されます。の設定によっては WorkSpace、リストに他のユーザータイルが表示されない場合があります。このような状況が発生した場合、事前に入力されたユーザー名が正しくない場合、 WorkSpaces ログオンエージェントはフィールドに正しい名前を入力できません。

この問題を回避するには、セキュリティポリシー設定 [Interactive logon: Don't display last signed-in] または [Interactive logon: Do not display last user name] (使用している Windows のバージョンに応じて) を有効にします。

1. グループポリシー管理ツール (gpmc.msc) を開き、 に使用するディレクトリのドメインまたはドメインコントローラーレベルで GPO に移動して選択します WorkSpaces。 (ドメイ

ンに WorkSpaces グループポリシー管理テンプレートがインストールされている場合は、WorkSpaces マシンアカウントに WorkSpaces GPO を使用できます。)

2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. 次のいずれかの設定を開きます。
   - Windows 7 の場合 — Interactive logon: Don't display last signed-in
   - Windows 10 の場合 — Interactive logon: Do not display last user name
5. 該当する設定の [プロパティ] ダイアログボックスで、[有効]、[OK] の順に選択します。

ユーザーがログオンするために Ctrl+Alt+Del キーを押すようにするには

WorkSpaces ウェブアクセスでは、ユーザーがログオンする前に CTRL+ALT+DEL を押すように要求する必要があります。ユーザーがログオンする前に Ctrl+Alt+Del キーを押すように要求すると、ユーザーがパスワードを入力するときに信頼されたパスを使用できるようになります。

1. グループポリシー管理ツール (gpmc.msc) を開き、 に使用するディレクトリのドメインまたはドメインコントローラーレベルで GPO に移動して選択します WorkSpaces。 (ドメインに WorkSpaces グループポリシー管理テンプレートがインストールされている場合は、WorkSpaces マシンアカウントに WorkSpaces GPO を使用できます。)
2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. [Interactive logon: Do not require CTRL+ALT+DEL] 設定を開きます。
5. [Local Security Setting] タブで、[Disabled] を選択して [OK] を選択します。

セッションがロックされているときにドメインとユーザー情報を表示するには

WorkSpaces ログオンエージェントは、ユーザー名とドメインを検索します。この設定を構成すると、ロック画面にユーザーのフルネーム (Active Directory で指定されている場合)、ドメイン名、およびユーザー名が表示されます。

1. グループポリシー管理ツール (gpmc.msc) を開き、 に使用するディレクトリのドメインまたはドメインコントローラーレベルで GPO に移動して選択します WorkSpaces。 (ドメイ

ンに WorkSpaces グループポリシー管理テンプレートがインストールされている場合は、WorkSpaces マシンアカウントに WorkSpaces GPO を使用できます。)

2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. [Interactive logon: Display user information when the session is locked] 設定を開きます。
5. [Local Security Setting] タブで、[User display name, domain and user names] を選択し、[OK] を選択します。

グループポリシーとセキュリティポリシーの設定の変更を適用するには

グループポリシーとセキュリティポリシーの設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションの再開後に有効になります。前の手順でグループポリシーとセキュリティポリシーの変更を適用するには、次のいずれかの操作を行います。

- を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
- 管理コマンドプロンプトから、gpupdate /force と入力します。

FedRAMP 認証または DoD SRG 準拠のために Amazon WorkSpaces をセットアップする

Federal Risk and Authorization Management Program (FedRAMP) または Department of Defense(DoD)Cloud Computing Security Requirements Guide (SRG) に準拠するには、ディレクトリレベルで連邦情報処理標準 (FIPS) エンドポイント暗号化を使用するように Amazon WorkSpaces を設定する必要があります。また、FedRAMP 認証を持っているか、DoD SRG に準拠している米国の AWS リージョンを使用する必要があります。

FedRAMP 認証レベル (Moderate または High) あるいは DoD SRG 影響レベル (2、4、または 5) は、Amazon WorkSpaces が使用されている米国の AWS リージョンによって異なります。各リージョンに適用される FedRAMP 認証と DoD SRG コンプライアンスのレベルについては、AWSコンプライアンスプログラムによる対象範囲内の のサービスを参照してください。

> **Note**
>
> FIPS エンドポイント暗号化を使用するだけでなく、WorkSpaces を暗号化することもできます。詳細については、「暗号化済み WorkSpaces」を参照してください。

要件

- FedRAMP 認証を持っているか、DoD SRG に準拠している米国の AWS リージョンで WorkSpaces を作成する必要があります。
- WorkSpaces ディレクトリは、エンドポイント暗号化に FIPS 140-2 検証モードを使用するように設定する必要があります。

  > **Note**
  >
  > FIPS 140-2 検証モード 設定を使用するには、WorkSpaces ディレクトリが新規であるか、ディレクトリ内の既存のすべての WorkSpaces がエンドポイント暗号化に FIPS 140-2 検証モードを使用している必要があります。それ以外の場合は、この設定を使用することはできません。したがって、作成する WorkSpaces は FedRAMP または DoD のセキュリティ要件に準拠しません。

- ユーザーは、次のいずれかの WorkSpaces クライアントアプリケーションから WorkSpaces にアクセスする必要があります。
  - Windows 2.4.3 以降
  - macOS 2.4.3 以降
  - Linux: 3.0.0 以降
  - iOS 2.4.1 以降
  - Android: 2.4.1 以降
  - Fire タブレット: 2.4.1 以降
  - ChromeOS: 2.4.1 以降
  - Web Access

FIPS エンドポイント暗号化を使用するには

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

2. ナビゲーションペインで [Directories] を選択します。
3. FedRAMP 認証および DoD SRG 準拠の WorkSpaces を作成するディレクトリに、既存の WorkSpaces が関連付けられていないことを確認します。ディレクトリに関連付けられた WorkSpaces があり、そのディレクトリで FIPS 140-2 検証モードの使用がすでに有効になっていない場合は、WorkSpaces を終了するか、新しいディレクトリを作成します。
4. 上記の条件を満たすディレクトリを選択し、[アクション]、[Update Details (詳細の更新)] の順に選択します。
5. [Update Directory Details (ディレクトリ詳細の更新)] ページで、矢印を選択して [Access Control Options (アクセスコントロールのオプション)] セクションを展開します。
6. [Endpoint Encryption (エンドポイントの暗号化)] で、[TLS Encryption Mode (Standard) (TLS 暗号化モード (標準))] ではなく [FIPS 140-2 Validated Mode (FIPS 140-2 検証済みモード)] を選択します。
7. [Update and Exit] を選択します。
8. FedRAMP 認証済みで DoD SRG に準拠した WorkSpaces をこのディレクトリから作成できるようになりました。これらの WorkSpaces にアクセスするには、前述の「要件」セクションにリストされているいずれかの WorkSpaces クライアントアプリケーションを使用する必要があります。

Linux の SSH 接続を有効にする WorkSpaces

コマンドライン WorkSpaces を使用して Amazon Linux に接続する場合は、SSH 接続を有効にできます。ディレクトリ WorkSpaces 内のすべての またはディレクトリ WorkSpaces 内の個々の への SSH 接続を有効にできます。

SSH 接続を有効にするには、新しいセキュリティグループを作成するか、既存のセキュリティグループを更新して、この目的でインバウンドトラフィックを許可するルールを追加します。セキュリティグループは、関連付けられたインスタンスのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をインスタンスレベルでコントロールします。セキュリティグループを作成または更新すると、ユーザーや他のユーザーは PuTTY やその他のターミナルを使用して、デバイスから Amazon Linux に接続できます WorkSpaces。詳細については、「the section called “セキュリティグループ”」を参照してください。

動画チュートリアルについては、 AWS ナレッジセンターの「SSH WorkSpaces を使用して Linux Amazon に接続するにはどうすればよいですか？」を参照してください。

コンテンツ

- Amazon Linux への SSH 接続の前提条件 WorkSpaces
- ディレクトリ WorkSpaces 内のすべての Amazon Linux への SSH 接続を有効にする
- Amazon Linux 2 でのパスワードベースの認証 WorkSpaces
- 特定の Amazon Linux への SSH 接続を有効にする WorkSpace
- Linux または PuTTY WorkSpace を使用して Amazon Linux に接続する PuTTY

Amazon Linux への SSH 接続の前提条件 WorkSpaces

- へのインバウンド SSH トラフィックの有効化 WorkSpace — 1 つ以上の Amazon Linux へのインバウンド SSH トラフィックを許可するルールを追加するには WorkSpaces、 への SSH 接続を必要とするデバイスのパブリックまたはプライベート IP アドレスがあることを確認します WorkSpaces。例えば、Virtual Private Cloud (VPC) 外のデバイスのパブリック IP アドレスや、 と同じ VPC 内の別の EC2 インスタンスのプライベート IP アドレスを指定できます WorkSpace。

  WorkSpace ローカルデバイスから に接続する場合は、インターネットブラウザで「IP アドレスは何ですか」という検索フレーズを使用するか、次のサービスを使用できます: IP を確認する。
- への接続 WorkSpace — デバイスから Amazon Linux への SSH 接続を開始するには、次の情報が必要です WorkSpace。
  - 接続先の Active Directory ドメインの NetBIOS 名。
  - WorkSpace ユーザー名。
  - 接続 WorkSpace 先の のパブリックまたはプライベート IP アドレス。

    プライベート: VPC が企業ネットワークに接続されており、そのネットワークにアクセスできる場合は、 のプライベート IP アドレスを指定できます WorkSpace。

    パブリック: にパブリック IP アドレス WorkSpace がある場合は、次の手順で説明するように、WorkSpaces コンソールを使用してパブリック IP アドレスを検索できます。

接続 WorkSpace する Amazon Linux の IP アドレスとユーザー名を見つけるには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. のリストで WorkSpaces、SSH 接続 WorkSpace を有効にする を選択します。
4. 実行モード 列で、ステータスが WorkSpace Available であることを確認します。

5. WorkSpace 名前の左にある矢印をクリックしてインラインの概要を表示し、次の情報を書き留めます。

   - WorkSpace IP 。これは のプライベート IP アドレスです WorkSpace。

     プライベート IP アドレスは、 に関連付けられた Elastic Network Interface を取得するために必要です WorkSpace。ネットワークインターフェイスは、 に関連付けられたセキュリティグループやパブリック IP アドレスなどの情報を取得するために必要です WorkSpace。
   - WorkSpace ユーザー名 。これは、 に接続するために指定するユーザー名です WorkSpace。
6. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
7. ナビゲーションペインで、[ネットワークインターフェイス] を選択します。
8. 検索ボックスに、ステップ 5 で書き留めた WorkSpace IP を入力します。
9. WorkSpace IP に関連付けられているネットワークインターフェイスを選択します。
10. にパブリック IP アドレス WorkSpace がある場合、IPv4 パブリック IP 列に表示されます。このパブリック IP アドレスを書き留めます (該当する場合) 。

接続先の Active Directory ドメインの NetBIOS 名を見つけるには

1. https://console.aws.amazon.com/directoryservicev2/ で AWS Directory Service コンソールを開きます。
2. ディレクトリのリストで、 のディレクトリのディレクトリ ID リンクをクリックします WorkSpace。
3. [ディレクトリの詳細] セクションで、[ディレクトリの NetBIOS 名] を書き留めます。

ディレクトリ WorkSpaces 内のすべての Amazon Linux への SSH 接続を有効にする

ディレクトリ内のすべての Amazon Linux への SSH 接続を有効にする WorkSpaces には、次の手順を実行します。

WorkSpaces ディレクトリ内のすべての Amazon Linux へのインバウンド SSH トラフィックを許可するルールを使用してセキュリティグループを作成するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[Security Groups] を選択します。

3. [Create Security Group (セキュリティグループの作成)] を選択します。
4. 名前を入力します。また、オプションで説明およびセキュリティグループを入力します。
5. VPC で、SSH 接続 WorkSpaces を有効にする を含む VPC を選択します。
6. [インバウンド] タブで [ルールの追加] を選択し、以下の操作を行います。
   - [タイプ] で [SSH] を選択します。
   - [プロトコル] で [SSH] を選択すると、自動的に TCP が指定されます。
   - [ポート範囲] で [SSH] を選択すると、自動的に 22 に指定されます。
   - ソース で、ユーザーが への接続に使用するコンピュータのパブリック IP アドレスの CIDR 範囲を指定します WorkSpaces。例えば、企業ネットワークやホームネットワークなどです。
   - [説明] (オプション) に、ルールの説明を入力します。
7. [Create] を選択します。

Amazon Linux 2 でのパスワードベースの認証 WorkSpaces

2023 年 11 月 10 日より前に WorkSpaces リリースされた Amazon Linux 2 は、デフォルトで SSH パスワード認証が有効になっています。11 月 10 日以降 WorkSpaces にリリースされた Amazon Linux 2 の場合。2023 年、SSH パスワード認証はデフォルトで無効になっています。

既存の Amazon Linux 2 WorkSpaces インスタンスでパスワード認証を無効にするには

1. WorkSpaces クライアントを起動し、 にログインします WorkSpace。
2. ターミナルウィンドウを開きます (アプリケーション > システムツール > MATE ターミナル)。
3. ターミナルウィンドウで、次のコマンドを実行します。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

新しく作成された Amazon Linux 2 WorkSpaces インスタンスでパスワード認証を有効にするには

1. WorkSpaces クライアントを起動し、 にログインします WorkSpace。
2. ターミナルウィンドウを開きます (アプリケーション > システムツール > MATE ターミナル)。
3. ターミナルウィンドウで、次のコマンドを実行します。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

Ubuntu とは異なり WorkSpaces、Amazon Linux 2 WorkSpaces のデフォルトでは、カスタムイメージの SSH パスワード認証設定は保持されません。カスタムイメージから WorkSpaces プロビジョニングされた Amazon Linux 2 で SSH パスワード認証をデフォルトで有効にする場合は、パスワード認証を有効にするだけでなく、カスタムイメージの作成ssh_pwauth時に が含まれる行を削除するように /etc/cloud/cloud.cfg ファイルも変更する必要があります。/etc/cloud/cloud.cfg ファイルを変更するには、次のコマンドを実行します。

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

特定の Amazon Linux への SSH 接続を有効にする WorkSpace

特定の Amazon Linux への SSH 接続を有効にするには WorkSpace、次の手順を実行します。

既存のセキュリティグループにルールを追加して、特定の Amazon Linux へのインバウンド SSH トラフィックを許可するには WorkSpace

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインの [Network & Security] で、[ネットワークインターフェイス] を選択します。
3. 検索バー WorkSpace に、SSH 接続を有効にする のプライベート IP アドレスを入力します。
4. [セキュリティグループ] 列で、セキュリティグループのリンクをクリックします。
5. [インバウンド] タブで、[編集] を選択します。
6. [ルールの追加] を選択し、次の操作を行います。
   - [タイプ] で [SSH] を選択します。
   - [プロトコル] で [SSH] を選択すると、自動的に TCP が指定されます。
   - [ポート範囲] で [SSH] を選択すると、自動的に 22 に指定されます。
   - [Source] で、[マイ IP] または [カスタム] を選択し、単一の IP アドレスまたは IP アドレス範囲を CIDR 表記で指定します。例えば、IPv4 アドレスが 203.0.113.25 である場合、この単一の IPv4 アドレスを CIDR 表記で示すには 203.0.113.25/32 と指定します。会社が特定の範囲からアドレスを割り当てている場合、範囲全体 (203.0.113.0/24など) を指定します。
   - [説明] (オプション) に、ルールの説明を入力します。
7. [保存] を選択します。

Linux または PuTTY WorkSpace を使用して Amazon Linux に接続する PuTTY

セキュリティグループを作成または更新して必要なルールを追加した後、ユーザーや他のユーザーは Linux または PuTTY を使用して、デバイスから に接続できます WorkSpaces。

> **Note**
>
> 以下の手順のいずれかを完了する前に、以下の点について確認してください。
>
> - 接続先の Active Directory ドメインの NetBIOS 名。
> - への接続に使用するユーザー名 WorkSpace。
> - 接続 WorkSpace 先の のパブリックまたはプライベート IP アドレス。
>
> この情報を取得する方法については、このトピック WorkSpacesの前半の「Amazon Linux への SSH 接続の前提条件」を参照してください。

Linux WorkSpace を使用して Amazon Linux に接続するには

1. 管理者としてコマンドプロンプトを開き、次のコマンドを入力します。*NetBIOS #* 、*#####* 、および *WorkSpace IP* には、該当する値を入力します。

   ```
   ssh "NetBIOS_NAME\Username"@WorkSpaceIP
   ```

   以下は、SSH コマンドの例です。ここで、

   - *NetBIOS_NAME* は anycompany
   - *Username* は janedoe
   - *WorkSpace IP* は 203.0.113.25 です。

   ```
   ssh "anycompany\janedoe"@203.0.113.25
   ```

2. プロンプトが表示されたら、 WorkSpaces クライアントで認証するときに使用するものと同じパスワード (Active Directory パスワード) を入力します。

PuTTY WorkSpace を使用して Amazon Linux に接続するには

1. PuTTY を開きます。
2. [PuTTY 設定] ダイアログボックスで、次の操作を行います。

   - [ホスト名 (または IP アドレス)] には、次のコマンドを入力します。値を、接続先の Active Directory ドメインの NetBIOS 名、 への接続に使用するユーザー名 WorkSpace、および接続 WorkSpace 先の の IP アドレスに置き換えます。

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - [Port (ポート)] に「**22**」と入力します。
   - [接続タイプ] で、[SSH] を選択します。

   SSH コマンドの例については、前の手順のステップ 1 を参照してください。
3. [Open (開く)] を選択します。
4. プロンプトが表示されたら、 WorkSpaces クライアントで認証するときに使用するものと同じパスワード (Active Directory パスワード) を入力します。

に必要な設定とサービスコンポーネント WorkSpaces

WorkSpace 管理者として、必要な設定とサービスコンポーネントについて次のことを理解する必要があります。

- the section called “ルーティングテーブルの設定”
- the section called “Windows 用コンポーネント”
- the section called “Linux 用コンポーネント”
- the section called “Ubuntu 向けのコンポーネント”

必須のルーティングテーブルの設定

のオペレーティングシステムレベルのルーティングテーブルを変更しないことをお勧めします WorkSpace。この WorkSpaces サービスでは、システム状態をモニタリングし、システムコンポーネントを更新するために、このテーブルで事前設定されたルートが必要です。組織でルーティングテーブルの変更が必要な場合は、変更を適用する前に AWS サポートまたは AWS アカウントチームにお問い合わせください。

Windows 向けの必須のサービスコンポーネント

Windows では WorkSpaces、サービスコンポーネントは次の場所にインストールされます。これらのオブジェクトを削除、変更、ブロック、または隔離しないでください。これを行うと、WorkSpace は正しく機能しません。

にウイルス対策ソフトウェアがインストールされている場合は WorkSpace、次の場所にインストールされているサービスコンポーネントに干渉していないことを確認してください。

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

32 ビット PCoIP エージェント

2021 年 3 月 29 日より、PCoIP エージェントを 32 ビットから 64 ビットにアップデートしています。PCoIP プロトコルを使用している Windows の場合、これは Teradici ファイルの場所が から `C:\Program Files (x86)\Teradici`に変更 WorkSpaces されていることを意味します`C:\Program Files\Teradici`。定期的なメンテナンス期間中に PCoIP エージェントを更新したため、 の一部は移行中に他の よりも長く 32 ビットエージェントを使用した WorkSpaces 可能性があります。

ファイアウォールルール、ウイルス対策ソフトウェアの除外 (クライアント側とホスト側)、グループポリシーオブジェクト (GPO) の設定、または Microsoft システムセンター構成マネージャー (SCCM)、Microsoft エンドポイント構成マネージャーなどの構成管理ツールの設定を 32 ビットエージェントへのフルパスで行っていた場合は、64 ビットエージェントへのフルパスもこれらの設定に追加する必要があります。

ビットの PCoIP コンポーネントへのパスをフィルタリングする場合は、64 ビットバージョンのコンポーネントにパスを追加してください。すべての WorkSpaces が同時に更新されるわけではないため、32 ビットパスを 64 ビットパスに置き換えないでください。そうしないと、 の一部が機能しない WorkSpaces 可能性があります。たとえば、除外フィルターや通信フィルターを `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe` に置いている場合

は、C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe も追加する必要があります。同様に、除外フィルターや通信フィルターを C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe に置いている場合は、C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe も追加する必要があります。

PCoIP アービターサービスの変更 — 64 ビットエージェントを使用するように が更新されると、PCoIP アービターサービス (C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe) WorkSpaces が削除されることに注意してください。

PCoIP ゼロクライアントと USB デバイス — PCoIP エージェントのバージョン 20.10.4 以降、Amazon は Windows レジストリを介した USB リダイレクトをデフォルトで WorkSpaces 無効にします。このレジストリ設定は、ユーザーが PCoIP ゼロクライアントデバイスを使用して に接続している場合の USB 周辺機器の動作に影響します WorkSpaces。詳細については、「PCoIP ゼロクライアントで USB プリンタと他の USB 周辺機器が動作しない」を参照してください。

Linux 向けの必須のサービスコンポーネント

Amazon Linux では WorkSpaces、サービスコンポーネントは次の場所にインストールされます。これらのオブジェクトを削除、変更、ブロック、または隔離しないでください。これを行うと WorkSpace、 は正しく機能しません。

> **Note**
>
> 以外のファイルを変更すると、 /etc/pcoip-agent/pcoip-agent.confが機能 WorkSpaces しなくなり、再構築が必要になる場合があります。/etc/pcoip-agent/pcoip-agent.conf の変更の詳細については、Amazon Linux の管理 WorkSpaces を参照してください。

- /etc/dhcp/dhclient.conf
- /etc/logrotate.d/pcoip-agent
- /etc/logrotate.d/pcoip-server
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh

- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent

- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Ubuntu 向けの必須のサービスコンポーネント

Ubuntu では WorkSpaces、サービスコンポーネントは次の場所にインストールされます。これらのオブジェクトを削除、変更、ブロック、または隔離しないでください。これを行うと WorkSpace、は正しく機能しません。

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent

- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

WorkSpaces のディレクトリを管理する

WorkSpaces は、ディレクトリを使用して、WorkSpaces とユーザーの情報を格納し管理します。次のオプションの 1 つを使用できます。

- AD Connector - 既存のオンプレミス Microsoft Active Directory を使用します。ユーザーはオンプレミスの認証情報を使用して WorkSpaces にサインインし、自分の WorkSpaces からオンプレミスのリソースにアクセスできます。
- AWS Managed Microsoft AD — でホストされる Microsoft Active Directory を作成します。AWS
- Simple AD — Samba 4 を搭載し、 でホストされている Microsoft Active Directory と互換性のあるディレクトリを作成しますAWS
- 相互信頼 — AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を作成します。

これらのディレクトリをセットアップする方法を示すチュートリアルと WorkSpaces の起動の詳細については、「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

> **Tip**
>
> さまざまなデプロイシナリオにおけるディレクトリおよび仮想プライベートクラウド (VPC) の設計上の考慮事項の詳細については、「Amazon WorkSpaces のデプロイのベストプラクティス」を参照してください。

ディレクトリを作成したら、Active Directory 管理ツールなどのツールを使用して、ほとんどのディレクトリ管理タスクを実行します。グループポリシーを使用して WorkSpaces コンソールやその他のタスクを使用して、ディレクトリ管理タスクを実行できます。ユーザーとグループの管理の詳細については、WorkSpaces ユーザーの管理 および WorkSpaces の Active Directory 管理ツールを設定する を参照してください。

> **Note**
>
> - 現在、共有ディレクトリは、Amazon WorkSpaces での使用はサポートされていません。
> - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合は、プライマリリージョンのディレクトリのみを Amazon WorkSpaces で使用す

るために登録できます。Amazon WorkSpaces で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用についてサポートされていません。

- Simple AD および AD Connector は、WorkSpaces で無料で利用できます。Simple AD または AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。

  空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD または AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

目次

WorkSpaces でディレクトリを登録する

WorkSpaces で既存の AWS Directory Service ディレクトリを使用できるようにするには、そのディレクトリを WorkSpaces で登録する必要があります。ディレクトリを登録したら、そのディレクトリで WorkSpaces を起動できます。

要件

WorkSpaces で使用するディレクトリを登録するには、次の要件を満たす必要があります。

- AWS Managed Microsoft AD または Simple AD を使用している場合、ディレクトリを専用プライベートサブネットに配置できるのは、ディレクトリが WorkSpaces の配置先の VPC にアクセスできる場合に限ります。

ディレクトリと VPC 設計の詳細については、Amazon WorkSpaces のデプロイのベストプラクティスホワイトペーパーを参照してください。

> **Note**
>
> Simple AD および AD Connector は、WorkSpaces で無料で利用できます。Simple AD または AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> 空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD または AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

ディレクトリを登録するには

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択します。
4. [Actions]、[Register] の順に選択します。

   > **Note**
   >
   > - 現在、共有ディレクトリは、Amazon WorkSpaces での使用はサポートされていません。
   > - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリが設定されている場合は、プライマリリージョンのディレクトリのみを Amazon WorkSpaces で使用するために登録できます。Amazon WorkSpaces で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用についてサポートされていません。

5. 同じアベイラビリティーゾーンにない VPC の 2 つのサブネットを選択します。これらのサブネットは WorkSpaces の起動に使用されます。詳細については、「Amazon のアベイラビリティーゾーン WorkSpaces」を参照してください。

> **Note**
>
> 選択するサブネットがわからない場合は、[No Preference (指定なし)] を選択します。

6. [セルフサービスアクセス許可の有効化] で [はい] を選択し、WorkSpaces の再構築、ボリュームサイズ/コンピューティングタイプ/実行モードの変更をユーザーに許可します。これにより、Amazon WorkSpaces の料金に影響する場合があります。それ以外の場合は [いいえ] を選択します。
7. [Enable Amazon WorkDocs] (Amazon WorkDocs の有効化) で、[Yes] (はい) を選択して Amazon WorkDocs で使用するディレクトリを登録するか、それ以外の場合は [No] (いいえ) を選択します。

> **Note**
>
> このオプションは、リージョンで Amazon WorkDocs が使用可能であり、 を使用していない場合にのみ表示されますAWS Managed Microsoft AD AWS Managed Microsoft AD を使用している場合は、ディレクトリの登録を終了してから、「AWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする」を参照してください。

8. [Register] を選択します。[Registered] の最初の値が `REGISTERING` されます。登録が完了した後、値は `Yes` となります。

WorkSpaces でディレクトリの使用が終了したら、登録を解除できます。ディレクトリを削除する前に、ディレクトリの登録を解除する必要があります。ディレクトリの登録を解除して削除する場合は、まず、ディレクトリに登録されているすべてのアプリケーションとサービスを検索して削除する必要があります。詳細については、AWS Directory Service 管理ガイドのディレクトリの削除を参照してください。

ディレクトリの登録を解除するには

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択します。
4. [Actions]、[Deregister] の順に選択します。
5. 確認を求めるメッセージが表示されたら、[Deregister] を選択します。登録解除が完了すると、[Registered] の値は `No` になります。

のディレクトリの詳細を更新する WorkSpaces

WorkSpaces コンソールを使用して、次のディレクトリ管理タスクを完了できます。

タスク

- 組織単位を選択する
- 自動パブリック IP アドレスを設定する
- デバイスのアクセスコントロール
- ローカル管理者の許可を管理する
- AD Connector アカウント (AD Connector) を更新する
- 多要素認証 (AD Connector)

組織単位を選択する

WorkSpace マシンアカウントは、 WorkSpaces ディレクトリのデフォルトの組織単位 (OU) に配置されます。最初に、マシンアカウントは、ディレクトリのコンピュータ OU または AD Connector が接続されているディレクトリに配置されます。ディレクトリまたは接続されたディレクトリから別の OU を選択することも、別のターゲットドメインに OU を指定することもできます。ディレクトリにつき、1 つの OU しか選択できないことに注意してください。

新しい OU を選択すると、作成または再構築 WorkSpaces されたすべての のマシンアカウントが、新しく選択された OU に配置されます。

組織単位を選択するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリを選択します。
4. ターゲットドメインと組織単位で、編集を選択します。
5. OU を見つけるには、ターゲットと組織単位の下で、OU 名の全部または一部を入力し、使用する OU を選択します。
6. (オプション) OU の識別子名を選択して、選択した OU をカスタム OU で上書きします。
7. [保存] を選択します。
8. (オプション) 既存の を再構築 WorkSpaces して OU を更新します。詳細については、「の再構築 WorkSpace」を参照してください。

自動パブリック IP アドレスを設定する

パブリック IP アドレスの自動割り当てを有効にすると、起動 WorkSpace する各 には、Amazon が提供するパブリックアドレスのプールからパブリック IP アドレスが割り当てられます。パブリックサブネット WorkSpace の は、パブリック IP アドレスがある場合、インターネットゲートウェイを介してインターネットにアクセスできます。自動割り当てを有効にする前に既に存在 WorkSpaces していた は、ユーザーが再構築するまでパブリックアドレスを受信しません。

WorkSpaces がプライベートサブネットにあり、Virtual Private Cloud (VPC) に NAT ゲートウェイを設定している場合、または WorkSpaces がパブリックサブネットにあり、Elastic IP アドレスを割り当てている場合は、パブリックアドレスの自動割り当てを有効にする必要はありません。詳細については、「の VPC を設定する WorkSpaces」を参照してください。

> **Warning**
>
> 所有している Elastic IP アドレスを に関連付けた後 WorkSpace、その Elastic IP アドレスと の関連付けを解除すると WorkSpace、 はパブリック IP アドレスを WorkSpace 失い、Amazon が提供するプールから新しいアドレスを自動的に取得しません。Amazon が提供するプールからの新しいパブリック IP アドレスを に関連付けるには WorkSpace、 を再構築 WorkSpaceする必要があります。を再構築しない場合は WorkSpace、所有している別の Elastic IP アドレスを に関連付ける必要があります WorkSpace。

Elastic IP アドレスを設定するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. のディレクトリを選択します WorkSpaces。
4. [Actions]、[Update Details] を選択します。
5. [Access to Internet] を展開し、[Enable]または [Disable] を選択します。
6. [更新] を選択します。

デバイスのアクセスコントロール

にアクセスできるデバイスのタイプを指定できます WorkSpaces。さらに、信頼されたデバイス (マネージドデバイスとも呼ばれます) WorkSpaces へのアクセスを制限できます。

へのデバイスアクセスを制御するには WorkSpaces

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリを選択します。
4. アクセスコントロールオプションで、編集を選択します。
5. 「信頼できるデバイス WorkSpaces 」で、すべての を許可、信頼できるデバイス「」、またはすべての を拒否「」を選択して、アクセスできるデバイスタイプを指定します。詳細については、「信頼できるデバイス WorkSpaces へのアクセスを制限する」を参照してください
6. 保存を選択します。

ローカル管理者の許可を管理する

ユーザーが でローカル管理者であるかどうかを指定できます。これにより WorkSpaces、ユーザーはアプリケーションをインストールし、 で設定を変更できます WorkSpaces。デフォルトでは、ユーザーはローカル管理者に設定されます。この設定を変更すると、 WorkSpaces 作成したすべての新しい と、再構築 WorkSpaces した に変更が適用されます。

ローカル管理者の権限を変更するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリを選択します。
4. ローカル管理者設定で、編集を選択します。
5. ユーザーがローカル管理者であることを確認するには、ローカル管理者設定を有効にするを選択します。
6. [保存] を選択します。

AD Connector アカウント (AD Connector) を更新する

ユーザーとグループの読み取り、 WorkSpaces マシンアカウントの AD Connector ディレクトリへの結合に使用される AD Connector アカウントを更新できます。

AD Connector アカウントを更新するには

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

2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリを選択し、詳細の表示 を選択します。
4. AD コネクタアカウントで、編集を選択します。
5. 新しいアカウントのサインイン認証情報を入力します。
6. [保存] を選択します。

多要素認証 (AD Connector)

AD Connector ディレクトリで多要素認証 (MFA) を有効にすることができます。AWS Directory Service での多要素認証の使用の詳細については、AD Connector の多要素認証を有効にするおよびAD Connector の前提条件を参照してください。

> **Note**
>
> - RADIUS サーバーは AWS でホストすることも、オンプレミスでホストすることもできます。
> - ユーザー名は、Active Directory と RADIUS サーバー間で一致する必要があります。

多要素認証を有効にするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Multi-Factor Authentication] を展開し、[Enable Multi-Factor Authentication] を選択します。
5. [RADIUS server IP address(es)] に、カンマで区切られた RADIUS サーバーのエンドポイントの IP アドレスを入力するか、RADIUSサーバーのロードバランサーの IP アドレスを入力します。
6. [Port] に、RADIUS サーバーが通信で使用しているポートを入力します。オンプレミスネットワークでは、AD Connector からのデフォルトの RADIUS サーバーポート (UDP:1812) を介した受信トラフィックが許可されている必要があります。
7. [Shared secret code] と [Confirm shared secret code] に、RADIUS サーバーの共有シークレットコードを入力します。
8. [Protocol] で、RADIUS サーバープロトコルを選択します。

9. [Server timeout] に、RADIUS サーバーの応答を待つ時間を秒単位で入力します。この値は 1 ~ 50 の範囲の値にする必要があります。
10. [Max retries] に、RADIUS サーバーとの通信を試行する回数を入力します。この値は 0 ~ 10 の範囲の値にする必要があります。
11. [Update and Exit] を選択します。

多要素認証は、[RADIUS Status] が [Enabled] になると使用できます。多要素認証の設定中、ユーザーは にログインできません WorkSpaces。

Amazon WorkSpaces の DNS サーバーの更新

WorkSpaces の起動後に Active Directory の DNS サーバーの IP アドレスを更新する必要がある場合は、新しい DNS サーバー設定で WorkSpaces を更新する必要があります。

以下のいずれかの方法で、新しい DNS 設定で WorkSpaces を更新できます。

- Active Directory の DNS 設定を更新する前に、WorkSpaces の DNS 設定を更新します。
- Active Directory の DNS 設定を更新した後、WorkSpaces を再構築します。

Active Directory の DNS 設定を更新する前に、WorkSpaces の DNS 設定を更新することをお勧めします (以下の手順のステップ 1 で説明しています)。

代わりに WorkSpaces を再構築する場合は、Active Directory の DNS サーバーの IP アドレスのいずれかを更新し (ステップ 2)、の再構築 WorkSpace の手順に従って WorkSpaces を再構築します。WorkSpaces を再構築したら、ステップ 3 の手順に従って DNS サーバーの更新をテストします。このステップを完了したら、Active Directory の 2 番目の DNS サーバーの IP アドレスを更新し、WorkSpaces を再構築します。ステップ 3 の手順に従って、2 番目の DNS サーバーの更新をテストしてください。「ベストプラクティス」セクションで説明したように、DNS サーバーの IP アドレスを一度に 1 つずつ更新することをお勧めします。

ベストプラクティス

DNS サーバーの設定を更新するときは、次のベストプラクティスをお勧めします。

- ドメインリソースの切断やアクセス不能を避けるために、オフピーク時間または計画されたメンテナンス期間中に DNS サーバーの更新を実行することを強くお勧めします。

- DNS サーバー設定の変更前の 15 分間、および 15 分間、新しい WorkSpaces を起動しないでください。
- DNS サーバー設定を更新するときは、一度に 1 つの DNS サーバーの IP アドレスを変更します。2 番目の IP アドレスを更新する前に、最初の更新が正しいことを確認します。IP アドレスを 1 つずつ更新するには、次の手順 (ステップ 1、ステップ 2、ステップ 3) を 2 回実行することをお勧めします。

ステップ 1: WorkSpaces の DNS サーバー設定を更新する

次の手順では、現在および新しい DNS サーバーの IP アドレス値を次のように参照します。

- 現在の DNS IP アドレス: *OldIP1*, *OldIP2*
- 新しい DNS IP アドレス: *NewIP1*、*NewIP2*

> **Note**
>
> この手順を 2 回目に実行する場合は、*OldIP1*を *OldIP2* に、*NewIP1* を *NewIP2* に置き換えます。

Windows WorkSpaces の DNS サーバー設定を更新する

複数の WorkSpaces がある場合は、WorkSpaces の Active Directory OU にグループポリシーオブジェクト (GPO) を適用することで、次のレジストリ更新を WorkSpaces にデプロイできます。GPO を操作する方法については、Windows の管理 WorkSpaces を参照してください。

これらの更新プログラムは、レジストリエディタまたは Windows PowerShell を使用して行うことができます。どちらの手順も、このセクションで説明しています。

レジストリエディタを使用して DNS レジストリ設定を更新するには

1. Windows WorkSpace で、Windows 検索ボックスを開き、**`registry editor`** と入力してレジストリエディタ (regedit.exe) を開きます。
2. 「このアプリがデバイスに変更を加えることを許可しますか?」と尋ねられたら、[はい] を選択します。
3. レジストリエディターで、次のレジストリエントリに移動します。

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight

4. [DomainJoinDns] レジストリキーを開きます。*OldIP1* で *NewIP1* を更新し、[OK] を選択します。
5. レジストリエディタを閉じます。
6. WorkSpace を再起動するか、SkyLightWorkspaceConfigService サービスを再起動します。

> **Note**
>
> SkyLightWorkspaceConfigService サービスを再起動した後、ネットワークアダプタが変更を反映するまでに最長 1 分かかる場合があります。

7. ステップ 2 に進み、Active Directory の DNS サーバー設定を更新して *OldIP1* を *NewIP1* に置き換えます。

PowerShell を使用して DNS レジストリ設定を更新するには

次の手順では、PowerShell コマンドを使用してレジストリを更新し、SkyLightWorkspaceConfigService サービスを再起動します。

1. Windows WorkSpace で、Windows 検索ボックスを開き、**powershell** と入力します。[管理者として実行] を選択します。
2. 「このアプリがデバイスに変更を加えることを許可しますか?」と尋ねられたら、[はい] を選択します。
3. PowerShell ウィンドウで、次のコマンドを実行して、現在の DNS サーバーの IP アドレスを取得します。

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

次のような出力が表示されます。

```
DomainJoinDns : OldIP1,OldIP2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon\SkyLight
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon
PSChildName   : SkyLight
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. PowerShell ウィンドウで、次のコマンドを実行して *OldIP1* を *NewIP1* に変更します。今のところ、*OldIP2* はそのままにしてください。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. 次のコマンドを実行して、SkyLightWorkspaceConfigService サービスを再起動します。

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> SkyLightWorkspaceConfigService サービスを再起動した後、ネットワークアダプタが変更を反映するまでに最長 1 分かかる場合があります。

6. ステップ 2 に進み、Active Directory の DNS サーバー設定を更新して *OldIP1* を *NewIP1* に置き換えます。

Linux WorkSpaces の DNS サーバー設定を更新する

Linux WorkSpace が複数ある場合は、設定管理ソリューションを使用してポリシーを配布し、適用することをお勧めします。例えば、AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise、または Ansible を使用できます。

Linux WorkSpace で DNS サーバー設定を更新するには

1. Linux WorkSpace で、ターミナルウィンドウを開きます ([アプリケーション] > [システムツール] > [MATE ターミナル])。
2. 次の Linux コマンドを使用して、/etc/dhcp/dhclient.conf ファイルを編集します。このファイルを編集するには、root ユーザー権限が必要です。sudo -i コマンドを使用して root になるか、次に示すように sudo を使用してすべてのコマンドを実行します。

```
sudo vi /etc/dhcp/dhclient.conf
```

この /etc/dhcp/dhclient.conf ファイルには、次の prepend コマンドが表示されます。ここで、*OldIP1* と *OldIP2* は DNS サーバーの IP アドレスです。

```
prepend domain-name-servers OldIP1, OldIP2; # skylight
```

3. *OldIP1* を *NewIP1* に置き換えて、今のところ *OldIP2* はそのままにします。
4. 変更を `/etc/dhcp/dhclient.conf` に保存します。
5. WorkSpace を再起動します。
6. ステップ 2 に進み、Active Directory の DNS サーバー設定を更新して *OldIP1* を *NewIP1* に置き換えます。

ステップ 2: Active Directory の DNS サーバー設定を更新する

このステップでは、Active Directory の DNS サーバー設定を更新します。「ベストプラクティス」セクションで説明したように、DNS サーバーの IP アドレスを一度に 1 つずつ更新することをお勧めします。

Active Directory の DNS サーバー設定を更新するには、 AWS Directory Service 管理ガイドの次のドキュメントを参照してください。

- AD Connector: AD Connector の DNS アドレスを更新する
- AWS マネージド Microsoft AD: オンプレミスドメインの DNS 条件付きフォワーダーを設定する
- Simple AD: DNS を設定する

DNS サーバーの設定を更新したら、ステップ 3 に進みます。

ステップ 3: 更新された DNS サーバー設定をテストする

ステップ 1 と ステップ 2, を完了した後、次の手順を使用して、更新された DNS サーバー設定が期待どおりに機能していることを確認します。

次の手順では、現在および新しい DNS サーバーの IP アドレス値を次のように参照します。

- 現在の DNS IP アドレス: *OldIP1*, *OldIP2*
- 新しい DNS IP アドレス: *NewIP1*、*NewIP2*

> **Note**
>
> この手順を 2 回目に実行する場合は、*OldIP1*を *OldIP2* に、*NewIP1* を *NewIP2* に置き換えます。

Windows WorkSpaces 用の更新された DNS サーバー設定をテストする

1. *OldIP1* DNS サーバーをシャットダウンします。
2. Windows WorkSpace にログインします。
3. Windows の [スタート] メニューで [Windows システム] を選択し、[コマンドプロンプト] を選択します。
4. 次のコマンドを実行します。*AD_Name* は、Active Directory の名前 (corp.example.com など) です。

   ```
   nslookup AD_Name
   ```

   nslookup コマンドは次の情報を返します。(この手順を 2 回目に実行する場合は、*NewIP2* の代わりに *OldIP2* を参照してください)。

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. 出力が期待したものではない場合、またはエラーが表示された場合は、ステップ 1 を繰り返します。
6. 1 時間待ってから、ユーザーの問題が報告されていないことを確認します。*NewIP1* が DNS クエリを取得し、応答していることを確認します。
7. 最初の DNS サーバーが正常に動作していることを確認したら、ステップ 1 を繰り返して 2 番目の DNS サーバーを更新します。今回は *OldIP2* を *NewIP2* に置き換えます。次に、ステップ 2 とステップ 3 を繰り返します。

Linux WorkSpaces 用の更新された DNS サーバー設定をテストする

1. *OldIP1* DNS サーバーをシャットダウンします。
2. Linux WorkSpace にログインします。
3. Linux WorkSpace で、ターミナルウィンドウを開きます ([アプリケーション] > [システムツール] > [MATE ターミナル])。

4. DHCP 応答で返された DNS サーバーの IP アドレスは、WorkSpace 上のローカル /etc/resolv.conf ファイルに書き込まれます。/etc/resolv.conf ファイルのコンテンツを表示するには、次のコマンドを実行します。

```
cat /etc/resolv.conf
```

次のような出力が表示されます。(この手順を 2 回目に実行する場合は、*NewIP2* の代わりに *OldIP2* を参照してください)。

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> /etc/resolv.conf ファイルを手動で変更した場合、WorkSpace を再起動すると、これらの変更は失われます。

5. 出力が期待したものではない場合、またはエラーが表示された場合は、ステップ 1 を繰り返します。
6. 実際の DNS サーバーの IP アドレスは /etc/dhcp/dhclient.conf ファイルに保存されます。このファイルの内容を表示するには、次のコマンドを実行します。

```
sudo cat /etc/dhcp/dhclient.conf
```

次のような出力が表示されます。(この手順を 2 回目に実行する場合は、*NewIP2* の代わりに *OldIP2* を参照してください)。

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. 1 時間待ってから、ユーザーの問題が報告されていないことを確認します。*NewIP1* が DNS クエリを取得し、応答していることを確認します。
8. 最初の DNS サーバーが正常に動作していることを確認したら、ステップ 1 を繰り返して 2 番目の DNS サーバーを更新します。今回は *OldIP2* を *NewIP2* に置き換えます。次に、ステップ 2 とステップ 3 を繰り返します。

WorkSpaces のディレクトリの削除

Amazon WorkDocs、Amazon WorkMail、または Amazon Chime のような他の WorkSpaces やアプリケーションで WorkSpaces が使用されていない場合は、そのディレクトリを削除できます。ディレクトリを削除する前に、ディレクトリの登録を解除する必要があります。

> **Note**
>
> Simple AD および AD Connector は、WorkSpaces で無料で利用できます。Simple AD または AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> Simple AD または AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

ディレクトリを削除した場合

Simple AD または AWS Directory Service for Microsoft Active Directory ディレクトリを削除すると、ディレクトリデータおよびスナップショットはすべて削除され、復元することはできません。ディレクトリが削除されても、ディレクトリに結合されている Amazon EC2 インスタンスはすべてそのまま残ります。ただし、ディレクトリの認証情報を使用して、このインスタンスにログインすることはできません。これらのインスタンスにログインするには、インスタンス専用の AWS アカウントを使用する必要があります。

AD Connector ディレクトリが削除されても、オンプレミスのディレクトリはそのまま残ります。ディレクトリに結合されている Amazon EC2 インスタンスもすべてそのまま残り、オンプレミスのディレクトリに結合された状態のまま変わりません。引き続き、ディレクトリの認証情報を使用して、このインスタンスにログインできます。

ディレクトリを削除するには

1. ディレクトリ内のすべての WorkSpaces を削除します。詳細については、「WorkSpace の削除」を参照してください。
2. ディレクトリに登録されているすべてのアプリケーションとサービスを見つけて削除します。詳細については、AWS Directory Service 管理ガイドのディレクトリの削除を参照してください。
3. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
4. ナビゲーションペインで [Directories] を選択します。
5. ディレクトリを選択し、[Actions]、[Deregister] の順に選択します。
6. 確認を求めるメッセージが表示されたら、[Deregister] を選択します。
7. ディレクトリをもう一度選択し、[Actions]、[Delete] の順に選択します。
8. 確認を求めるメッセージが表示されたら、[Delete] を選択します。

> **Note**
>
> アプリケーション割り当ての削除には、予想以上に時間がかかる場合があります。次のエラーメッセージが表示された場合は、すべてのアプリケーションの割り当てを削除したことを確認し、30～60 分待ってから、ディレクトリの削除を再試行します。
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (オプション) ディレクトリの Virtual Private Cloud (VPC) のすべてのリソースを削除した後で、VPC を削除し、NAT ゲートウェイで使用されている Elastic IP アドレスを解放できます。詳細については、Amazon VPC ユーザーガイドの VPC の削除および Elastic IP アドレスの使用を参照してください。
10. （オプション）不要になったカスタムバンドルとイメージを削除するには、、「WorkSpaces カスタムバンドルまたはイメージを削除する」を参照してください。

AWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする

Amazon WorkSpaces で AWS Managed Microsoft AD を使用している場合は、Amazon WorkDocs コンソールまたは AWS Directory Service コンソールを使用して、ディレクトリの Amazon WorkDocs を有効にすることができます。

> **Note**
>
> Amazon WorkDocs は、Amazon WorkSpaces が利用可能な AWS リージョンの一部ではご利用いただけません。詳細については、Amazon WorkDocs の料金を参照してください。

Amazon WorkDocs コンソールで WorkDocs を有効にするには

1. Amazon WorkDocs コンソール (https://console.aws.amazon.com/zocalo/) を開きます。
2. [Create a New WorkDocs Site] を選択します。
3. [Standard Setup (標準セットアップ)] で、[Launch (起動)] を選択します。
4. ディレクトリを選択し、サイト名を作成します。
5. WorkDocs サイトを管理するユーザーを指定します。管理者、またはディレクトリに作成された任意のユーザーを使用できます。

詳細については、Amazon WorkDocs 管理ガイドの AWS Managed Microsoft AD の開始方法を参照してください。

AWS Directory Service コンソールから WorkDocs を有効にするには

1. https://console.aws.amazon.com/directoryservicev2/ で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. [ディレクトリ] ページで、ディレクトリを選択します。
4. [ディレクトリの詳細] ページで、[アプリケーション管理] タブを選択します。
5. [Application access URL (アプリケーションのアクセス URL)] セクションで、ディレクトリにアクセス URL が割り当てられていない場合は、[Create (作成)] ボタンが表示されます。ディレクトリのエイリアスを入力し、[Create (作成)] を選択します。詳細については、AWS Directory Service 管理ガイドのアクセス URL の作成を参照してください。

6. [Application access URL (アプリケーションのアクセス URL)] セクションで、[有効化] を選択して Amazon WorkDocs のシングルサインオンを有効にします。詳細については、AWS Directory Service 管理ガイドの Single Sign-On を参照してください。

WorkSpaces の Active Directory 管理ツールを設定する

WorkSpaces ディレクトリのほとんどの管理タスクは、Active Directory 管理ツールなどのディレクトリ管理ツールを使用して実行します。ただし、ディレクトリ関連のタスクの一部は WorkSpaces コンソールを使用して実行します。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。

5 つ以上の WorkSpaces を含む AWS Managed Microsoft AD または Simple AD でディレクトリを作成する場合は、Amazon EC2 インスタンスに管理を集中化することをお勧めします。ディレクトリ管理ツールは WorkSpace にインストールすることができますが、Amazon EC2 インスタンスを使用する方がより堅実なソリューションとなります。

Active Directory 管理ツールを設定するには

1. Amazon EC2 Windows インスタンスを起動し、次のいずれかのオプションを使用して WorkSpaces ディレクトリに結合します。
   - 既存の Amazon EC2 Windows インスタンスがない場合は、インスタンスの起動時に、そのインスタンスをディレクトリドメインに結合できます。詳細については、AWS Directory Service 管理ガイドの Windows EC2 インスタンスにシームレスに参加するを参照してください。
   - 既存の Amazon EC2 Windows インスタンスがある場合は、手動でディレクトリに結合できます。詳細については、AWS Directory Service 管理ガイドの Windows インスタンスを手動で追加するを参照してください。
2. Amazon EC2 Windows インスタンスに Active Directory 管理ツールをインストールします。詳細については、AWS Directory Service 管理ガイドの Active Directory 管理ツールのインストールを参照してください。

> **Note**
>
> Active Directory 管理ツールをインストールするときは、[グループポリシーの管理] も選択して、グループポリシー管理エディター (gpmc.msc) ツールをインストールします。

機能のインストールが完了すると、Windows 管理ツールの Windows [スタート] メニューから、Active Directory ツールが使用できるようになります。

3. ディレクトリ管理者として、ツールを次のように実行します。

   a. Windows の [スタート] メニューで、[Windows 管理ツール] を開きます。
   b. Shift キーを押しながら、使用するツールへのショートカットを右クリックし、[別のユーザーとして実行] を選択します。
   c. 管理者のサインイン認証情報を入力します。Simple AD の場合、ユーザー名は **`Administrator`** で、AWS Managed Microsoft AD の場合、管理者は **`Admin`** です。

使い慣れた Active Directory ツールを使用して、ディレクトリ管理タスクを実行できるようになりました。たとえば、Active Directory ユーザーとコンピュータツールを使用して、ユーザーの追加、ユーザーの削除、ディレクトリ管理者へのユーザーの昇格、またはユーザーパスワードのリセットを行うことができます。ディレクトリ内のユーザーを管理する権限を持つユーザーとして、Windows インスタンスにログインする必要があります。

ユーザーをディレクトリ管理者に昇格するには

> **Note**
>
> この手順は、Simple AD で作成されたディレクトリにのみ適用され、AWS Managed AD では適用されません。AWS Managed AD で作成されたディレクトリについては、AWS Directory Service 管理ガイドのAWSManaged Microsoft ADのユーザーとグループを管理するを参照してください。

1. [Active Directory ユーザーとコンピュータ] ツールを開きます。
2. ドメインの下の Users フォルダに移動し、昇格するユーザーを選択します。
3. [Action]、[Properties] の順に選択します。
4. *#####*プロパティのダイアログボックスで、[メンバーとして追加] をクリックします。
5. ユーザーを以下のグループに追加し、[OK] を選択します。

   - Administrators
   - Domain Admins
   - Enterprise Admins

- Group Policy Creator Owners
- Schema Admins

ユーザーを追加または削除するには

Amazon WorkSpaces コンソールから新しいユーザーを作成できるのは、WorkSpace の起動プロセス中のみです。Amazon WorkSpaces コンソールからユーザーを削除することはできません。ユーザーグループの管理など、ほとんどのユーザー管理タスクは、ディレクトリで実行する必要があります。

> **Important**
>
> ユーザーを削除する前に、ユーザーに割り当てられた WorkSpace を削除する必要があります。詳細については、「WorkSpace の削除」を参照してください

ユーザーとグループの管理に使用するプロセスは、使用しているディレクトリの種類によって異なります。

- AWS Managed Microsoft AD を使用している場合は、AWS Directory Service 管理ガイドの AWS Managed Microsoft AD のユーザーとグループの管理を参照してください。
- Simple AD を使用している場合は、AWS Directory Service 管理ガイドのSimple AD でユーザーとグループを管理するを参照してください。
- AD Connector または信頼関係を使用して Microsoft Active Directory を使用する場合は、Active Directory モジュールを使用してユーザーとグループを管理できます。

ユーザーのパスワードをリセットするには

既存のユーザーのパスワードをリセットするときは、[User must change password at next logon] を設定しないでください。設定してしまうと、ユーザーは WorkSpace に接続できません。代わりに、安全な一時パスワードをユーザーに割り当てて、ユーザーが次回ログオンしたときに WorkSpace 内から手動でパスワードを変更するように依頼します。

> **Note**
>
> AD Connector を使用している場合、またはユーザーが AWSGovCloud (米国西部) リージョンにいる場合、ユーザーは自分のパスワードをリセットできません。([パスワードを忘れた

場合] オプションは、WorkSpaces クライアントアプリケーションのログイン画面では使用できません。)

WorkSpaces を使用して仮想デスクトップを起動します。

WorkSpaces を使用すると、WorkSpaces として知られている、ユーザー向けの仮想クラウドベースの Microsoft Windows、Amazon Linux、Ubuntu Linux デスクトップを提供できます。

> **Note**
>
> Amazon WorkSpaces コンソールに表示される WorkSpace の [Computer Name] (コンピュータ名) の値は、起動した WorkSpace の種類 (Amazon Linux、Ubuntu、Windows) によって異なります。WorkSpace のコンピュータ名には、次のいずれかの形式を使用できます。
>
> - Amazon Linux: A-*xxxxxxxxxxxxx*
> - Ubuntu: U-*xxxxxxxxxxxxx*
> - Windows: IP-C*xxxxxx* または WSAMZN-*xxxxxxx* または EC2AMAZ-*xxxxxxx*
>
> Windows WorkSpaces の場合、コンピュータ名の形式はバンドルの種類によって決定されます。パブリックバンドルから作成された WorkSpaces の場合、またはパブリックイメージに基づいてカスタムバンドルから作成された WorkSpaces の場合は、パブリックイメージが作成された時点までに決定されます。
> 2020 年 6 月 22 日以降、パブリックバンドルから起動された Windows WorkSpaces では、IP-C*xxxxxx* 形式ではなく、コンピュータ名に WSAMZN-*xxxxxxx* 形式が使用されます。
> パブリックイメージに基づくカスタムバンドルでは、パブリックイメージが 2020 年 6 月 22 日より前に作成された場合、コンピュータ名は EC2AMAZ-*xxxxxxx* 形式になります。パブリックイメージが 2020 年 6 月 22 日以降に作成された場合、コンピュータ名は WSAMZN-*xxxxxxx* 形式になります。
> Bring-Your-Own-License (BYOL) バンドルでは、デフォルトでコンピュータ名に DESKTOP-*xxxxxxx* または EC2AMAZ-*xxxxxxx* のいずれかの形式が使用されます。
> カスタムバンドルまたは BYOL バンドル内のコンピュータ名にカスタム形式を指定した場合、カスタム形式はこれらの既定値を上書きします。カスタム形式を指定するには、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。
> 重要 — Windows のシステム設定で WorkSpace のコンピュータ名を変更すると、WorkSpace にアクセスできなくなります。

WorkSpaces は、ディレクトリを使用して、WorkSpace とユーザーの情報を格納し管理します。以下のいずれかを実行できます。

- Simple AD ディレクトリを作成します。
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD ともいいます) を作成します。
- Active Directory Connector を使用して、既存の Active Directory に接続します。
- AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を作成します。

> **Note**
>
> - 現在、共有ディレクトリは、Amazon WorkSpaces での使用はサポートされていません。
> - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合は、プライマリリージョンのディレクトリのみを Amazon WorkSpaces で使用するために登録できます。Amazon WorkSpaces で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用についてサポートされていません。
> - Simple AD および AD Connector は、WorkSpaces で無料で利用できます。Simple AD または AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
>
>   空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD または AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

以下のチュートリアルでは、サポートされているディレクトリサービスオプションを使用して WorkSpace を起動する方法を説明します。

チュートリアル

- AWS Managed Microsoft AD を使用して WorkSpace を起動する
- Simple AD を使用して WorkSpace を起動する
- AD Connector を使用して WorkSpace を起動する

- 信頼できるドメインを使用して WorkSpace を起動する

AWS Managed Microsoft AD を使用して WorkSpace を起動する

WorkSpaces を使用すると、WorkSpaces として知られている、ユーザー向けの仮想クラウドベースの Windows および Linux デスクトップを提供できます。

WorkSpaces は、ディレクトリを使用して、WorkSpace とユーザーの情報を格納し管理します。ディレクトリには、Simple AD、AD Connector、または Microsoft Active Directory 用の AWS Directory Service (AWS Managed Microsoft AD とも呼ばれます) のいずれかを選択できます。さらに、AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を確立することもできます。

このチュートリアルでは、AWS Managed Microsoft AD を使用する WorkSpace を起動します。他のオプションを使用するチュートリアルについては、「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

タスク

- 開始する前に
- ステップ 1: AWS Managed Microsoft AD ディレクトリを作成する
- ステップ 2: WorkSpace の作成
- ステップ 3: WorkSpace に接続する
- 次のステップ

開始する前に

- WorkSpaces はすべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、WorkSpaces のリージョンを選択します。サポートされるリージョンについては、AWS リージョン別の WorkSpaces の料金を参照してください。
- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。バンドルは、オペレーティングシステム、ストレージ、コンピューティング、およびソフトウェアリソースの組み合わせです。詳細については、「Amazon WorkSpace バンドル」を参照してください。
- AWS Directory Service を使用してディレクトリを作成する場合、または WorkSpace を起動する場合は、パブリックサブネットと 2 つのプライベートサブネットで構成された仮想プライベートクラウドを作成または選択する必要があります。詳細については、「の VPC を設定する WorkSpaces」を参照してください。

ステップ 1: AWS Managed Microsoft AD ディレクトリを作成する

まず、AWS Managed Microsoft AD ディレクトリを作成します。AWS Directory Service は、VPC のプライベートサブネットにそれぞれ 2 つのディレクトリサーバーを作成します。最初はディレクトリにユーザーがいないことに注意してください。WorkSpace を起動したら、次のステップでユーザーを追加します。

> **Note**
>
> - 現在、共有ディレクトリは、Amazon WorkSpaces での使用はサポートされていません。
> - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリが設定されている場合は、プライマリリージョンのディレクトリのみを Amazon WorkSpaces で使用するために登録できます。Amazon WorkSpaces で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用についてサポートされていません。

AWS Managed Microsoft AD ディレクトリを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. [Set up Directory]、[Create Microsoft AD] の順にクリックします。
4. 以下のようにディレクトリを設定します。

   a. [Organization name] には、ディレクトリの一意の組織名 (例: my-demo-directory) を入力します。この名前は、長さが 4 文字以上で、英数字とハイフン (-) のみで構成され、ハイフン以外の文字で開始または終了している必要があります。

   b. [Directory DNS] には、ディレクトリの完全修飾名を入力します (例: workspaces.demo.com)。

   > **Important**
   >
   > WorkSpaces の起動後に DNS サーバーを更新する必要がある場合は、Amazon WorkSpaces の DNS サーバーの更新 の手順に従って WorkSpaces が正しく更新されていることを確認します。

c. [NetBIOS name] には、ディレクトリの短縮名を入力します (例: workspaces) 。

d. [Admin password] と [Confirm Password] に、ディレクトリ管理者アカウントのパスワードを入力します。パスワードの要件に関する詳細については、AWS Directory Service 管理ガイドの AWS Managed Microsoft AD ディレクトリを作成するを参照してください。

e. (オプション) [Description] に、ディレクトリの説明を入力します。

f. [VPC] では、作成した VPC を選択します。

g. [Subnets] で、2 つのプライベートサブネットを選択します (CIDR ブロック `10.0.1.0/24` および `10.0.2.0/24`) 。

h. [Next Step] を選択します。

5. [Create Microsoft AD] を選択します。

6. [Done] を選択します。ディレクトリの最初のステータスは `Creating` です。ディレクトリの作成が完了すると、ステータスが `Active` に変わります。

ステップ 2: WorkSpace の作成

AWS Managed Microsoft AD ディレクトリを作成し、WorkSpace を作成する準備が整いました。

WorkSpace を作成するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. [Launch WorkSpaces] を選択します。
4. [Select a Directory] (ディレクトリの選択) ページで、作成したディレクトリを選択し、[Next Step] (次のステップ) を選択します。WorkSpaces がディレクトリを登録します。
5. [Identify Users] ページで、次のようにディレクトリに新しいユーザーを追加します。

   a. [Username]、[First Name]、[Last Name]、および [Email] に値を入力します。アクセス権のある E メールアドレスを使用してください。

   b. [Create Users] を選択します。

   c. [Next Step] を選択します。

6. [Select Bundle] ページで、バンドル;を選択し、[Next Step] を選択します。

> **Note**
>
> 各バンドルの推奨用途と仕様を確認して、ユーザーに最適なバンドルを選択できるようにしてください。各ユースケースの詳細については、「Amazon WorkSpaces バンドル」を参照してください。バンドルの仕様、推奨用途、および料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

7. [WorkSpaces Configuration] ページで、実行モードを選択してから、[Next Step] を選択します。
8. [Review & Launch WorkSpaces] ページで、[Launch WorkSpaces] を選択します。WorkSpace の最初のステータスは `PENDING` です。起動が完了すると、ステータスは `AVAILABLE` になり、ユーザーに指定した E メールアドレスに招待状が送信されます。

> **Note**
>
> ユーザーが既に Active Directory に存在する場合、招待メールは送信されません。代わりに、ユーザーに招待メールを手動で送信してください。詳細については、「招待 E メールの送信」を参照してください

9. (オプション) リージョンで Amazon WorkDocs がサポートされている場合は、ディレクトリ内のすべてのユーザーのために Amazon WorkDocs を有効にできます。詳細については、「AWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする」を参照してください Amazon WorkDocs の詳細については、Amazon WorkDocs 管理ガイドの Amazon WorkDocs Drive を参照してください。

ステップ 3: WorkSpace に接続する

招待メールを受け取ったら、選択したクライアントを使用して WorkSpace に接続できます。サインインすると、クライアントは WorkSpace デスクトップを表示します。

WorkSpace に接続するには

1. 招待メールでリンクを開きます。プロンプトが表示されたら、パスワードを入力して、ユーザーを有効化します。このパスワードは WorkSpace にサインインする際に必要となるため、覚えておいてください。

> **Note**
>
> パスワードは大文字と小文字が区別され、8〜64 文字の長さにする必要があります。パスワードには、小文字 (a〜z)、大文字 (A〜Z)、数字 (0〜9) のそれぞれのカテゴリから少なくとも 1 つの文字と、~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ が含まれている必要があります。

2. 各クライアントの要件の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントを確認し、次のいずれかの操作を行います。

   - プロンプトが表示されたら、クライアントアプリケーションの 1 つをダウンロードするか、Web Access を起動します。
   - プロンプトが表示されず、まだクライアントアプリケーションをインストールしていない場合は、https://clients.amazonworkspaces.com/ を開き、いずれかのクライアントアプリケーションをダウンロードするか、ウェブアクセスを起動します。

   > **Note**
   >
   > ウェブブラウザ (Web Access) を使用して Amazon Linux WorkSpaces に接続することはできません。

3. クライアントを起動し、招待 E メールから登録コードを入力して、[Register] を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. （オプション）資格情報を保存するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

次のステップ

作成した WorkSpace は引き続きカスタマイズできます。たとえば、ソフトウェアをインストールして WorkSpace からカスタムバンドルを作成することができます。WorkSpaces および WorkSpaces ディレクトリに対してさまざまな管理タスクを実行することもできます。WorkSpace の処理が終了したら、それを削除できます。詳細については、次のドキュメントを参照してください。

- カスタム WorkSpaces イメージとバンドルを作成する

- の管理 WorkSpaces
- WorkSpaces のディレクトリを管理する
- WorkSpace の削除

複数のモニターのセットアップや周辺機器の使用など、WorkSpaces クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントおよび周辺機器のサポートを参照してください。

Simple AD を使用して WorkSpace を起動する

WorkSpaces を使用すると、WorkSpaces として知られている、ユーザー向けの仮想クラウドベースの Microsoft Windows および Linux デスクトップを提供できます。

WorkSpaces は、ディレクトリを使用して、WorkSpace とユーザーの情報を格納し管理します。ディレクトリには、Simple AD、AD Connector、または Microsoft Active Directory 用の AWS Directory Service (AWS Managed Microsoft AD とも呼ばれます) のいずれかを選択できます。さらに、AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を確立することもできます。

このチュートリアルでは、Simple AD を使用する WorkSpace を起動します。他のオプションを使用するチュートリアルについては、「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

タスク

- 開始する前に
- ステップ 1: Simple AD ディレクトリを作成する
- ステップ 2: WorkSpace の作成
- ステップ 3: WorkSpace に接続する
- 次のステップ

開始する前に

- Simple AD は、すべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、Simple AD ディレクトリのリージョンを選択します。Simple AD でサポートされるリージョンの詳細については、 AWS Directory Service のリージョンの可用性を参照してください。

- WorkSpaces はすべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、WorkSpaces のリージョンを選択します。サポートされるリージョンについては、AWS リージョン別の WorkSpaces の料金を参照してください。
- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。バンドルは、オペレーティングシステム、ストレージ、コンピューティング、およびソフトウェアリソースの組み合わせです。詳細については、「Amazon WorkSpace バンドル」を参照してください。
- AWS Directory Service を使用してディレクトリを作成する場合、または WorkSpace を起動する場合は、パブリックサブネットと 2 つのプライベートサブネットで構成された仮想プライベートクラウドを作成または選択する必要があります。詳細については、「の VPC を設定する WorkSpaces」を参照してください

ステップ 1: Simple AD ディレクトリを作成する

Simple AD ディレクトリを作成します。AWS Directory Service は、VPC のプライベートサブネットにそれぞれ 2 つのディレクトリサーバーを作成します。最初はディレクトリにユーザーがいないことに注意してください。WorkSpace を作成したら、次のステップでユーザーを追加します。

> **Note**
>
> Simple AD は、WorkSpaces で無料でご利用になれます。Simple AD ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> 空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD ディレクトリを削除した後に WorkSpaces を再度ご使用になる際は、いつでも新しいディレクトリを作成できます。

Simple AD ディレクトリを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. [Set up Directory] (ディレクトリの設定)、[Simple AD]、[Next] (次へ) の順に選択します。
4. 以下のようにディレクトリを設定します。

a. [Organization name] には、ディレクトリの一意の組織名 (例: my-example-directory) を入力します。この名前は、長さが 4 文字以上で、英数字とハイフン (-) のみで構成され、ハイフン以外の文字で開始または終了している必要があります。

b. [Directory DNS name] (ディレクトリの DNS 名) には、ディレクトリの完全修飾名を入力します (例: example.com)。

> **Important**
>
> WorkSpaces の起動後に DNS サーバーを更新する必要がある場合は、Amazon WorkSpaces の DNS サーバーの更新 の手順に従って WorkSpaces が正しく更新されていることを確認します。

c. [NetBIOS name] には、ディレクトリの短縮名を入力します (例: example) 。

d. [Admin password] と [Confirm Password] に、ディレクトリ管理者アカウントのパスワードを入力します。パスワードの要件の詳細については、AWS Directory Service 管理ガイドの Microsoft AD Directory の作成方法を参照してください。

e. (オプション) [Description] に、ディレクトリの説明を入力します。

f. [Directory size] (ディレクトリのサイズ) で、[Small] (スモール) を選択します。

g. [VPC] では、作成した VPC を選択します。

h. [Subnets] で、2 つのプライベートサブネットを選択します (CIDR ブロック `10.0.1.0/24` および `10.0.2.0/24`) 。

i. [次へ] を選択します。

5. [Create directory] (ディレクトリの作成) を選択します。

6. ディレクトリの最初のステータスは `Requested` で、次に `Creating` となります。ディレクトリの作成が完了すると (これには数分かかる場合があります)、ステータスは `Active` になります。

ディレクトリ作成時の動作

WorkSpaces が、あなたの代わりに次のタスクを完了します。

- IAM ロールを作成して、WorkSpaces サービスが Elastic Network Interface を作成し、WorkSpaces ディレクトリの一覧を表示できるようにします。そのロールには、`workspaces_DefaultRole` という名前が付きます。

- ユーザーおよび WorkSpace 情報を格納するために使用される VPC の Simple AD ディレクトリをセットアップします。このディレクトリには、Administrator というユーザー名と指定されたパスワードを持つ管理者アカウントがあります。
- 2 つのセキュリティグループを作成します。1 つはディレクトリコントローラー用で、もう 1 つはディレクトリ内の WorkSpaces 用です。

ステップ 2: WorkSpace の作成

これで、WorkSpace を起動する準備ができました。

ユーザーの WorkSpace を作成するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. [Launch WorkSpaces] を選択します。
4. [Select a Directory] ページで、次のようにします。
   a. [Directory] で、作成したディレクトリを選択します。
   b. [Enable Self Service Permissions] (セルフサービスアクセス許可の有効化) で、[Yes] (はい) または [No] (いいえ) を選択し、説明を入力します。
   c. [Amazon WorkDocs の有効化] で、[Yes] を選択します。

      > **Note**
      > このオプションは、選択されたリージョンで Amazon WorkDocs が使用可能な場合にのみ使用できます。

   d. [Next Step] を選択します。WorkSpaces が Simple AD ディレクトリを登録します。
5. [Identify Users] ページで、次のようにディレクトリに新しいユーザーを追加します。
   a. [Username]、[First Name]、[Last Name]、および [Email] に値を入力します。アクセス権のある E メールアドレスを使用してください。
   b. [Create Users] を選択します。
   c. [Next Step] を選択します。
6. [Select Bundle] ページで、バンドル;を選択し、[Next Step] を選択します。

> **Note**
>
> 各バンドルの推奨用途と仕様を確認して、ユーザーに最適なバンドルを選択できるようにしてください。各ユースケースの詳細については、「Amazon WorkSpaces バンドル」を参照してください。バンドルの仕様、推奨用途、および料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

7. [WorkSpaces Configuration] ページで、実行モードを選択してから、[Next Step] を選択します。
8. [Review & Launch WorkSpaces] ページで、[Launch WorkSpaces] を選択します。WorkSpace の最初のステータスは `PENDING` です。起動が完了すると (最長 20 分かかる場合があります)、ステータスは `AVAILABLE` になり、ユーザーに指定した E メールアドレスに招待状が送信されます。

> **Note**
>
> ユーザーが既に Active Directory に存在する場合、招待メールは送信されません。代わりに、ユーザーに招待メールを手動で送信してください。詳細については、「招待 E メールの送信」を参照してください

ステップ 3: WorkSpace に接続する

招待メールを受け取ったら、選択したクライアントを使用して WorkSpace に接続できます。サインインすると、クライアントは WorkSpace デスクトップを表示します。

WorkSpace に接続するには

1. 招待メールでリンクを開きます。プロンプトが表示されたら、パスワードを入力して、ユーザーを有効にします。このパスワードは WorkSpace にサインインする際に必要となるため、覚えておいてください。

> **Note**
>
> パスワードは大文字と小文字が区別され、8〜64 文字の長さにする必要があります。パスワードには、小文字 (a〜z)、大文字 (A〜Z)、数字 (0〜9) のそれぞれのカテゴリから少なくとも 1 つの文字と、~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/ が含まれている必要があります。

2. 各クライアントの要件の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントを確認し、次のいずれかの操作を行います。

   - プロンプトが表示されたら、クライアントアプリケーションの 1 つをダウンロードするか、Web Access を起動します。
   - プロンプトが表示されず、まだクライアントアプリケーションをインストールしていない場合は、https://clients.amazonworkspaces.com/ を開き、いずれかのクライアントアプリケーションをダウンロードするか、ウェブアクセスを起動します。

   > **Note**
   >
   > ウェブブラウザ (Web Access) を使用して Amazon Linux WorkSpaces に接続することはできません。

3. クライアントを起動し、招待 E メールから登録コードを入力して、[Register] を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. （オプション）資格情報を保存するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

次のステップ

作成した WorkSpace は引き続きカスタマイズできます。たとえば、ソフトウェアをインストールして WorkSpace からカスタムバンドルを作成することができます。WorkSpaces および WorkSpaces ディレクトリに対してさまざまな管理タスクを実行することもできます。WorkSpace の処理が終了したら、それを削除できます。詳細については、次のドキュメントを参照してください。

- カスタム WorkSpaces イメージとバンドルを作成する
- の管理 WorkSpaces
- WorkSpaces のディレクトリを管理する
- WorkSpace の削除

複数のモニターのセットアップや周辺機器の使用など、WorkSpaces クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントおよび周辺機器のサポートを参照してください。

AD Connector を使用して WorkSpace を起動する

WorkSpaces を使用すると、WorkSpaces として知られている、ユーザー向けの仮想クラウドベースの Microsoft Windows および Linux デスクトップを提供できます。

WorkSpaces は、ディレクトリを使用して、WorkSpace とユーザーの情報を格納し管理します。ディレクトリには、Simple AD、AD Connector、または Microsoft Active Directory 用の AWS Directory Service (AWS Managed Microsoft AD とも呼ばれます) のいずれかを選択できます。さらに、AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を確立することもできます。

このチュートリアルでは、AD Connector を使用する WorkSpace を起動します。他のオプションを使用するチュートリアルについては、「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

タスク

開始する前に

- WorkSpaces はすべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、WorkSpaces のリージョンを選択します。サポートされるリージョンについては、AWS リージョン別の WorkSpaces の料金を参照してください。
- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。バンドルは、オペレーティングシステム、ストレージ、コンピューティング、およびソフトウェアリソースの組み合わせです。詳細については、「Amazon WorkSpace バンドル」を参照してください。
- 少なくとも 2 つのプライベートサブネットを持つ Virtual Private Cloud を作成します。詳細については、「の VPC を設定する WorkSpaces」を参照してください VPC は、仮想プライベートネットワーク (VPN) 接続または を通じてオンプレミスのネットワークに接続されている必要がありますAWS Direct Connect 詳細については、AWS Directory Service 管理ガイドのAD Connector の前提条件を参照してください。

- WorkSpace からインターネットにアクセスできます。詳細については、「からのインターネットアクセスを提供する WorkSpace」を参照してください

ステップ 1: AD Connector の作成

> **Note**
>
> AD Connector は、WorkSpaces で無料でご利用になれます。AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> 空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

AD Connector を作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. [Set up Directory]、[Create AD Connector] をクリックします。
4. [Organization name] には、ディレクトリの一意の組織名（例: my-example-directory）を入力します。この名前は、長さが 4 文字以上で、英数字とハイフン（-）のみで構成され、ハイフン以外の文字で開始または終了している必要があります。
5. [Connected directory DNS] には、オンプレミスディレクトリの完全修飾名（例: example.com）を入力します。
6. [Connected directory NetBIOS name] には、オンプレミスディレクトリの短い名前（例: example）を入力します。
7. [Connector account username] では、オンプレミスディレクトリにユーザーのユーザー名を入力します。ユーザーには、ユーザーとグループの読み取り、コンピュータオブジェクトの作成、コンピュータのドメインへの参加を許可する必要があります。
8. [Connector account password] (Connector アカウントのパスワード) と [Confirm password] (パスワードの確認) に、オンプレミスユーザーのパスワードを入力します。
9. [DNS address] には、オンプレミスディレクトリ内の少なくとも 1 つの DNS サーバーの IP アドレスを入力します。

> **Important**
>
> WorkSpaces の起動後に DNS サーバーの IP アドレスを更新する必要がある場合は、Amazon WorkSpaces の DNS サーバーの更新 の手順 に従って WorkSpaces が正しく更新されていることを確認します。

10. （オプション）[Description] に、ディレクトリの説明を入力します。
11. [Size] を [Small] のままにします。
12. [VPC] で、自分の VPC を選択します。
13. [Subnet] で、サブネットを選択します。指定した DNS サーバーには、各サブネットからアクセスできる必要があります。
14. [Next Step] を選択します。
15. [AD Connector の作成] の選択 ディレクトリが接続されるには数分かかります。ディレクトリの最初のステータスは `Requested` で、次に `Creating` となります。ディレクトリの作成が完了すると、ステータスが `Active` に変わります。

ステップ 2: WorkSpace の作成

これで、オンプレミスディレクトリで 1 人以上のユーザーが WorkSpace を起動する準備が整いました。

既存のユーザーの WorkSpace を起動するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. [Launch WorkSpaces] を選択します。
4. [Directory] で、作成したディレクトリを選択します。
5. (オプション) このディレクトリで初めて WorkSpace を起動する場合で、Amazon WorkDocs がリージョンでサポートされている場合、このディレクトリのすべてのユーザーに対して Amazon WorkDocs を有効または無効にすることができます。Amazon WorkDocs の詳細については、Amazon WorkDocs 管理ガイドの Amazon WorkDocs Drive を参照してください。
6. [次へ] を選択します。WorkSpaces が AD Connector を登録します。
7. オンプレミスディレクトリから 1 人以上の既存ユーザーを選択します。WorkSpaces コンソールを使用して、オンプレミスディレクトリに新規ユーザーを追加しないでください。

選択するユーザーを見つけるには、ユーザー名の全体または一部を入力し、[Search] または [Show All Users] をクリックします。E メールアドレスを持っていないユーザーは選択できないことに注意してください。

ユーザーを選択したら、[Add Selected]、[Next Step] の順に選択します。

8. [Select Bundle] で、WorkSpaces 用に使用するデフォルトの WorkSpace バンドルを選択します。[Assign WorkSpace Bundles] で、必要に応じて個々の WorkSpace に異なるバンドルを選択することができます。完了したら、[Next Step] を選択します。

> **Note**
>
> 各バンドルの推奨用途と仕様を確認して、ユーザーに最適なバンドルを選択できるようにしてください。各ユースケースの詳細については、「Amazon WorkSpaces バンドル」を参照してください。バンドルの仕様、推奨用途、および料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

9. WorkSpace の実行モードを選択し、[Next Step] を選択します。詳細については、「WorkSpace の実行モードを管理する」を参照してください
10. [Launch WorkSpaces] を選択します。WorkSpace の最初のステータスは PENDING です。起動が完了すると、ステータスが [AVAILABLE] に変わります。
11. 各ユーザーの E メールアドレスに招待状を送信します。(AD Connector を使用している場合、これらの招待状は自動的に送信されません) 詳細については、「招待 E メールの送信」を参照してください

ステップ 3: WorkSpace に接続する

任意のクライアントを使用して WorkSpace に接続できます。サインインすると、クライアントは WorkSpace デスクトップを表示します。

WorkSpace に接続するには

1. 招待メールでリンクを開きます。
2. 各クライアントの要件の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントを確認し、次のいずれかの操作を行います。

   - プロンプトが表示されたら、クライアントアプリケーションの 1 つをダウンロードするか、Web Access を起動します。

- プロンプトが表示されず、まだクライアントアプリケーションをインストールしていない場合は、https://clients.amazonworkspaces.com/ を開き、いずれかのクライアントアプリケーションをダウンロードするか、ウェブアクセスを起動します。

> **Note**
>
> ウェブブラウザ (Web Access) を使用して Amazon Linux WorkSpaces に接続することはできません。

3. クライアントを起動し、招待 E メールから登録コードを入力して、[Register] を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. （オプション）資格情報を保存するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

> **Note**
>
> AD Connector を使用しているため、ユーザーは自分のパスワードをリセットできません。([パスワードを忘れた場合] オプションは、WorkSpaces クライアントアプリケーションのログイン画面では使用できません。) ユーザーパスワードをリセットする方法については、WorkSpaces の Active Directory 管理ツールを設定する を参照してください。

次のステップ

作成した WorkSpace は引き続きカスタマイズできます。たとえば、ソフトウェアをインストールして WorkSpace からカスタムバンドルを作成することができます。WorkSpaces および WorkSpaces ディレクトリに対してさまざまな管理タスクを実行することもできます。WorkSpace の処理が終了したら、それを削除できます。詳細については、次のドキュメントを参照してください。

- カスタム WorkSpaces イメージとバンドルを作成する
- の管理 WorkSpaces
- WorkSpaces のディレクトリを管理する
- WorkSpace の削除

複数のモニターのセットアップや周辺機器の使用など、WorkSpaces クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントおよび周辺機器のサポートを参照してください。

信頼できるドメインを使用して WorkSpace を起動する

WorkSpaces を使用すると、WorkSpaces として知られている、ユーザー向けの仮想クラウドベースの Microsoft Windows、Amazon Linux、Ubuntu Linux デスクトップを提供できます。

WorkSpaces は、ディレクトリを使用して、WorkSpace とユーザーの情報を格納し管理します。ディレクトリには、Simple AD、AD Connector、または Microsoft Active Directory 用の AWS Directory Service (AWS Managed Microsoft AD とも呼ばれます) のいずれかを選択できます。さらに、AWS Managed Microsoft AD ディレクトリとオンプレミスドメイン間の信頼関係を確立することもできます。

このチュートリアルでは、信頼関係を使用する WorkSpace を起動します。他のオプションを使用するチュートリアルについては、「WorkSpaces を使用して仮想デスクトップを起動します。」を参照してください。

タスク

- 開始する前に
- ステップ 1: 信頼関係を確立する
- ステップ 2: WorkSpace の作成
- ステップ 3: WorkSpace に接続する
- 次のステップ

開始する前に

- 別の信頼されたドメインで AWS アカウントを使用して WorkSpaces を起動することは、AWS Managed Microsoft AD で可能です (この AD とオンプレミスのディレクトリとの信頼関係が設定されている場合)。ただし、Simple AD または AD Connector を使用する WorkSpaces では、信頼されたドメインのユーザーに対して WorkSpaces を起動することはできません。
- WorkSpaces はすべてのリージョンで利用できるわけではありません。サポートされているリージョンを確認し、WorkSpaces のリージョンを選択します。サポートされるリージョンについては、AWS リージョン別の WorkSpaces の料金を参照してください。

- WorkSpace を起動するときは、WorkSpace バンドルを選択する必要があります。バンドルは、ストレージ、計算、およびソフトウェアリソースの組み合わせです。詳細については、「Amazon WorkSpaces バンドル」を参照してください。
- AWS Directory Service を使用してディレクトリを作成する場合、または WorkSpace を起動する場合は、パブリックサブネットと 2 つのプライベートサブネットで構成された仮想プライベートクラウドを作成または選択する必要があります。詳細については、「の VPC を設定する WorkSpaces」を参照してください

ステップ 1: 信頼関係を確立する

信頼関係をセットアップするには

1. Virtual Private Cloud (VPC) に AWS Managed Microsoft AD を設定します。詳細については、AWS Directory Service 管理ガイドのAWS Managed Microsoft AD ディレクトリを作成するを参照してください。

   > **Note**
   >
   > - 現在、共有ディレクトリは、Amazon WorkSpaces での使用はサポートされていません。
   > - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリが設定されている場合は、プライマリリージョンのディレクトリのみを Amazon WorkSpaces で使用するために登録できます。Amazon WorkSpaces で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用についてサポートされていません。

2. AWS Managed Microsoft AD とオンプレミスドメイン間の信頼関係を作成します。信頼が双方向の信頼として設定されていることを確認します。詳細については、AWS Directory Service 管理ガイドのチュートリアル: AWS Managed Microsoft AD とオンプレミスドメイン間の信頼関係を作成を参照してください。

オンプレミスの認証情報を使用して WorkSpaces の管理と Workspaces による認証を行い、WorkSpaces をオンプレミスのユーザーとグループに対してプロビジョニングするために一方向

または双方向の信頼を使用できます。詳細については、「Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain with AWS Directory Service」を参照してください。

> **Note**
>
> Ubuntu WorkSpaces は Active Directory の統合に System Security Services Daemon (SSSD) を使用していますが、SSSD はフォレストトラストをサポートしていません。その代わりに外部信頼を設定してください。Amazon Linux と Ubuntu の WorkSpaces では、双方向の信頼を推奨しています。

ステップ 2: WorkSpace の作成

AWS Managed Microsoft AD とオンプレミスの Microsoft Active Directory ドメイン間で信頼関係を確立した後、オンプレミスドメインのユーザーに対して WorkSpaces をプロビジョニングできます。

GPO 設定が WorkSpaces に適用される前に、ドメイン間でレプリケートされていることを確認する必要があります。

信頼されたオンプレミスドメインのユーザーの WorkSpaces を起動するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. [Launch WorkSpaces] を選択します。
4. [Select a Directory] ページで、先ほど登録したディレクトリを選択し、[Next Step] を選択します。
5. [Identify Users] ページで、以下を実行します。
   a. [Select trust from forest] では、作成した信頼関係を選択します。
   b. ユーザーをオンプレミス ドメインから選択し、[Add Selected] を選択します。
   c. [Next Step] を選択します。
6. WorkSpaces に使用するバンドルを選択し、[Next Step] を選択します。

> **Note**
>
> 各バンドルの推奨用途と仕様を確認して、ユーザーに最適なバンドルを選択できるようにしてください。各ユースケースの詳細については、「Amazon WorkSpaces バンド

ル」を参照してください。バンドルの仕様、推奨用途、および料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

7. 実行モードを選択して、暗号化設定を選択し、タグを設定します。完了したら、[Next Step] を選択します。
8. [Launch WorkSpaces] を選択します。WorkSpaces が使用可能になるまでに 20 分、暗号化を有効にした場合は最大 40 分かかることに注意してください。WorkSpace の最初のステータスは PENDING です。起動が完了すると、ステータスが [AVAILABLE] に変わります。
9. 各ユーザーの E メールアドレスに招待状を送信します。(信頼関係を使用している場合、これらの招待状は自動的に送信されません) 詳細については、「招待 E メールの送信」を参照してください

ステップ 3: WorkSpace に接続する

招待メールを受け取ったら、WorkSpace に接続できます。ユーザーは、username、corp\username、または corp.example.com\username のようなユーザー名を入力できます。

WorkSpace に接続するには

1. 招待メールでリンクを開きます。プロンプトが表示されたら、パスワードを入力して、ユーザーを有効にします。このパスワードは WorkSpace にサインインする際に必要となるため、覚えておいてください。

> **Note**
>
> パスワードは大文字と小文字が区別され、8〜64 文字の長さにする必要があります。パスワードには、小文字 (a〜z)、大文字 (A〜Z)、数字 (0〜9) のそれぞれのカテゴリから少なくとも 1 つの文字と、~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/ が含まれている必要があります。

2. 各クライアントの要件の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントを確認し、次のいずれかの操作を行います。
   - プロンプトが表示されたら、クライアントアプリケーションの 1 つをダウンロードするか、Web Access を起動します。

- プロンプトが表示されず、まだクライアントアプリケーションをインストールしていない場合は、https://clients.amazonworkspaces.com/ を開き、いずれかのクライアントアプリケーションをダウンロードするか、ウェブアクセスを起動します。

> **Note**
>
> ウェブブラウザ (Web Access) を使用して Amazon Linux WorkSpaces に接続することはできません。

3. クライアントを起動し、招待 E メールから登録コードを入力して、[Register] を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. （オプション）資格情報を保存するかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

次のステップ

作成した WorkSpace は引き続きカスタマイズできます。たとえば、ソフトウェアをインストールして WorkSpace からカスタムバンドルを作成することができます。WorkSpaces および WorkSpaces ディレクトリに対してさまざまな管理タスクを実行することもできます。WorkSpace の処理が終了したら、それを削除できます。詳細については、次のドキュメントを参照してください。

- カスタム WorkSpaces イメージとバンドルを作成する
- の管理 WorkSpaces
- WorkSpaces のディレクトリを管理する
- WorkSpace の削除

複数のモニターのセットアップや周辺機器の使用など、WorkSpaces クライアントアプリケーションの使用方法の詳細については、Amazon WorkSpaces ユーザーガイドの WorkSpaces クライアントおよび周辺機器のサポートを参照してください。

WorkSpace ユーザーを管理する

各 WorkSpace は 1 人のユーザーに割り当てられており、複数のユーザーで共有することはできません。デフォルトでは、ディレクトリごとに 1 ユーザーあたり 1 つの WorkSpace のみ許可されます。

目次

WorkSpaces ユーザーの管理

WorkSpaces の管理者は、WorkSpaces ユーザーを管理するために以下のタスクを実行します。

ユーザー情報を編集する

WorkSpaces コンソールを使用して、WorkSpace のユーザーの以下の情報を編集できます。

> **Note**
>
> この機能は、AWS Managed Microsoft AD または Simple AD を使用する場合にのみ利用できます。AD Connector または信頼関係を使用して Microsoft Active Directory を使用する場合は、Active Directory モジュールを使用してユーザーとグループを管理できます。

ユーザー情報を編集するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. ユーザーを選択したら、[Actions] (アクション)、[Edit User] (ユーザーの編集) の順に選択します。
4. 必要に応じて、[First Name] (名)、[Last Name] (姓)、[Email] (E メール) を更新します

5. [更新] を選択します。

ユーザーを追加または削除する

Amazon WorkSpaces コンソールからユーザーを作成できるのは、WorkSpace の起動プロセス中のみです。Amazon WorkSpaces コンソールからユーザーを削除することはできません。ユーザーグループの管理など、ほとんどのユーザー管理タスクは、ディレクトリで実行する必要があります。

ユーザーとグループを追加または削除するには

ユーザーとグループを追加、削除、または管理するには、ディレクトリを通じてこれを行う必要があります。WorkSpaces ディレクトリのほとんどの管理タスクは、Active Directory 管理ツールなどのディレクトリ管理ツールを使用して実行します。詳細については、「WorkSpaces の Active Directory 管理ツールを設定する」を参照してください

> **Important**
>
> ユーザーを削除する前に、ユーザーに割り当てられた WorkSpace を削除する必要があります。詳細については、「WorkSpace の削除」を参照してください

ユーザーとグループの管理に使用するプロセスは、使用しているディレクトリの種類によって異なります。

- AWS Managed Microsoft AD を使用している場合は、AWS Directory Service 管理ガイドの AWS Managed Microsoft AD のユーザーとグループの管理を参照してください。
- Simple AD を使用している場合は、AWS Directory Service 管理ガイドのSimple AD でユーザーとグループを管理するを参照してください。
- AD Connector または信頼関係を使用して Microsoft Active Directory を使用する場合は、Active Directory モジュールを使用してユーザーとグループを管理できます。

招待 E メールの送信

必要に応じて、手動で招待メールを送信することができます。

> **Note**
>
> AD Connector または信頼されたドメインを使用している場合、招待メールはユーザーに自動的には送信されないため、手動で送信する必要があります。また、ユーザーが既に Active Directory に存在する場合も、招待メールは自動的に送信されません。

招待 E メールを再送信するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. [WorkSpace] ページで、検索ボックスを使用して招待を送信するユーザーを検索し、検索結果から対応する WorkSpace を選択します。一度に選択できる WorkSpace は 1 つだけです。
4. [Actions] (アクション)、[Invite User] (ユーザーを招待) の順に選択します。
5. [Invite users to the WorkSpace] (WorkSpace にユーザーを招待) ページで、[Send invite] (招待を送信) を選択します。

ユーザー用に複数の WorkSpaces を作成する

デフォルトでは、ディレクトリごとに 1 ユーザーあたり 1 つの WorkSpace のみ作成できます。ただし、必要に応じて、ディレクトリ設定に応じて、1 ユーザーに対して複数の WorkSpace を作成できます。

- WorkSpaces 用のディレクトリが 1 つしかない場合は、そのユーザーに対して複数のユーザー名を作成します。たとえば、Mary Major という名前のユーザーは、mmajor1、mmajor2 などのユーザー名を持つことができます。各ユーザー名は、同じディレクトリ内の異なる WorkSpace に関連付けられますが、WorkSpaces がすべて同じ AWS リージョンの同じディレクトリに作成されている限り、WorkSpaces は同じ登録コードを持ちます。
- WorkSpaces に複数のディレクトリがある場合は、ユーザーの WorkSpace を別々のディレクトリに作成します。複数のディレクトリで同じユーザー名を使用することも、ディレクトリで異なるユーザー名を使用することもできます。WorkSpace の登録コードは異なります。

> **Tip**
>
> ユーザー用に作成したすべての WorkSpaces を簡単に見つけることができるように、各 WorkSpace に同じ基本ユーザー名を使用します。

例えば、Active Directory ユーザー名を mmajor とする Mary Major という名前のユーザーがある場合、mmajor、mmajor1、mmjor2、mmjor3 などのユーザー名や、mmjor_windows や mmmajor_linux などの多少変化させたものを使用して、当該ユーザーのための WorkSpaces を作成します。すべての WorkSpaces のベースユーザー名 (mmajor) の冒頭が同じであれば、WorkSpaces コンソールでユーザー名を並べ替えて、そのユーザーのすべての WorkSpaces をグループ化できます。

Important

- 2 つの WorkSpaces が別々のディレクトリにある限り、ユーザーは PCoIP と WSP WorkSpace の両方を持つことができます。同じユーザーが PCoIP と WSP WorkSpace を同じディレクトリ内に持つことはできません。
- クロスリージョンリダイレクトで使用する複数の WorkSpaces を設定する場合は、異なる AWS リージョンの異なるディレクトリに WorkSpaces をセットアップし、各ディレクトリで同じユーザー名を使用する必要があります。クロスリージョンリダイレクトの詳細については、Amazon のクロスリージョンリダイレクト WorkSpaces を参照してください。

WorkSpaces 間で切り替えるには、特定のワークスペースに関連付けられたユーザー名と登録コードを使用してログインします。ユーザーが Windows、macOS、または Linux 用の WorkSpaces クライアントアプリケーションのバージョン 3.0 以降を使用している場合は、クライアントアプリケーションで [設定]、[ログイン情報の管理] の順に選択し、WorkSpace に異なる名前を割り当てることができます。

ユーザーが にログインする方法をカスタマイズする WorkSpaces

Uniform Resource Identifier (URIs WorkSpaces を使用して へのユーザーのアクセスをカスタマイズし、組織内の既存のワークフローと統合するシンプルなログインエクスペリエンスを提供します。例えば、 WorkSpaces 登録コードを使用してユーザーを登録するログイン URIs を自動的に生成できます。上の結果:

- ユーザーは手動登録プロセスを省略できます。
- ユーザーのユーザー名は、 WorkSpaces クライアントのログインページに自動的に入力されます。

- 組織内で多要素認証 (MFA) が使用されている場合、クライアントログインページに組織のユーザー名と MFA コードが自動的に入力されます。

URI アクセスは、リージョンベースの登録コード (`WSpdx+ABC12D` など) と完全修飾ドメイン名 (FQDN) ベースの登録コード (`desktop.example.com` など) の両方で動作します。FQDN ベースの登録コードの作成および使用の詳細については、Amazon のクロスリージョンリダイレクト WorkSpaces を参照してください。

以下のサポートされているデバイスで、クライアントアプリケーション WorkSpaces に対する への URI アクセスを設定できます。

- Windows コンピュータ
- macOS コンピュータ
- Ubuntu Linux 18.04、20.04、22.04 コンピュータ
- iPad
- Android デバイス

URIs を使用して にアクセスするには WorkSpaces、まず https://clients.amazonworkspaces.com/ を開き、指示に従って、デバイスのクライアントアプリケーションをインストールする必要があります。

URI アクセスは、Windows および macOS コンピュータの Firefox および Chrome ブラウザ、Ubuntu Linux 18.04、20.04、22.04 コンピュータの Firefox ブラウザ、および Windows コンピュータの Internet Explorer および Microsoft Edge ブラウザでサポートされています。WorkSpaces クライアントの詳細については、「Amazon WorkSpaces ユーザーガイド」のWorkSpaces 「クライアント」を参照してください。

> **Note**
>
> Android デバイスでは、URI アクセスは Firefox ブラウザでのみ機能し、Google Chrome ブラウザでは機能しません。

への URI アクセスを設定するには WorkSpaces、次の表に示す URI 形式のいずれかを使用します。

> **Note**
>
> URI のデータコンポーネントに次の予約文字が含まれている場合、あいまいさを避けるために、データコンポーネントでパーセントエンコードを使用することをお勧めします。
> `@ : / ? & =`
> 例えば、これらの文字のいずれかを含むユーザー名がある場合、その URI 内のユーザー名をパーセントでエンコードする必要があります。詳細については、「Uniform Resource Identifier (URI): 一般的な構文」を参照してください。

サポートされている構文	説明
workspaces://	WorkSpaces クライアントアプリケーションを開きます。(注: workspaces:// 単独の使用は、現在 Linux クライアントアプリケーションではサポートされていません)。
workspaces://@registrationcode	WorkSpaces 登録コードを使用してユーザーを登録します。また、クライアントのログインページが表示されます。
workspaces://username@registrationcode	WorkSpaces 登録コードを使用してユーザーを登録します。また、クライアントログインページの [ユーザー名] フィールドにユーザー名を自動的に入力します。
workspaces://username@registrationcode?MFACode=mfa	WorkSpaces 登録コードを使用してユーザーを登録します。また、[ユーザー名] フィールドにユーザー名を入力し、クライアントログインページの [MFA コード] フィールドに多要素認証 (MFA) コードを自動的に入力します。
workspaces://@registrationcode?MFACode=mfa	WorkSpaces 登録コードを使用してユーザーを登録します。また、クライアントログインページの [MFA code] フィールドに Multi-Factor Authentication (MFA) コードを自動的に入力します。

> **Note**
>
> ユーザーが Windows クライアント WorkSpace から に既に接続しているときに URI リンクを開くと、新しい WorkSpaces セッションが開き、元の WorkSpaces セッションは開いたままになります。ユーザーが macOS iPad 、iPad、または Android クライアント WorkSpace から に接続したときに URI リンクを開くと、新しいセッションは開かれず、元の WorkSpaces セッションのみが開いたままになります。

ユーザーのセルフサービス WorkSpace管理機能を有効にする

では WorkSpaces、ユーザーがエクスペリエンスをより詳細に制御できるように、セルフサービス WorkSpace 管理機能を有効にできます。また、 の IT サポートスタッフのワークロードを減らすこともできます WorkSpaces。セルフサービス機能を有効にすると、ユーザーは WorkSpaces クライアントから直接次のタスクを 1 つ以上実行できます。

- 認証情報はクライアントにキャッシュされます。これにより、認証情報を再入力 WorkSpace せずに に再接続できます。
- を再起動 (再起動) します WorkSpace。
- のルートボリュームとユーザーボリュームのサイズを増やします WorkSpace。
- のコンピューティングタイプ (バンドル) を変更します WorkSpace。
- の実行モードを切り替えます WorkSpace。
- を再構築します WorkSpace。

Supported Clients (サポートされるクライアント)

- Android、Android または Android 対応の Chrome OS システム
- Linux
- macOS
- Windows

ユーザーの自己管理機能を有効にするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。

3. セルフサービス管理機能を有効にするディレクトリを選択します。
4. セルフサービスのアクセス許可まで下にスクロールし、編集 を選択します。ユーザーがクライアントから実行できる WorkSpace 管理タスクを決定するために、必要に応じて以下のオプションを有効または無効にします。

   - Remember me (このアカウントを記憶する) — ユーザーは、ログイン画面の [Remember Me] (このアカウントを記憶する) または [Keep me logged in] (ログイン状態を保つ) のチェックボックスを選択して、認証情報をクライアントにキャッシュするかどうかを選択できます。認証情報は、RAM にのみキャッシュされます。ユーザーが認証情報をキャッシュすることを選択した場合、認証情報を再入力 WorkSpaces せずに に再接続できます。ユーザーが認証情報をキャッシュできる期間を管理する方法については、Kerberos チケットの最大ライフタイムを設定する を参照してください。
   - クライアント WorkSpace からの再起動 — ユーザーは を再起動 (再起動) できます WorkSpace。再起動すると、ユーザーは から切断され WorkSpace、シャットダウンされ、再起動されます。ユーザーデータ、オペレーティングシステム、およびシステム設定には影響しません。
   - ボリュームサイズを増やす — ユーザーは、IT サポートに連絡することなく、 のルートボリュームとユーザーボリュームを指定されたサイズ WorkSpace に拡張できます。ユーザーはルートボリューム (Windows の場合は C: ドライブ、Linux の場合は /) のサイズを最大 175 GB まで増やすことができ、ユーザーボリューム (Windows の場合は D: ドライブ、Linux の場合は /home) のサイズを最大 100 GB まで増やすことができます。 WorkSpace ルートとユーザーボリュームは変更できないセットグループに含まれています。使用可能なボリュームは [ルート (GB)、ユーザー (GB)]: [80、10]、[80、50]、[80、100]、[175 ~ 2000、100 ~ 2000] です。詳細については、「の変更 WorkSpace」を参照してください。

     新しく作成された の場合 WorkSpace、ユーザーはこれらのドライブのサイズを増やす前に 6 時間待つ必要があります。それ以降、6 時間に 1 度のみ行うことができます。ボリュームサイズの増加中は、ユーザーは でほとんどのタスクを実行できます WorkSpace。実行できないタスクは、 WorkSpace コンピューティングタイプの変更、 WorkSpace 実行モードの切り替え、 の再起動 WorkSpace、 の再構築です WorkSpace。プロセスが完了したら、変更を有効にするために を再起動 WorkSpace する必要があります。このプロセスには最長で 1 時間程度かかることがあります。

> **Note**
>
> ユーザーが のボリュームサイズを増やすと WorkSpace、 の請求レートが増加します WorkSpace。

- コンピューティングタイプの変更 — ユーザーはコンピューティングタイプ (バンドル) WorkSpace を切り替えることができます。新しく作成された の場合 WorkSpace、ユーザーは別のバンドルに切り替える前に 6 時間待つ必要があります。それ以降は、6 時間に 1 度のみ大きなバンドルに切り替えるか、30 日間に 1 回小さなバンドルに切り替えることができます。 WorkSpace コンピューティングタイプの変更が進行中の場合、ユーザーは から切断され WorkSpace、 を使用または変更することはできません WorkSpace。 WorkSpace は、コンピューティングタイプの変更プロセス中に自動的に再起動されます。このプロセスには最長で 1 時間程度かかることがあります。

> **Note**
>
> ユーザーが WorkSpace コンピューティングタイプを変更すると、 の請求レートが変更されます WorkSpace。

- 実行モードを切り替える — ユーザーは AlwaysOnとAutoStop実行モード WorkSpace を切り替えることができます。詳細については、「WorkSpace の実行モードを管理する」を参照してください。

> **Note**
>
> ユーザーが の実行モードを切り替えると WorkSpace、 の請求レートが変更されます WorkSpace。

- クライアント WorkSpace からの再構築 — ユーザーは のオペレーティングシステムを WorkSpace 元の状態に再構築できます。 WorkSpace が再構築されると、ユーザーボリューム (D: ドライブ) が最新のバックアップから再作成されます。バックアップは、12 時間ごとに完了するため、ユーザーのデータには最大 12 時間分含まれます。新しく作成された の場合 WorkSpace、ユーザーは を再構築するまで 12 時間待つ必要があります WorkSpace。 WorkSpace 再構築が進行中の場合、ユーザーは から切断され WorkSpace、 を使用または変更することはできません WorkSpace。このプロセスには最長で 1 時間程度かかることがあります。

- 診断ログのアップロード — ユーザーは、クライアントの使用を中断することなく、WorkSpaces クライアントログファイルを に直接アップロード WorkSpaces WorkSpaces して、問題をトラブルシューティングできます。ユーザーの診断ログのアップロードを有効にするか、ユーザー自身で有効にすると、ログファイルは自動的に に送信されます WorkSpaces 。 WorkSpaces ストリーミングセッションの前または最中に診断ログのアップロードを有効にできます。

5. [保存] を選択します。

ユーザーの Amazon Connect オーディオ最適化を有効にする

WorkSpaces 管理コンソールで、WorkSpaces フリートの Amazon Connect 問い合わせコントロールパネル (CCP) のオーディオ最適化を有効にして、セキュリティを強化し、ネイティブ品質のオーディオを有効にできます。CCP オーディオ最適化を有効にすると、CCP オーディオはクライアントエンドポイントによって処理されますが、WorkSpaces ユーザーは WorkSpaces 内から CCP と対話できます。

Amazon Connect の問い合わせコントロールパネル (CCP) のオーディオ最適化は、以下で機能します。

- WorkSpaces Windows クライアント。
- Amazon Linux と Windows WorkSpaces。
- PCoIP または WSP を使用する WorkSpaces。

要件

- Amazon Connect で設定する必要があります。
- 呼び出し発信用のメディアを持たない CCP を作成することにより、Amazon Connect Streams API を使用してカスタム CCP を構築する必要があります。このように、メディアは標準の CCP を使用してローカルデスクトップ上で処理され、シグナリングおよびコール制御はメディアなしで CCP とのリモート接続で処理されます。Amazon Connect streams API の詳細については、GitHub リポジトリ (https://github.com/aws/amazon-connect-streams) を参照してください。構築するカスタム CCP は、Amazon Connect エージェントが WorkSpaces 内で使用する CCP です。

- WorkSpaces クライアントエンドポイントに、Amazon Connect でサポートされているウェブブラウザがインストールされている必要があります。サポートされているブラウザの一覧については、「Amazon Connect でサポートされるブラウザ」を参照してください。

> **Note**
>
> ユーザーがサポートされていないブラウザを使用している場合、CCP にログインしようとすると、サポートされているブラウザをダウンロードするように求められます。

Amazon Connect オーディオ最適化を有効にする

Amazon Connect オーディオ最適化をユーザーに対して有効にするには:

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Amazon Connect Audio Optimization] (Amazon Connect オーディオ最適化) を展開します。

> **Note**
>
> Amazon Connect で設定する前に、[Update] (更新) をクリックして、以前に管理コンソールで行った未保存の変更を保存します。

5. [Configure Amazon Connect] (Amazon Connect を設定する) を選択します。
6. Amazon Connect の問い合わせコントロールパネル (CCP) の名前を入力します。

> **Note**
>
> CCP を指定した名前は、ユーザーアドインメニューで使用されます。ユーザーにとって意味のある名前を選択してください。

7. Amazon Connect が生成した Amazon Connect の問い合わせコントロールパネルの URL を入力します。URL の取得の詳細については、「問い合わせコントロールパネルへのアクセスを提供する」を参照してください。
8. [Create Amazon Connect] (Amazon Connect を作成) を選択します。

ディレクトリの Amazon Connect オーディオ最適化の詳細を更新する

ディレクトリの Amazon Connect オーディオ最適化の詳細を更新するには:

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Amazon Connect Audio Optimization] (Amazon Connect オーディオ最適化) を展開します。

> **Note**
>
> Amazon Connect で設定する前に、[Update] (更新) をクリックして、以前に管理コンソールで行った未保存の変更を保存します。

5. [Configure Amazon Connect] (Amazon Connect を設定する) を選択します。
6. [Edit] (編集) を選択します。
7. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
8. Amazon Connect の問い合わせコントロールパネル名と URL を更新します。
9. [Save (保存)] を選択します。

ディレクトリの Amazon Connect オーディオ最適化を削除する

ディレクトリの Amazon Connect オーディオ最適化を削除するには:

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Amazon Connect Audio Optimization] (Amazon Connect オーディオ最適化) を展開します。

> **Note**
>
> Amazon Connect で設定する前に、[Update] (更新) をクリックして、以前に管理コンソールで行った未保存の変更を保存します。

5. [Configure Amazon Connect] (Amazon Connect を設定する) を選択します。
6. [Amazon Connect] を選択します。

詳細については、「エージェントトレーニングガイド」を参照してください。

診断ログのアップロードを有効にする

WorkSpaces クライアントの問題をトラブルシューティングするには、診断ログの自動アップロードを有効にします。これは現在、Windows、macOS、および Web Access クライアントでサポートされています。

> **Note**
>
> WorkSpaces クライアント診断ログのアップロード機能は、現在 AWS GovCloud（米国西部) リージョンでは利用できません。

診断ログのアップロード

診断ログのアップロードを使用すると、 WorkSpaces クライアントログファイルを に直接アップロード WorkSpaces して、 WorkSpaces クライアントの使用を中断することなく問題をトラブルシューティングできます。ユーザーの診断ログのアップロードを有効にするか、ユーザー自身で有効にすると、ログファイルは自動的に に送信されます WorkSpaces 。 WorkSpaces ストリーミングセッション前またはストリーミングセッション中に診断ログのアップロードを有効にできます。

管理対象デバイスから診断ログを自動的にアップロードするには、診断アップロードをサポートするクライアントをインストール WorkSpacesします。ログのアップロードはデフォルトで有効になっています。設定は、次のいずれかの方法で変更できます。

オプション 1: AWS コンソールの使用

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 診断ログを有効にするディレクトリ名を選択します。
4. [セルフサービス許可] までスクロールします。
5. 詳細を表示 を選択します。
6. [編集] を選択します。
7. [診断ログのアップロード] を選択します。
8. [保存] を選択します。

オプション 2: API コールを使用する

ディレクトリ設定を編集して、Windows、macOS、および Linux クライアントが WorkSpaces API コールを使用して診断ログを自動的にアップロードするように有効化または無効化できます。有効にすると、クライアントの問題が発生すると、ログはユーザーとのやり取り WorkSpaces なしで に送信されます。詳細については、WorkSpaces 「 API リファレンス」を参照してください。

または、クライアントのインストール後に、診断ログの自動アップロードを有効にするかどうかをユーザーが選択できます。詳細については、WorkSpaces「Windows クライアントアプリケーション」、WorkSpaces macOS クライアントアプリケーション」、およびWorkSpaces「Linux クライアントアプリケーション」を参照してください。

> **Note**
>
> - 診断ログには機密情報は含まれません。ユーザーによって診断ログの自動アップロードをディレクトリレベルで無効にしたり、これらの機能を無効にしたりできます。
> - 診断ログのアップロード機能にアクセスするには、次のバージョンの WorkSpaces クライアントをインストールする必要があります。
>   - Windows クライアントの 5.4.0 以降
>   - macOS クライアントの 5.8.0 以降
>   - Ubuntu 22.04 クライアントの 2023.1
>   - Ubuntu 20.04 クライアントの 2023.1
>   - Web Access クライアントを使用して診断ログのアップロード機能にアクセスすることもできます。

の管理 WorkSpaces

WorkSpaces コンソール WorkSpaces を使用して を管理できます。

ディレクトリ管理タスクを実行するには、「the section called “ディレクトリ管理を設定する”」を参照してください。

> **Note**
>
> - で ENA、NVMe、PV ドライバーなどのネットワーク依存ドライバーを必ず更新してください WorkSpaces。これは、少なくとも 6 か月に 1 回行う必要があります。詳細については、「Elastic Network Adapter (ENA) ドライバー のインストールまたはアップグレードAWS NVMe ドライバー」、「Windows インスタンス 用」、および「Windows インスタンス での PV ドライバーのアップグレード」を参照してください。
> - EC2Config, EC2LaunchEC2Launch V2 エージェントを定期的に最新バージョンに更新してください。これは、少なくとも 6 か月に 1 回行う必要があります。詳細については、「EC2Config と EC2Launch の更新」を参照してください。

内容

- WorkSpace の復元
- Microsoft 365 Bring Your Own License (BYOL)
- ウィンドウズ BYOL のアップグレード WorkSpaces
- の移行 WorkSpace
- WorkSpace の削除

Windows の管理 WorkSpaces

グループポリシーオブジェクト (GPOsを使用して、Windows WorkSpaces または Windows WorkSpaces ディレクトリの一部であるユーザーを管理するための設定を適用できます。

> **Note**
>
> Linux インスタンスはグループポリシーに従いません。Amazon Linux の管理については WorkSpaces、「」を参照してくださいAmazon Linux の管理 WorkSpaces。

WorkSpaces コンピュータオブジェクトの組織単位と WorkSpaces ユーザーオブジェクトの組織単位を作成することをお勧めします。

Amazon に固有のグループポリシー設定を使用するには WorkSpaces、使用しているプロトコルのグループポリシー管理テンプレートを PCoIP または WorkSpaces Streaming Protocol (WSP) のいずれかにインストールする必要があります。

> **Warning**
>
> グループポリシーの設定は、次のように WorkSpace ユーザーのエクスペリエンスに影響を与える可能性があります。
>
> - インタラクティブなログオンメッセージを実装してログオンバナーを表示すると、ユーザーは にアクセスできなくなります WorkSpaces。インタラクティブログオンメッセージグループポリシー設定は、現在 PCoIP WorkSpacesではサポートされていません。ログオンメッセージは WSP でサポートされており WorkSpaces、ユーザーはログオンバナーを受け入れた後に再度ログインする必要があります。
> - グループポリシー設定を使用してリムーバブルストレージを無効にすると、ログインに失敗します。ユーザーはドライブ D にアクセスできず、一時ユーザープロファイルにログインされます。

- グループポリシー設定を使用してリモートデスクトップユーザーのローカルグループからユーザーを削除すると、それらのユーザーはクライアントアプリケーションを通じて認証できなくなります。 WorkSpaces このグループポリシー設定の詳細については、Microsoft のドキュメントのリモートデスクトップサービスによるログオンを許可するを参照してください。
- ローカルセキュリティポリシーでログを許可するから組み込みの Users グループを削除すると、PCoIP WorkSpaces ユーザーは WorkSpaces クライアントアプリケーション WorkSpaces を介して に接続できなくなります。また、PCoIP WorkSpaces は PCoIP エージェントソフトウェアの更新を受信しません。PCoIP エージェントの更新には、セキュリティやその他の修正が含まれている場合や、 の新機能を有効にする場合があります WorkSpaces。このセキュリティポリシーの使用方法の詳細については、Microsoft ドキュメントのローカルでログオンを許可するを参照してください。
- グループポリシー設定は、ドライブアクセスの制限に使用できます。ドライブ C またはドライブ D へのアクセスを制限するようにグループポリシー設定を構成すると、ユーザーはにアクセスできません WorkSpaces。この問題を回避するために、ユーザーがドライブ C およびドライブ D にアクセスできることを確認します。
- WorkSpaces オーディオ入力機能には、 内のローカルログオンアクセスが必要です WorkSpace。Windows では、オーディオ入力機能はデフォルトで有効になっています WorkSpaces。ただし、 でユーザーのローカルログオンを制限するグループポリシー設定がある場合 WorkSpaces、オーディオ入力は では機能しません WorkSpaces。そのグループポリシー設定を削除すると、 の次回の再起動後にオーディオ入力機能が有効になります WorkSpace。このグループポリシー設定の詳細については、Microsoft のドキュメントのローカルでのログオンを許可するをご参照ください。

  オーディオ入力リダイレクトの有効化または無効化の詳細については、PCoIP のオーディオ入力リダイレクトを有効化/無効化する または WSP のオーディオ入力リダイレクトを有効化/無効化する を参照してください。
- グループポリシーを使用して Windows パワープランをバランス型またはパワーセーバーに設定すると WorkSpaces 、アイドル状態のままにすると がスリープ状態になる可能性があります。グループポリシーを使用して、Windows の電源プランを [High performance] (高パフォーマンス) に設定することを強くお勧めします。詳細については、「Windows WorkSpace がアイドル状態のままになるとスリープ状態になる」を参照してください
- グループポリシー設定によっては、セッションから切断されているときに、ユーザーが強制的にログオフされます。ユーザーが で開いているアプリケーション WorkSpaces はすべて閉じられます。

- 「アクティブでアイドル状態のリモートデスクトップサービスセッションの時間制限を設定」は、現在 WSP ではサポートされていません WorkSpaces。WSP セッション中は使用しないでください。アクティビティがあり、セッションがアイドル状態でない場合でも切断が発生するためです。

Active Directory 管理ツールを使用して GPO を操作する方法については、WorkSpaces の Active Directory 管理ツールを設定する を参照してください。

内容

WorkSpaces ストリーミングプロトコル (WSP) のグループポリシー管理テンプレートファイルをインストールする

WorkSpaces ストリーミングプロトコル (WSP) を使用する WorkSpaces ときに に固有のグループポリシー設定を使用するには、WSP のグループポリシー管理テンプレートwsp.admxとwsp.admlファイルを WorkSpaces ディレクトリのドメインコントローラーのセントラルストアに追加する必要があります。.admx および .adml ファイルの詳細については、「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。ディレクトリ管理 WorkSpace またはディレクトリに結合されている Amazon EC2 インスタンスで次の手順を実行します WorkSpaces。

WSP のグループポリシー管理用テンプレートファイルをインストールするには

1. 実行中の Windows から WorkSpace、 C:\Program Files\Amazon\WSP ディレクトリ内の wsp.admxおよび wsp.adml ファイルのコピーを作成します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します\\example.com。
3. sysvol フォルダを開きます。
4. *FQDN* という名前のフォルダを開きます。
5. Policies フォルダを開きます。今、*FQDN*\sysvol*FQDN*\Policies に入っているはずです。
6. まだ存在しない場合は、PolicyDefinitions という名前のフォルダを作成します。
7. PolicyDefinitions フォルダを開きます。
8. wsp.admx ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions フォルダにコピーします。
9. PolicyDefinitions フォルダに en-US という名前のフォルダを作成します。
10. en-US フォルダを開きます。
11. wsp.adml ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US フォルダにコピーします。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト ([フォレスト:*FQDN*]) を展開します。
3. [ドメイン] を展開します。
4. FQDN を展開します (`example.com` など)。
5. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
6. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、委任された権限を持つドメインコンテナの下に GPO を作成してリンクする必要があります。
   > を使用してディレクトリを作成すると AWS Managed Microsoft AD、 はドメインルートの下に *yourdomainname* 組織単位 (OU) AWS Directory Service を作成します。この OU の名前は、ディレクトリの作成時に入力した NetBIOS 名に基づきます。NetBIOS 名を指定しなかった場合、デフォルトでは、Directory DNS 名の最初の部分が使用されます (例えば、`corp.example.com` の場合、NetBIOS 名は `corp` となります)。
   > GPO を作成するには、デフォルトのドメインポリシーを選択する代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。
   > *yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

7. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
8. この WSP グループポリシーオブジェクトを使用して、WSP を使用する WorkSpaces ときに に固有のグループポリシー設定を変更できるようになりました。

WorkSpaces ストリーミングプロトコル (WSP) のグループポリシー設定を管理する

グループポリシー設定を使用して、WSP WorkSpaces を使用する Windows を管理します。

WSP のプリンターサポートを設定する

デフォルトでは、 は基本的なリモート印刷 WorkSpaces を有効にします。これは、ホスト側で汎用プリンタードライバーを使用して互換性のある印刷を行うため、印刷機能が限られています。

Windows クライアントの高度なリモート印刷 (WSP では使用できません) では、両面印刷など、プリンター固有の機能を使用できますが、ホスト側に一致するプリンタードライバーをインストールする必要があります。

リモート印刷は仮想チャネルとして実装されます。仮想チャネルが無効になっている場合、リモート印刷は機能しません。

Windows では WorkSpaces、グループポリシー設定を使用して、必要に応じてプリンターのサポートを設定できます。

プリンターのサポートを設定するには

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできませ

ん。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Configure remote printing] 設定を開きます。
10. [Configure remote printing (リモート印刷を設定)] ダイアログボックスで、次のいずれかを実行します。
    - ローカルプリンタのリダイレクトを有効にするには、[Enabled (有効)] を選択し、[Printing options (印刷オプション)] で [Basic (基本)] を選択します。クライアントコンピュータの現在のデフォルトプリンタを自動的に使用するには、[Map local default printer to the remote host (ローカルデフォルトプリンタをリモートホストにマップする)] を選択します。
    - 印刷を無効にするには、[Disabled (無効)] を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP のクリップボードリダイレクト (コピー/貼り付け) を設定する

デフォルトでは、 は双方向 (コピー/貼り付け) のクリップボードリダイレクト WorkSpaces をサポートします。Windows では WorkSpaces、グループポリシー設定を使用してこの機能を無効にしたり、クリップボードのリダイレクトを許可する方向を設定したりできます。

Windows のクリップボードリダイレクトを設定するには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。

2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Configure clipboard redirection] 設定を開きます。
10. [Configure clipboard redirection] (クリップボードリダイレクトの設定) ダイアログボックスで、[Enabled] (有効) または [Disabled] (無効) を選択します。

    [Configure clipboard redirection] (クリップボードリダイレクトの設定) を [Enabled] (有効) にすると、以下のクリップボードリダイレクトオプションが使用可能になります。

    - [Copy and Paste] (コピーして貼り付ける) では、クリップボードのコピーと貼り付けの双方向リダイレクトを許可します。
    - [Copy Only] (コピーのみ) では、サーバーのクリップボードからクライアントのクリップボードへのデータのコピーのみを許可します。
    - [Paste Only] (貼り付けのみ) では、クライアントのクリップボードからサーバーのクリップボードへのデータの貼り付けのみを許可します。
11. [OK] をクリックします。

12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

既知の制限事項

でクリップボードのリダイレクトを有効にすると WorkSpace、Microsoft Office アプリケーションから 890 KB を超えるコンテンツをコピーすると、アプリケーションが遅くなったり、最大 5 秒間応答しなくなる可能性があります。

WSP のセッション再開タイムアウトを設定する

ネットワーク接続が失われると、アクティブな WorkSpaces クライアントセッションは切断されます。Windows および macOS 用の WorkSpaces クライアントアプリケーションは、ネットワーク接続が一定時間内に復元されると、セッションを自動的に再接続しようとします。デフォルトのセッション再開タイムアウトは 20 分 (1200 秒) ですが、ドメインのグループポリシー設定によって制御 WorkSpaces される の値を変更できます。

自動セッション再起動タイムアウト値を設定するには

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理工ディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable automatic reconnect] (自動再接続を有効/無効にする) 設定を開きます。
10. [Enable/disable automatic reconnect] (自動再接続を有効化/無効化) ダイアログボックスで、[Enabled] (有効) を選択し、[Reconnect timeout (seconds)] (再接続タイムアウト (秒)) を必要なタイムアウト (秒) に設定します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP の動画入力リダイレクトを有効化/無効化する

デフォルトでは、 はローカルカメラからのデータのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のビデオ入力リダイレクトを有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。

2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*`yourdomainname`* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*`yourdomainname`* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable video-in redirection (ビデオ入力リダイレクトを有効/無効にする)] 設定を開きます。
10. [Enable/disable video-in redirection (ビデオ入力リダイレクトを有効/無効にする)] ダイアログボックスで、[Enabled (有効)] または [Disabled (無効)] を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP のオーディオ入力リダイレクトを有効化/無効化する

デフォルトでは、 はローカルマイクからのデータのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable audio-in redirection (オーディオ入力リダイレクトを有効/無効にする)] 設定を開きます。
10. [Enable/disable audio-in redirection (オーディオ入力リダイレクトを有効/無効にする)] ダイアログボックスで、[Enabled (有効)] または [Disabled (無効)] を選択します。

11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション 、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP のオーディオ出力リダイレクトを有効化/無効化する

デフォルトでは、 はローカルスピーカーにデータを WorkSpaces リダイレクトします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のオーディオ出力リダイレクトを有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します WorkSpaces。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を拡張します。例えば `example.com` です。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*`yourdomainname`* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*`yourdomainname`*

OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [オーディオ出力リダイレクトを有効/無効にする] 設定を開きます。
10. [オーディオ出力リダイレクトを有効/無効にする] ダイアログボックスで、[有効] または [無効] を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace。Amazon WorkSpaces コンソールで、 を選択し WorkSpace、アクション > 再起動 WorkSpacesを選択します。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP のタイムゾーンリダイレクトを無効化する

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンをミラーリングするように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のようにさまざまな理由から、タイムゾーンのリダイレクトをオフにすることもできます。例:

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行 WorkSpace することを意図したタスクが にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のタイムゾーンリダイレクトを無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable time zone redirection (タイムゾーンリダイレクトを有効/無効にする)] 設定を開きます。
10. [Enable/disable time zone redirection (タイムゾーンリダイレクトを有効/無効にする)] ダイアログボックスで [Disabled (無効)] を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

- を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
- 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

13. のタイムゾーン WorkSpaces を目的のタイムゾーンに設定します。

のタイムゾーン WorkSpaces が静的になり、クライアントマシンのタイムゾーンがミラーリングされなくなりました。

WSP セキュリティ設定の指定

WSP では、転送中のデータは TLS 1.2 暗号化を使用して暗号化されます。デフォルトでは、次の暗号はすべて暗号化に使用でき、クライアントとサーバーはどちらの暗号を使用するかをネゴシエートします。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

Windows では WorkSpaces、グループポリシー設定を使用して TLS セキュリティモードを変更し、特定の暗号スイートを新規追加またはブロックできます。これらの設定とサポートされている暗号スイートの詳細については、[PCoIP セキュリティ設定の構成] グループポリシーダイアログボックスを参照してください。

WSP セキュリティ設定を構成するには

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を拡張します。例えば `example.com` です。

6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [セキュリティ設定の構成] を開きます。
10. [セキュリティ設定の構成] ダイアログボックスで、[有効] を選択します。許可する暗号スイートを追加し、ブロックする暗号スイートを削除します。これらの設定の詳細については、[セキュリティ設定の構成] ダイアログボックスに表示される説明を参照してください。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動するには WorkSpace、Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション 、再起動 WorkSpacesを選択します。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP の拡張機能を設定する

デフォルトでは、 WorkSpaces 拡張機能のサポートは無効になっています。必要に応じて、次の方法で拡張機能を使用する WorkSpace ように を設定できます。

- サーバーとクライアント – サーバーとクライアントの両方の拡張機能を有効にする

- サーバーのみ – サーバーのみの拡張機能を有効にする
- クライアントのみ – クライアントのみの拡張機能を有効にする

Windows では WorkSpaces、グループポリシー設定を使用して拡張機能の使用を設定できます。

WSP の拡張機能を設定するには

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します WorkSpaces。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を拡張します。例えば、次のようになります: `example.com`
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*`yourdomainname`* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*`yourdomainname`* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理工ディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [拡張機能の設定] を開きます。
10. [拡張機能の設定] ダイアログボックスで、[有効] を選択し、必要なサポートオプションを設定します。[クライアントのみ]、[サーバーとクライアント]、または [サーバーのみ] を選択します。
11. [OK] をクリックします。

12. グループポリシー設定の変更は、 の次回のグループポリシー更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace。Amazon WorkSpaces コンソールで、 を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP のスマートカードリダイレクトを有効化/無効化する

デフォルトでは、Amazon WorkSpaces はセッション前認証またはセッション内認証 のいずれにもスマートカードの使用をサポートしていません。セッション前認証とは、ユーザーが にログインしている間に実行されるスマートカード認証を指します WorkSpaces。セッション内認証とは、ログイン後に実行される認証をいいます。

必要に応じて、グループポリシー設定 WorkSpaces を使用して、Windows のセッション前認証とセッション内認証を有効にできます。また、セッション前認証は、 EnableClientAuthentication API アクションまたは enable-client-authentication AWS CLI コマンドを使用して AD Connector ディレクトリ設定を通じて有効にする必要があります。詳細については、AWS Directory Service 管理ガイドの AD Connector のスマートカード認証を有効にするを参照してください。

> **Note**
>
> Windows でスマートカードを使用できるようにするには WorkSpaces、追加の手順が必要です。詳細については、「認証にスマートカードを使用する」を参照してください。

Windows のスマートカードリダイレクトを有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。

7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable smart card redirection] (スマートカードリダイレクトを有効/無効にする) 設定を開きます。
10. [Enable/disable smart card redirection] (スマートカードリダイレクトを有効/無効にする) ダイアログボックスで、[Enabled] (有効) または [Disabled] (無効) を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、セッションの WorkSpace再起動後に有効になります。グループポリシーの変更を適用するには、 を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション 、再起動 WorkSpacesを選択します) 。

WSP の WebAuthn (FIDO2) リダイレクトを有効または無効にする

デフォルトでは、Amazon WorkSpaces はセッション内認証に WebAuthn 認証機能を使用できます。セッション内認証とは、ログイン後に実行され、セッション内で実行されているウェブアプリケーションによってリクエストされる WebAuthn 認証を指します。

要件

WebAuthn WSP の (FIDO2) リダイレクトには、以下が必要です。

- WSP ホストエージェントバージョン 2.0.0.1425 以降
- WorkSpaces クライアント :

  - Linux Ubuntu 22.04 2023.3 以降
  - Windows 5.19.0 以降
  - Mac クライアント 5.19.0 以降
- Amazon DCV リダイレクト拡張機能 WorkSpaces を実行している WebAuthn にインストールされているウェブブラウザ：
  - Google Chrome 116 以降
  - Microsoft Edge 116 以降

Windows の WebAuthn (FIDO2) リダイレクトの有効化または無効化 WorkSpaces

必要に応じて、グループポリシー設定を使用して、Windows の WebAuthn 認証機関によるセッション内認証のサポート WorkSpaces を有効または無効にできます。この設定を有効にするか、設定しない場合、 WebAuthn リダイレクトが有効になり、ユーザーはリモート 内でローカル認証を利用できるようになります WorkSpace。

機能を有効にすると、セッション内のブラウザからのすべての WebAuthn リクエストがローカルクライアントにリダイレクトされます。ユーザーは、Windows Hello、 などのローカルにアタッチされたセキュリティデバイス YubiKey 、またはその他の FIDO2 準拠の認証ツールを使用して、認証プロセスを完了できます。

Windows の WebAuthn (FIDO2) リダイレクトを有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. WebAuthn リダイレクトの有効化/無効化設定を開きます。
10. WebAuthn リダイレクトの有効化/無効化ダイアログボックスで、有効化または無効化を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 WorkSpace セッションの再起動後に有効になります。グループポリシーの変更を適用するには、Amazon WorkSpaces コンソール WorkSpace に移動し、 を選択して を再起動します WorkSpace。次に、アクション 、再起動) WorkSpacesを選択します。

Amazon DCV WebAuthn リダイレクト拡張機能のインストール

次のいずれかを実行して、この機能を有効に WebAuthn した後、使用する Amazon DCV WebAuthn リダイレクト拡張機能をインストールする必要があります。

- ユーザーはブラウザでブラウザ拡張機能を有効にするように求められます。

> **Note**
>
> これは 1 回限りのブラウザプロンプトです。WSP エージェントのバージョンを 2.0.0.1425 以降に更新すると、ユーザーに通知が送信されます。エンドユーザーが WebAuthn リダイレクトを必要としない場合は、ブラウザから拡張機能を削除できます。

以下の GPO WebAuthn ポリシーを使用して、リダイレクト拡張機能のインストールプロンプトをブロックすることもできます。

- 以下の GPO ポリシーを使用して、ユーザーにリダイレクト拡張機能を強制インストールできます。GPO ポリシーを有効にすると、ユーザーがインターネットアクセスでサポートされているブラウザを起動すると、拡張機能が自動的にインストールされます。
- ユーザーは、Microsoft Edge アドオンまたは Chrome Web Store を使用して拡張機能を手動でインストールできます。

グループポリシーを使用してブラウザ拡張機能を管理およびインストールする

Amazon DCV WebAuthn リダイレクト拡張機能は、Active Directory (AD) ドメインに参加しているセッションホストのドメインから一元的にインストールするか、セッションホストごとにローカルグループポリシーエディタを使用してインストールできます。このプロセスは、使用しているブラウザによって異なります。

Microsoft Edge の場合

1. Microsoft Edge 管理テンプレート をダウンロードしてインストールします。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
8. コンピュータ設定 、管理テンプレート 、Microsoft Edge 、および拡張機能を選択する
9. 拡張機能管理設定の構成 を開き、それを有効に設定します。
10. 拡張機能管理設定の構成 で、次のように入力します。

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. [OK] をクリックします。

12. グループポリシー設定の変更は、 WorkSpace セッションの再起動後に有効になります。グループポリシーの変更を適用するには、Amazon WorkSpaces コンソール WorkSpace に移動し、を選択して を再起動します WorkSpace。次に、アクション 、再起動) WorkSpacesを選択します。

> **Note**
>
> 次の設定管理設定を適用することで、拡張機能のインストールをブロックできます。
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

Google Chrome の場合

1. Google Chrome 管理テンプレートをダウンロードしてインストールします。詳細については、「マネージド PCs」を参照してください。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:***FQDN***]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
8. コンピュータ設定 、管理テンプレート 、Google Chrome 、拡張機能 を選択します。
9. 拡張機能管理設定の構成 を開き、それを有効に設定します。
10. 拡張機能管理設定の構成 で、次のように入力します。

    ```
    {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
    { "installation_mode":"force_installed","update_url":"https://clients2.google.com/
    service/update2/crx"}}
    ```

11. [OK] をクリックします。

12. グループポリシー設定の変更は、 WorkSpace セッションの再起動後に有効になります。グループポリシーの変更を適用するには、Amazon WorkSpaces コンソール WorkSpace に移動し、を選択して を再起動します WorkSpace。次に、アクション 、再起動) WorkSpacesを選択します。

> **Note**
>
> 次の設定管理設定を適用することで、拡張機能のインストールをブロックできます。
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

WSP の画面ロックの場合のセッションの切断を有効化/無効化する

必要に応じて、Windows ロック画面が検出されたときにユーザーの WorkSpaces セッションを切断できます。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、 で有効になっている認証のタイプに応じて、自分自身を認証できます WorkSpaces。

このグループポリシー設定は、デフォルトでは無効になっています。必要に応じて、グループポリシー設定 WorkSpaces を使用して、Windows の Windows ロック画面が検出されたときにセッションの切断を有効にできます。

> **Note**
>
> - このグループポリシー設定は、パスワード認証セッションとスマートカード認証セッションの両方に適用されます。
> - Windows でスマートカードを使用できるようにするには WorkSpaces、追加の手順が必要です。詳細については、「認証にスマートカードを使用する」を参照してください。

Windows の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。

2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [Enable/disable disconnect session on screen lock] (画面ロックの場合のセッションの切断を有効/無効にする) 設定を開きます。
10. [Enable/disable disconnect session on screen lock] (画面ロックの場合のセッションの切断を有効/無効にする) ダイアログボックスで、[Enabled] (有効) または [Disabled] (無効) を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

WSP の間接ディスプレイドライバー (IDD) を有効または無効にする

デフォルトでは、 WorkSpaces は間接ディスプレイドライバー (IDD) の使用をサポートしています。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows の間接ディスプレイドライバー (IDD) を有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 WorkSpaces ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon Elastic Compute Cloud インスタンスで、グループポリシー管理ツール (gpmc.msc) を開きます。
3. フォレスト (フォレスト: FQDN) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. デフォルトドメインポリシー を選択し、メニューを右クリックしてコンテキストを開き、編集を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリである場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、`yourdomainname`組織単位 (OU) またはそのドメイン名の下にある任意の OU を選択し、メニューを右クリックしてコンテキストを開き、このドメインに GPO を作成するを選択し、ここでリンクします。OU の詳細については、`yourdomainname` AWS 「 Directory Service 管理ガイド」の「作成内容https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_what_gets_created.html」を参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. AWS 「間接ディスプレイドライバーを有効にする」設定を開きます。

10. AWS 「間接ディスプレイドライバーを有効にする」ダイアログボックスで、「有効」または「無効」を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    a. を再起動します WorkSpace （ WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します ）。

    b. 管理コマンドプロンプトで、`gpupdate /force` と入力します。

WSP の表示設定の構成

WorkSpaces では、最大フレームレート、最小画質、最大画質、YUV エンコーディングなど、複数の異なる表示設定を設定できます。これらの設定は、必要な画質、応答性、色精度に基づいて調整します。

デフォルトでは、最大フレームレートの値は 25 です。最大フレームレートの値は、1 秒あたりの最大許容フレーム数 (fps) を指定します。値を 0 にすると、無制限に設定されます。

デフォルトでは、最小画質の値は 30 です。最小画質は、最善の画像応答性、つまり最善の画質になるように最適化できます。最善の応答性を実現するには、最小品質を下げます。最善の品質を実現するには、最小品質を上げます。

- 最善の応答性を実現する理想的な値は、30～90 です。
- 最適な品質を実現する理想的な値は、60～90 です。

デフォルトでは、最低画質の値は 80 です。最大画質は画像の応答性や画質には影響しませんが、最大値を設定してネットワークの使用を制限します。

デフォルトでは、画像エンコーディングは YUV420 に設定されています。[YUV444 エンコーディングを有効にする] を選択すると、YUV444 エンコーディングが有効になり、高い色精度が得られます。

Windows では WorkSpaces、グループポリシー設定を使用して、最大フレームレート、最小画質、最大画質値を設定できます。

Windows の表示設定を構成するには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します WorkSpaces。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [ディスプレイ設定の構成] を開きます。
10. [ディスプレイ設定] ダイアログボックスで [有効] を選択し、[最大フレームレート (fps)]、[最小画質]、[最大画質] の各値を目的のレベルに設定します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次回のグループポリシー更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace。Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション 、再起動 WorkSpacesを選択します。

- 管理コマンドプロンプトで、**gpupdate /force** と入力します。

WSP の AWS 仮想ディスプレイ専用ドライバーの VSync を有効または無効にする

デフォルトでは、 は AWS 仮想ディスプレイ専用ドライバーの VSync 機能の使用 WorkSpaces をサポートしています。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

VSync for Windows を有効または無効にするには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 WorkSpaces ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon Elastic Compute Cloud インスタンスで、グループポリシー管理ツール (gpmc.msc) を開きます。
3. フォレストを展開します (フォレスト: FQDN) 。
4. [ドメイン] を展開します。
5. FQDN を展開します (`example.com` など)。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. デフォルトドメインポリシー を選択し、メニューを右クリックしてコンテキストを開き、編集を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリである場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、`yourdomainname`組織単位 (OU) またはそのドメイン名の下にある任意の OU を選択し、メニューを右クリックしてコンテキストを開き、このドメインに GPO を作成するを選択し、ここでリンクします。OU の詳細については、`yourdomainname`AWS 「 Directory Service 管理ガイド」の「作成内容」を参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. AWS 仮想表示専用ドライバー設定の VSync を有効にする機能を開きます。

10. AWS 仮想表示専用ドライバーの VSync を有効にするダイアログボックスで、有効または無効を選択します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次の手順を実行します。

    a. 次のいずれか WorkSpace を実行して、 を再起動します。

        i. オプション 1 — WorkSpaces コンソールで、再起動する WorkSpace を選択します。次に、アクション 、再起動 WorkSpacesを選択します。

        ii. オプション 2 — 管理コマンドプロンプトで、 と入力しますgpupdate /force。

    b. 設定を適用する WorkSpace には、 に再接続します。

    c. Workspace を再起動します。

WSP のログ詳細度の設定

デフォルトでは、WSP のログ詳細レベル WorkSpaces は情報 に設定されます。ログレベルは、以下のように詳細度の低いものから最も詳細なものまで設定できます。

- エラー – 最も低い詳細度
- 警告
- 情報 – デフォルト
- デバッグ – 最も高い詳細度

Windows では WorkSpaces、グループポリシー設定を使用してログの詳細レベルを設定できます。

Windows のログの詳細レベルを設定するには WorkSpaces

1. WorkSpaces WSP の最新のグループポリシー管理テンプレートが、 ディレクトリのドメインコントローラーのセントラルストアにインストールされていることを確認します WorkSpaces。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト ([フォレスト:*FQDN*]) を展開します。
4. [ドメイン] を展開します。

5. FQDN を拡張します。例えば `example.com` です。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。*yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

8. グループポリシー管理エディタで、[Computer Configuration (コンピュータの設定)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Amazon]、[WSP] の順に選択します。
9. [ログ詳細度の設定] を開きます。
10. [ログ詳細度の設定] ダイアログボックスで、[有効] を選択し、ログの詳細度レベルを、[デバッグ]、[エラー]、[情報]、または [警告] に設定します。
11. [OK] をクリックします。
12. グループポリシー設定の変更は、 の次回のグループポリシー更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace。Amazon WorkSpaces コンソールで、 を選択し WorkSpace、アクション 、再起動 WorkSpacesを選択します。
    - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

PCoIP のグループポリシー管理用テンプレートをインストールする

PCoIP プロトコルを使用する WorkSpaces ときに Amazon に固有のグループポリシー設定を使用するには、 に使用されている PCoIP エージェント (32 ビットまたは 64 ビット) のバージョンに適したグループポリシー管理テンプレートを追加する必要があります WorkSpaces。

> **Note**
>
> を 32 ビットエージェントと 64 ビットエージェント WorkSpaces と混在させる場合は、32 ビットエージェントのグループポリシー管理テンプレートを使用できます。グループポリシー設定は 32 ビットエージェントと 64 ビットエージェントの両方に適用されます。すべての WorkSpaces が 64 ビットエージェントを使用している場合は、64 ビットエージェントの管理テンプレートの使用に切り替えることができます。

に 32 WorkSpaces ビットエージェントまたは 64 ビットエージェントがあるかどうかを確認するには

1. にログインし WorkSpace、表示、Ctrl + Alt + 削除 を選択するか、タスクバーを右クリックしてタスクマネージャー を選択してタスクマネージャーを開きます。
2. タスクマネージャで、[詳細] タブに移動し、列見出しを右クリックし、[列の選択] を選択します。
3. [列の選択] ダイアログボックスで、[プラットフォーム] を選択し、[OK] をクリックします。
4. [詳細] タブで、`pcoip_agent.exe` を探し、[プラットフォーム] 列でその値を確認し、PCoIP エージェントが 32 ビットであるか 64 ビットであるか判別します。(32 ビットと 64 ビットの WorkSpaces コンポーネントが混在している場合があります。これは正常です。)

PCoIP のグループポリシー管理用テンプレートをインストールする (32 ビット)

32 ビット PCoIP エージェントで PCoIP プロトコルを使用する WorkSpaces ときに に固有のグループポリシー設定を使用するには、PCoIP PCoIP のグループポリシー管理テンプレートをインストールする必要があります。ディレクトリ管理 WorkSpace またはディレクトリに参加している Amazon EC2 インスタンスで次の手順を実行します。

.adm ファイルの操作の詳細については、マイクロソフトのドキュメントの「グループポリシー管理用テンプレート (.adm) ファイルを管理するための推奨事項」を参照してください。

PCoIP のグループポリシー管理用テンプレートをインストールするには

1. 実行中の Windows から WorkSpace、 `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` ディレクトリに `pcoip.adm` ファイルのコピーを作成します。

2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、 WorkSpaces マシンアカウントを含むドメイン内の組織単位に移動します。
3. コンピュータアカウントの組織単位のコンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and link it here] を選択します。
4. 「新しい GPO」ダイアログボックスに、WorkSpaces マシンポリシー などの GPO のわかりやすい名前を入力し、ソーススターター GPO を （ なし ） に設定します。[OK] をクリックします。
5. 新しい GPO のコンテキスト (右クリック) メニューを開き、[Edit] を選択します。
6. グループポリシー管理エディタで、[Computer Configuration]、[Policies]、[Administrative Templates] の順に選択します。メインメニューから [Action]、[Add/Remove Templates] の順に選択します。
7. [Add/Remove Templates] ダイアログボックスで、[Add] を選択し、先ほどコピーした `pcoip.adm` ファイルを選択したら、[Open]、[Close] の順に選択します。
8. [Group Policy Management Editor] を終了します。この GPO を使用して、 に固有のグループポリシー設定を変更できるようになりました WorkSpaces。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、 WorkSpaces マシンアカウントの GPO に移動して選択します WorkSpaces。メインメニューの [Action]、[Edit] を選択します。
2. グループポリシー管理エディタで、[Computer Configuration]、[Policies]、[Administrative Templates]、[Classic Administrative Templates]、[PCoIP Session Variables] の順に選択します。
3. この PCoIP セッション可変グループポリシーオブジェクトを使用して、PCoIP を使用する WorkSpaces ときに Amazon に固有のグループポリシー設定を変更できるようになりました。

> **Note**
>
> ユーザーによる設定の上書きを許可するには、[Overridable Administrator Settings] (上書き可能な管理者設定) を選択します。許可しない場合は、[Not Overridable Administrator Settings] (上書き可能でない管理者設定) を選択します。

PCoIP のグループポリシー管理用テンプレートをインストールする (64 ビット)

PCoIP プロトコルを使用する WorkSpaces ときに に固有のグループポリシー設定を使用するには、PCoIP のグループポリシー管理テンプレートPCoIP.admxとPCoIP.admlファイルをディレクトリのドメインコントローラー WorkSpacesのセントラルストアに追加する必要があります。.admx および .adml ファイルの詳細については、「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。 WorkSpaces ディレクトリ管理 WorkSpace またはディレクトリに結合されている Amazon EC2 インスタンスで次の手順を実行します。

PCoIP のグループポリシー管理用テンプレートファイルをインストールするには

1. 実行中の Windows から WorkSpace、 C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions ディレクトリ内の PCoIP.admxおよび PCoIP.adml ファイルのコピーを作成します。PCoIP.admlファイルは、そのディレクトリの en-US サブフォルダにあります。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します\\example.com。
3. sysvol フォルダを開きます。
4. *FQDN* という名前のフォルダを開きます。
5. Policies フォルダを開きます。今、*FQDN*\sysvol*FQDN*\Policies に入っているはずです。
6. まだ存在しない場合は、PolicyDefinitions という名前のフォルダを作成します。
7. PolicyDefinitions フォルダを開きます。
8. PCoIP.admx ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions フォルダにコピーします。
9. PolicyDefinitions フォルダに en-US という名前のフォルダを作成します。
10. en-US フォルダを開きます。
11. PCoIP.adml ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US フォルダにコピーします。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト ([フォレスト:*FQDN*]) を展開します。
3. [ドメイン] を展開します。
4. FQDN を展開します (`example.com` など)。
5. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
6. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して GPO を作成することはできません。代わりに、委任された権限を持つドメインコンテナの下に GPO を作成してリンクする必要があります。
   > を使用してディレクトリを作成すると AWS Managed Microsoft AD、 はドメインルートの下に *yourdomainname* 組織単位 (OU) AWS Directory Service を作成します。この OU の名前は、ディレクトリの作成時に入力した NetBIOS 名に基づきます。NetBIOS 名を指定しなかった場合、デフォルトでは、Directory DNS 名の最初の部分が使用されます (例えば、`corp.example.com` の場合、NetBIOS 名は `corp` となります)。
   > GPO を作成するには、デフォルトのドメインポリシーを選択する代わりに、*yourdomainname* OU (またはその下にある任意の OU) を選択し、コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, and Link it here] (このドメインに GPO を作成し、ここにリンクする) を選択します。
   > *yourdomainname* OU の詳細については、AWS Directory Service 管理ガイドの作成されるものを参照してください。

7. グループポリシー管理エディタで、[コンピュータの設定]、[ポリシー]、[管理用テンプレート]、[PCoIP セッション変数] の順に選択します。
8. この PCoIP セッション可変グループポリシーオブジェクトを使用して、PCoIP を使用する WorkSpaces ときに に固有のグループポリシー設定を変更できるようになりました。

> **Note**
>
> ユーザーによる設定の上書きを許可するには、[Overridable Administrator Settings] (上書き可能な管理者設定) を選択します。許可しない場合は、[Not Overridable Administrator Settings] (上書き可能でない管理者設定) を選択します。

PCoIP のグループポリシー設定を管理する

グループポリシー設定を使用して、PCoIP WorkSpaces を使用する Windows を管理します。 PCoIP

PCoIP のプリンタサポートを設定する

デフォルトでは、 は基本的なリモート印刷 WorkSpaces を有効にします。これは、互換性のある印刷を確保するためにホスト側で汎用プリンタードライバーを使用するため、印刷機能が限られています。

Windows クライアントの高度なリモート印刷では、両面印刷など、プリンター固有の機能を使用できますが、ホスト側に一致するプリンタードライバーをインストールする必要があります。

リモート印刷は仮想チャネルとして実装されます。仮想チャネルが無効になっている場合、リモート印刷は機能しません。

Windows では WorkSpaces、グループポリシー設定を使用して、必要に応じてプリンターのサポートを設定できます。

プリンターのサポートを設定するには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure remote printing] 設定を開きます。
4. [Configure remote printing (リモート印刷を設定)] ダイアログボックスで、次のいずれかを実行します。

- 高度なリモート印刷を有効にするには、[Enabled (有効)] を選択し、[Options (オプション)] の [Configure remote printing (リモート印刷を設定)] で [Basic and Advanced printing for Windows clients (Windows クライアントの基本印刷と高度な印刷)] を選択します。クライアントコンピュータの現在のデフォルトプリンターを自動的に使用するには、[Automatically set default printer (デフォルトプリンターを自動的に設定する)] を選択します。
- 印刷を無効にするには、[Enabled (有効)] を選択し、[Options (オプション)] の [Configure remote printing (リモート印刷を設定)] で [printing disabled (印刷無効)] を選択します。

5. [OK] をクリックします。
6. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

デフォルトでは、ローカルプリンターへの自動リダイレクトは無効になっています。グループポリシー設定を使用してこの機能を有効にし、 に接続するたびにローカルプリンターをデフォルトプリンターとして設定できます WorkSpace。

> **Note**
>
> ローカルプリンターリダイレクトは、Amazon Linux では使用できません WorkSpaces。

ローカルプリンターへの自動リダイレクトを有効にするには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure remote printing] 設定を開きます。
4. [Enabled] (有効) を選択し、[Options] (オプション) の [Configure remote printing] (リモート印刷を設定) で、次のいずれかを選択します。

- Basic and Advanced printing for Windows clients (Windows クライアント用の基本印刷と高度な印刷)
- Basic printing (基本印刷)

5. [Automatically set default printer] (デフォルトのプリンターを自動的に設定) を選択し、[OK] を選択します。
6. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

PCoIP のクリップボードリダイレクト (コピー/貼り付け) を有効または無効にする

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

クリップボードのリダイレクトを有効または無効にするには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure clipboard redirection] 設定を開きます。
4. [Configure clipboard redirection (クリップボードのリダイレクトの設定)] ダイアログボックスで、[有効] を選択し、次のいずれかの設定を選択して、クリップボードのリダイレクトが許可される方向を決定します。終了したら、[OK] を選択します。

   - 双方向で無効
   - エージェントからクライアントのみ (ローカルコンピュータWorkSpace へ) を有効にしました
   - クライアントからエージェントのみ (ローカルコンピュータから WorkSpace) を有効にしました

- 双方向で有効

5. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

既知の制限事項

でクリップボードのリダイレクトを有効にすると WorkSpace、Microsoft Office アプリケーションから 890 KB を超えるコンテンツをコピーすると、アプリケーションが遅くなったり、最大 5 秒間応答しなくなる可能性があります。

PCoIP のセッション再開タイムアウトを設定する

ネットワーク接続が失われると、アクティブな WorkSpaces クライアントセッションは切断されます。Windows および macOS 用の WorkSpaces クライアントアプリケーションは、ネットワーク接続が一定時間内に復元されると、セッションを自動的に再接続しようとします。デフォルトのセッション再開タイムアウトは 20 分ですが、ドメインのグループポリシー設定によって制御 WorkSpaces される の値を変更できます。

自動セッション再起動タイムアウト値を設定するには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure Session Automatic Reconnection Policy] 設定を開きます。
4. [Configure Session Automatic Reconnection Policy] ダイアログボックスで [Enabled] を選択し、[Configure Session Automatic Reconnection Policy] オプションを必要なタイムアウト値 (分単位) に設定して、[OK] を選択します。

5. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

PCoIP のオーディオ入力リダイレクトを有効化/無効化する

デフォルトでは、Amazon はローカルマイクからのデータのリダイレクト WorkSpaces をサポートしています。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

> **Note**
>
> でユーザーのローカルログオンを制限するグループポリシー設定がある場合 WorkSpaces、オーディオ入力は では機能しません WorkSpaces。そのグループポリシー設定を削除すると、 の次回の再起動後にオーディオ入力機能が有効になります WorkSpace。このグループポリシー設定の詳細については、Microsoft のドキュメントの「ローカルでのログオンを許可する」をご参照ください。

オーディオ入力リダイレクトを有効または無効にするには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション可変 に移動します。
3. [Enable/disable audio in the PCoIP session] (PCoIP セッションでのオーディオ入力を有効/無効にする) 設定を開きます。
4. [Enable/disable audio in the PCoIP session] (PCoIP セッションでのオーディオ入力を有効/無効にする) ダイアログボックスで、[Enabled] (有効) または [Disabled] (無効) を選択します。
5. [OK] をクリックします。

6. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

PCoIP のタイムゾーンリダイレクトを無効化する

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンをミラーリングするように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のようにさまざまな理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行 WorkSpace することを意図したタスクが にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

タイムゾーンのリダイレクトを無効にするには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure timezone redirection] (タイムゾーンリダイレクトを構成) の設定を開きます。
4. [Configure timezone redirection] (タイムゾーンリダイレクトを設定) ダイアログボックスで [Disabled] (無効) を選択します。

5. [OK] をクリックします。
6. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。
7. のタイムゾーン WorkSpaces を目的のタイムゾーンに設定します。

のタイムゾーン WorkSpaces が静的になり、クライアントマシンのタイムゾーンがミラーリングされなくなりました。

PCoIP セキュリティ設定を構成する

PCoIP については、転送中のデータは、TLS 1.2 暗号化と SigV4 リクエスト署名を使用して暗号化されます。PCoIP プロトコルは、AES で暗号化された UDP トラフィックをストリーミングピクセルに使用します。ポート 4172 (TCP および UDP) を使用するストリーミング接続は、AES-128 および AES-256 暗号を使用して暗号化されますが、暗号化はデフォルトで 128 ビットとなります。このデフォルトを 256 ビットに変更するには、[Configure PCoIP Security Settings] (PCoIP セキュリティ設定を構成) グループポリシー設定を使用します。

このグループポリシー設定を使用して、TLS セキュリティモードを変更し、特定の暗号スイートをブロックすることもできます。これらの設定とサポートされている暗号スイートの詳細については、[Configure PCoIP Security Settings] (PCoIP セキュリティ設定を構成) グループポリシーダイアログボックスを参照してください。

PCoIP セキュリティ設定を構成するには

1. WorkSpaces PCoIP 用の最新のグループポリシー管理テンプレート (32 ビット) または WorkSpaces PCoIP 用のグループポリシー管理テンプレート (64 ビット) がインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Configure PCoIP Security Settings] (PCoIP セキュリティ設定を構成) の設定を開きます。

4. [Configure PCoIP Security Settings] (PCoIP セキュリティ設定を構成) ダイアログボックスで、[Enabled] (有効) を選択します。ストリーミングトラフィックのデフォルトの暗号化を 256 ビットに設定するには、[PCoIP Data Encryption Ciphers] (PCoIP データ暗号化暗号) オプションに移動し、[AES-256-GCM only] (AES-256-GCM のみ) を選択します。
5. (オプション) TLS セキュリティモードの設定を調整し、ブロックする暗号スイートをリストします。これらの設定の詳細については、[Configure PCoIP Security Settings] (PCoIP セキュリティ設定を構成) ダイアログボックスに表示される説明を参照してください。
6. [OK] をクリックします。
7. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

U2F の YubiKey USB リダイレクトを有効にする

> **Note**
>
> Amazon WorkSpaces は現在、 YubiKey U2F でのみ USB リダイレクトをサポートしています。他のタイプの USB デバイスもリダイレクトされる場合がありますが、それらはサポートされていないため、正常に動作しない可能性があります。

YubiKey U2F の USB リダイレクトを有効にするには

1. WorkSpaces PCoIP (32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP 64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIP セッション変数 に移動します。
3. [Enable/disable USB in the PCOIP session] (PCoIP セッションでの USB を有効/無効にする) 設定を開きます。
4. [Enabled] (有効)、[OK] の順に選択します。

5. [Configure PCoIP USB allowed and unallowed device rules] (PCoIP USB の許可および許可されないデバイスのルール設定) を開きます。
6. [有効] を選択し、[USB 認証テーブルを入力 (最大 10 個のルール)] で、USB デバイスの許可リストルールを設定します。

   - 承認ルール - 110500407。この値は、ベンダー ID (VID) と製品 ID (PID) の組み合わせです。VID/PID の組み合わせの形式は 1xxxxyyyy です。xxxx は 16 進形式の VID で、yyyy は 16 進形式の PID です。この例では、1050 が VID で、0407 が PID です。USB 値の詳細については、 YubiKey YubiKey 「USB ID 値」を参照してください。
7. [USB 認証テーブルを入力 (最大 10 個のルール)] で、USB デバイスのブロックリストルールを設定します。

   - [Unauthorization Rule] (非承認ルール) に、空の文字列を設定します。これは、承認リスト内の USB デバイスだけが許可されることを意味します。

   > **Note**
   >
   > USB 承認ルールと USB 非承認ルールをそれぞれ最大 10 個定義することができます。複数のルールを区切るには、縦棒 (|) 文字を使用します。承認ルールと非承認ルールの詳細については、Teradici PCoIP Standard Agent for Windows を参照してください。

8. [OK] をクリックします。
9. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

設定を有効にすると、USB デバイスルール設定で制限が設定され WorkSpaces ていない限り、サポートされているすべての USB デバイスは にリダイレクトできます。

Kerberos チケットの最大ライフタイムを設定する

Windows の「記憶する」機能を無効にしていない場合 WorkSpaces、 WorkSpace ユーザーは WorkSpaces クライアントアプリケーションの「記憶する」または「ログインしたまま」チェック

ボックスを使用して認証情報を保存できます。この機能により、ユーザーはクライアントアプリケーションの実行中に簡単に に接続できます WorkSpaces。認証情報は、ユーザーの Kerberos チケットの最大有効期間が終了するまで安全にキャッシュに保存されます。

で AD Connector ディレクトリ WorkSpace を使用している場合は、Microsoft Windows ドキュメントの WorkSpaces 「ユーザーチケットの最大有効期間」の手順に従って、グループポリシーを通じてユーザーの Kerberos チケットの最大有効期間を変更できます。

[Remember Me] (このアカウントを記憶する) 機能を有効または無効にする方法については、ユーザーのセルフサービス WorkSpace管理機能を有効にする を参照してください。

インターネットアクセス用のデバイスプロキシサーバー設定を構成する

デフォルトでは、 WorkSpaces クライアントアプリケーションは HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定されているプロキシサーバーを使用します。Amazon WorkSpaces クライアントアプリケーションは、更新、登録、認証に HTTPS ポートを使用します。

> **Note**
>
> サインイン認証情報を使用した認証を必要とするプロキシサーバーはサポートされていません。

Microsoft ドキュメントの「デバイスプロキシとインターネット接続の設定を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Windows のデバイスプロキシサーバー設定を設定できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

WorkSpaces Windows クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces macOS クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces Web Access クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

デスクトップトラフィックのプロキシ

PCoIP WorkSpaces の場合、デスクトップクライアントアプリケーションは、UDP のポート 4172 トラフィック (デスクトップトラフィックの場合) のプロキシサーバーの使用や TLS 復号化および検査をサポートしていません。ポート 4172 に直接接続する必要があります。

WSP の場合 WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート 4195 TCP トラフィックの HTTP プロキシサーバーの使用をサポートしています。TLS の復号および検査はサポートしていません。

WSP は、UDP 経由のデスクトップトラフィックに対するプロキシの使用をサポートしていません。TCP WorkSpacesトラフィックのプロキシの使用をサポートしているのは、Windows および macOS デスクトップクライアントアプリケーションと WSP ウェブアクセスのみです。

> **Note**
>
> プロキシサーバーを使用する場合、クライアントアプリケーションが WorkSpaces サービスに対して行う API コールもプロキシされます。API コールとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイテンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket (TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響を与える可能性があります。

プロキシを使用する必要がある場合は、ストリーミングの品質と応答性に悪影響を及ぼす可能性のあるネットワークレイテンシーを追加しないように、プロキシサーバーを WorkSpace可能な限りクライアントの近く、できれば同じネットワーク内に配置してください。

Amazon WorkSpaces for Zoom 会議メディアプラグインのサポートを有効にする

Zoom は、Zoom VDI プラグインを使用して WorkSpaces、WSP および PCoIP Windows ベースの向けに最適化されたリアルタイム通信をサポートします。クライアントとの直接通信により、ビデオ通話はクラウドベースの仮想デスクトップをバイパスし、ユーザーの 内で会議が実行されているときにローカルのような Zoom エクスペリエンスを提供できます WorkSpace。

WSP の Zoom Meeting Media Plugin を有効にする

Zoom VDI コンポーネントをインストールする前に、Zoom 最適化をサポートするように WorkSpaces 設定を更新します。

前提条件

プラグインを使用する前に、次の要件が満たされていることを確認してください。

- Windows WorkSpaces クライアントバージョン 5.10.0 以降と Zoom VDI プラグインバージョン 5.17.10 以降
- 内 WorkSpaces — Zoom VDI Meeting クライアントバージョン 5.17.10 以降

開始する前に

1. 拡張機能グループポリシー設定を有効にします。詳細については、「WSP の拡張機能を設定する」を参照してください。
2. 自動再接続グループポリシー設定を無効にします。詳細については、「WSP のセッション再開タイムアウトを設定する」を参照してください。

Zoom コンポーネントのインストール

Zoom 最適化を有効にするには、Windows に Zoom が提供する 2 つのコンポーネントをインストールします WorkSpaces。詳細については、「Amazon Web Services での Zoom の使用」を参照してください。

1. 内に Zoom VDI Meeting クライアントバージョン 5.12.6 以降をインストールします WorkSpace。
2. がインストールされているクライアントに Zoom VDI プラグイン (Windows ユニバーサルインストーラ) バージョン 5.12.6 以降 WorkSpace をインストールする

3. VDI プラグインのステータスが Zoom VDI クライアント内で接続済みと表示されることを確認して、プラグインが Zoom トラフィックを最適化していることを確認します。詳細については、「Amazon WorkSpaces 最適化の確認方法」を参照してください。

PCoIP 用の Zoom 会議メディアプラグインを有効にする

Active Directory への管理権限を持つユーザーは、グループポリシーオブジェクト (GPO) を使用してレジストリキーを生成できます。これにより、ユーザーは強制更新を使用してドメイン WorkSpaces 内のすべての Windows にレジストリキーを送信できます。または、管理者権限を持つユーザーは、WorkSpaces ホストにレジストリキーを個別にインストールすることもできます。

前提条件

プラグインを使用する前に、次の要件が満たされていることを確認してください。

- Windows WorkSpaces クライアントバージョン 5.4.0 以降と Zoom VDI プラグインバージョン 5.12.6 以降。
- 内 WorkSpaces — Zoom VDI Meeting クライアントバージョン 5.12.6 以降。

Windows WorkSpaces ホストでレジストリキーを作成する

Windows WorkSpaces ホストでレジストリキーを作成するには、次の手順を実行します。Windows で Zoom を使用するには、レジストリキーが必要です WorkSpaces。

1. 管理者として Windows レジストリエディタを開きます。
2. `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon` に移動します。
3. Extension キーが存在しない場合は、右クリックして [New] (新規) > [Key] (キー) を選択し、「Extension」という名前を付けます。
4. 新しい Extension キーで右クリックし、[New] (新規) > [DWORD] を選択し、「enable」という名前を付けます。この名前は小文字にする必要があります。
5. 新しい DWORD を選択し、値を 1 に変更します。
6. コンピュータを再起動してプロセスを完了します。
7. WorkSpaces ホストで、最新の Zoom VDI クライアントをダウンロードしてインストールします。 WorkSpaces クライアント (5.4 以降) で、Amazon 用の最新の Zoom VDI クライアントプラグインをダウンロードしてインストールします WorkSpaces。詳細については、Zoom サポートウェブサイトの「VDI のリリースとダウンロード」を参照してください。

Zoom を起動してビデオ通話を開始します。

トラブルシューティング

Windows で Zoom をトラブルシューティングするには、次のアクションを実行します WorkSpaces。

- レジストリキーのアクティベーションと適用が正しいことを確認します。
- `C:\ProgramData\Amazon\Amazon WorkSpaces Extension` に移動します。`wse_core_dll` と表示されていることを確認します。
- ホストとクライアントの間でバージョンが正しいこと、また一致していることを確認します。

問題が解決しない場合は、 センター AWS Support を使用して にお問い合わせください。 AWS Support

次の例を使用し、ディレクトリの管理者として GPO を適用できます。

- WSE.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
```

```
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
```

```
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

Amazon Linux の管理 WorkSpaces

Windows と同様に WorkSpaces、Amazon Linux WorkSpaces はドメインに参加しているため、Active Directory ユーザーとグループを使用して以下を行うことができます。

- Amazon Linux を管理する WorkSpaces
- ユーザーにアクセス権を付与 WorkSpaces する

Linux インスタンスはグループポリシーに従っていないため、設定管理ソリューションを使用してポリシーの配信と適用を行うことをお勧めします。例えば、AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise、または Ansible を使用できます。

> **Note**
>
> ローカルプリンターリダイレクトは、Amazon Linux では使用できません WorkSpaces。

Amazon Linux で WorkSpaces ストリーミングプロトコル (WSP) の動作を制御する WorkSpaces

WSP の動作は、`/etc/wsp/` ディレクトリにある `wsp.conf` ファイルの構成設定によって制御されます。ポリシーの変更をデプロイして適用するには、Amazon Linux をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。

> **Note**
>
> - `wsp.conf` ファイルに対して正しくない、またはサポートされていない変更を行った場合、ポリシーの変更が で新しく確立された接続に適用されない可能性があります WorkSpace。

- Amazon Linux WorkSpaces on WSP バンドルには、現在次の制限があります。
  - 現在、 AWS GovCloud （ 米国西部) および AWS GovCloud （ 米国東部) でのみ利用可能です。
  - 動画入力はサポートされていません。
  - 画面ロック時のセッション切断はサポートされていません。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。

WSP Amazon Linux のクリップボードリダイレクトを設定する WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を設定します。この設定は、 を切断して再接続するときに有効になります WorkSpace。

WSP Amazon Linux のクリップボードリダイレクトを設定するには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.
```
clipboard = X
```

   X に指定できる値は以下のとおりです。

   `enabled` – クリップボードリダイレクトは両方向ともに有効です (デフォルト)

   `disabled` – クリップボードリダイレクトは両方向ともに無効です

   `paste-only` – クリップボードリダイレクトは有効ですが、ローカルクライアントデバイスからコンテンツをコピーし、リモートホストデスクトップに貼り付けることのみが可能です。

   `copy-only` – クリップボードリダイレクトは有効ですが、リモートホストデスクトップからコンテンツをコピーし、ローカルクライアントデバイスに貼り付けることのみが可能です。

WSP Amazon Linux のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を無効にします。この設定は、 を切断して再接続するときに有効になります WorkSpace。

WSP Amazon Linux のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. ファイルの末尾に次の行を追加します。

```
audio-in = X
```

   X に指定できる値は以下のとおりです。

   `enabled` – オーディオ入力リダイレクトは有効です (デフォルト)

   `disabled` – オーディオ入力リダイレクトは無効です

WSP Amazon Linux のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンをミラーリングするように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行 WorkSpace することを意図したタスクが にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

必要に応じて、WSP 設定ファイルを使用してこの機能を設定します。この設定は、 を切断して再接続した後に有効になります WorkSpace。

WSP Amazon Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. ファイルの末尾に次の行を追加します。

```
timezone_redirect= X
```

X に指定できる値は以下のとおりです。

[enabled] (有効) — タイムゾーンのリダイレクトは有効です (デフォルト)

disabled (無効) — タイムゾーンのリダイレクトは無効です

Amazon Linux で PCoIP エージェントの動作を制御する WorkSpaces

PCoIP Agent の動作は、pcoip-agent.conf ディレクトリにある /etc/pcoip-agent/ ファイルの構成設定によって制御されます。ポリシーの変更をデプロイして適用するには、Amazon Linux をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。エージェントを再起動すると、開いている接続がすべて終了されウィンドウマネージャーが再起動されます。変更を適用するには、 を再起動することをお勧めします WorkSpace。

> **Note**
>
> pcoip-agent.conf ファイルに対して正しくない、またはサポートされていない変更を行うと、 が機能 WorkSpace しなくなる可能性があります。が機能 WorkSpace しなくなった場合は、SSH WorkSpace を使用して に接続して変更をロールバックするか、 を再構築 WorkSpaceする必要がある場合があります。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。使用可能な設定の完全なリストについては、任意の Amazon Linux のターミナルman pcoip-agent.confからを実行します WorkSpace。

PCoIP Amazon Linux のクリップボードリダイレクトを設定する WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。PCoIP エージェント設定を使用して、必要に応じてこの機能を無効にします。この設定は、 を再起動したときに有効になります WorkSpace。

PCoIP Amazon Linux のクリップボードリダイレクトを設定するには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで pcoip-agent.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. ファイルの末尾に次の行を追加します。

```
pcoip.server_clipboard_state = X
```

   X に指定できる値は以下のとおりです。

   0 – クリップボードリダイレクトは両方向ともに無効です

   1 – クリップボードリダイレクトは両方向ともに有効です

   2 – クリップボードリダイレクトはクライアントからエージェントへのみ有効です (ローカルクライアントデバイスからリモートホストデスクトップへのコピーと貼り付けのみを許可)

   3 – クリップボードリダイレクトはエージェントからクライアントへのみ有効です (リモートホストデスクトップからローカルクライアントデバイスへのコピーと貼り付けのみを許可)

> **Note**
>
> クリップボードのリダイレクトは仮想チャネルとして実装されます。仮想チャンネルが無効になっている場合、クリップボードのリダイレクトは機能しません。仮想チャネルを有効にするには、Teradici のドキュメントの「PCoIP Virtual Channels」をご参照ください。

PCoIP Amazon Linux のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。PCoIP エージェント設定を使用して、必要に応じてこの機能を無効にします。この設定は、 を再起動したときに有効になります WorkSpace。

PCoIP Amazon Linux のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで pcoip-agent.conf ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. ファイルの末尾に次の行を追加します。

   ```
   pcoip.enable_audio = X
   ```

   X に指定できる値は以下のとおりです。

   0 – オーディオ入力リダイレクトは無効です

   1 – オーディオ入力リダイレクトは有効です

PCoIP Amazon Linux のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンをミラーリングするように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行 WorkSpace することを意図したタスクが にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Linux で必要な場合は WorkSpaces、PCoIP エージェント conf を使用してこの機能を無効にすることができます。この設定は、 を再起動したときに有効になります WorkSpace。

PCoIP Amazon Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで pcoip-agent.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. ファイルの末尾に次の行を追加します。

```
pcoip.enable_timezone_redirect= X
```

   X に指定できる値は以下のとおりです。

   0 – タイムゾーンのリダイレクトは無効です

   1 – タイムゾーンのリダイレクトは有効です

Amazon Linux WorkSpaces 管理者に SSH アクセスを付与する

デフォルトでは、ドメイン管理者グループに割り当てられたユーザーとアカウントのみが SSH WorkSpaces を使用して Amazon Linux に接続できます。

Active Directory で Amazon Linux WorkSpaces 管理者専用の管理者グループを作成することをお勧めします。

Linux_Workspaces_Admins Active Directory グループのメンバーの sudo アクセスを有効にするには

1. 次の例に示すように、sudoers を使用して visudo ファイルを編集します。

```
[example\username@workspace-id ~]$ sudo visudo
```

2. 次の行を追加します。

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

専用の管理者グループを作成したら、次のステップに従ってグループのメンバーのログインを有効にします。

Linux_WorkSpaces_Admins Active Directory グループのメンバーのログインを有効にするには

1. 昇格された権限で `/etc/security/access.conf` を編集します。

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 次の行を追加します。

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

SSH 接続の有効化の詳細については、Linux の SSH 接続を有効にする WorkSpaces を参照してください。

Amazon Linux のデフォルトシェルを上書きする WorkSpaces

Linux のデフォルトシェルを上書きするには WorkSpaces、ユーザーの `~/.bashrc` ファイルを編集することをお勧めします。たとえば、`Z shell` シェルの代わりに `Bash` を使用するには、`/home/username/.bashrc` に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動するか、 WorkSpace から WorkSpace ログアウト (切断だけでなく) してから再度ログインする必要があります。

不正なアクセスからカスタムリポジトリを保護する

カスタムリポジトリへのアクセスを制御するには、パスワードではなく、Amazon Virtual Private Cloud (Amazon VPC) に組み込まれているセキュリティ機能を使用することをお勧めします。たとえば、ネットワークアクセスコントロールリスト (ACL) とセキュリティグループを使用します。これらの機能の詳細については、Amazon VPC ユーザーガイドのセキュリティを参照してください。

リポジトリを保護するためにパスワードを使用する必要がある場合は、Fedora ドキュメントの「リポジトリ定義ファイル」に示されているように、yum リポジトリ定義ファイルを作成してください。

Amazon Linux Extras Library リポジトリを使用する

Amazon Linux では、Extras Library を使用してアプリケーションおよびソフトウェア更新をインスタンスにインストールできます。Extras Library の使用については、Linux インスタンス用 Amazon EC2 ユーザーガイドの Extras Library (Amazon Linux) を参照してください。

> **Note**
>
> Amazon Linux リポジトリを使用している場合は、Amazon Linux WorkSpaces にインターネットアクセスがあるか、このリポジトリとメインの Amazon Linux リポジトリに Virtual Private Cloud (VPC) エンドポイントを設定する必要があります。詳細については、「からのインターネットアクセスを提供する WorkSpace」を参照してください。

Linux での認証にスマートカードを使用する WorkSpaces

Linux WorkSpaces on WorkSpaces Streaming Protocol (WSP) バンドルでは、認証に共通アクセスカード (CAC) と個人識別検証 (PIV) スマートカードを使用できます。詳細については、「認証にスマートカードを使用する」を参照してください。

インターネットアクセス用のデバイスプロキシサーバー設定を構成する

デフォルトでは、 WorkSpaces クライアントアプリケーションは HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定されているプロキシサーバーを使用します。Amazon WorkSpaces クライアントアプリケーションは、更新、登録、認証に HTTPS ポートを使用します。

> **Note**
>
> サインイン認証情報を使用した認証を必要とするプロキシサーバーはサポートされていません。

Microsoft ドキュメントの「デバイスプロキシとインターネット接続の設定を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Linux のデバイスプロキシサーバー設定を設定

できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

WorkSpaces Windows クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces macOS クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces Web Access クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

デスクトップトラフィックのプロキシ

PCoIP WorkSpaces の場合、デスクトップクライアントアプリケーションは、UDP のポート 4172 トラフィック (デスクトップトラフィックの場合) のプロキシサーバーの使用や TLS 復号化および検査をサポートしていません。ポート 4172 に直接接続する必要があります。

WSP の場合 WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート 4195 TCP トラフィックの HTTP プロキシサーバーの使用をサポートしています。TLS の復号および検査はサポートしていません。

WSP は、UDP 経由のデスクトップトラフィックに対するプロキシの使用をサポートしていません。TCP トラフィックのプロキシの使用をサポートしているのは、 WorkSpaces Windows および macOS デスクトップクライアントアプリケーションと WSP ウェブアクセスのみです。

> **Note**
>
> プロキシサーバーを使用する場合、クライアントアプリケーションが WorkSpaces サービスに対して行う API コールもプロキシされます。API コールとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイ

テンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket (TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響を与える可能性があります。

プロキシを使用する必要がある場合は、ストリーミングの品質と応答性に悪影響を及ぼす可能性のあるネットワークレイテンシーを追加しないように、プロキシサーバーを可能な限り WorkSpace クライアントの近く、できれば同じネットワーク内に配置してください。

Ubuntu を管理する WorkSpaces

Windows や Amazon Linux と同様に WorkSpaces、Ubuntu WorkSpaces はドメインに参加しているため、Active Directory ユーザーとグループを使用して次のことができます。

- Ubuntu を管理する WorkSpaces
- ユーザーにアクセス権を付与 WorkSpaces する

ADsys を使用して、グループポリシー WorkSpaces で Ubuntu を管理できます。 ADsys Active Directory 統合の詳細については、「Ubuntu Active Directory の統合に関するよくある質問」を参照してください。Landscape や Ansible など、他の構成および管理ソリューションを使用することもできます。

Ubuntu での WorkSpaces ストリーミングプロトコル (WSP) の動作を制御する WorkSpaces

WSP の動作は、`/etc/wsp/` ディレクトリにある `wsp.conf` ファイルの構成設定によって制御されます。ポリシーの変更をデプロイして適用するには、Ubuntu をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。

> **Note**
>
> `wsp.conf` ポリシーに正しくない、またはサポートされていない変更を加えた場合、 への新しく確立された接続に適用されない可能性があります WorkSpace。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。

Ubuntu のクリップボードリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を無効にします。

Ubuntu のクリップボードリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. `[policies]` グループの末尾に次の行を追加します。

   ```
   clipboard = X
   ```

   X に指定できる値は以下のとおりです。

   [enabled] (有効) — クリップボードリダイレクトは両方向ともに有効です (デフォルト)

   [disabled] (無効) — クリップボードのリダイレクトは両方向ともに無効です

   [paste-only] (ペーストのみ) — クリップボードのリダイレクトが有効で、ローカルクライアントデバイスからコンテンツをコピーし、リモートホストデスクトップにペーストするのみが可能です。

   [copy-only] (コピーのみ) — クリップボードのリダイレクトが有効で、リモートホストのデスクトップからコンテンツをコピーし、ローカルのクライアントデバイスにペーストするのみが可能です。

Ubuntu のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を無効にします。

Ubuntu のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
audio-in = X
```

X に指定できる値は以下のとおりです。

[enabled] (有効) — オーディオインリダイレクトは有効です (デフォルト)

[disabled] (無効)— オーディオインリダイレクトは無効です

Ubuntu のビデオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はビデオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を無効にします。

Ubuntu のビデオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
video-in = X
```

X に指定できる値は以下のとおりです。

[enabled] (有効) — ビデオインリダイレクトは有効です (デフォルト)

[disabled] (無効)— ビデオインリダイレクトは無効です

Ubuntu のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンをミラーリングするように設定されています WorkSpace。この動作は、タイムゾーンのリダイレク

トによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行 WorkSpace することを意図したタスクが にスケジュールされている。
- ユーザーは多くの旅行をしており、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

必要に応じて、WSP 設定ファイルを使用してこの機能を設定します。

Ubuntu のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
timezone-redirection = X
```

X に指定できる値は以下のとおりです。

[enabled] (有効) — タイムゾーンのリダイレクトは有効です (デフォルト)

disabled (無効) — タイムゾーンのリダイレクトは無効です

Ubuntu のプリンターリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はプリンターのリダイレクト WorkSpaces をサポートします。必要に応じて、WSP 設定ファイルを使用してこの機能を無効にします。

Ubuntu のプリンターリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
remote-printing = X
```

X に指定できる値は以下のとおりです。

[enabled] (有効) — プリンターリダイレクトは有効です (デフォルト)

[disabled] (無効)— プリンターリダイレクトは無効です

WSP の画面ロックの場合のセッションの切断を有効化/無効化する

画面ロックでセッションの切断を有効にして、ロック画面が検出されたときにユーザーが WorkSpaces セッションを終了できるようにします。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、 に対してどのタイプの認証が有効になっているかに応じて、自分自身を認証できます WorkSpaces。

デフォルトでは、 WorkSpaces は画面ロック時のセッションの切断をサポートしていません。必要に応じて、WSP 設定ファイルを使用してこの機能を有効にします。

Ubuntu の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
disconnect-on-lock = X
```

X に指定できる値は以下のとおりです。

有効 — 画面ロック時の接続解除が有効です

無効 — 画面ロック時の接続解除は無効です (デフォルト)

Ubuntu WorkSpaces 管理者に SSH アクセスを付与する

デフォルトでは、ドメイン管理者グループに割り当てられたユーザーとアカウントのみが SSH WorkSpaces を使用して Ubuntu に接続できます。他のユーザーやアカウントが SSH WorkSpaces を使用して Ubuntu に接続できるようにするには、Active Directory で Ubuntu 管理者専用の WorkSpaces 管理者グループを作成することをお勧めします。

`Linux_WorkSpaces_Admins` Active Directory グループのメンバーの sudo アクセスを有効にするには

1. 次の例に示すように、`sudoers` を使用して `visudo` ファイルを編集します。

```
[username@workspace-id ~]$ sudo visudo
```

2. 次の行を追加します。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

専用の管理者グループを作成したら、次のステップに従ってグループのメンバーの口グインを有効にします。

`Linux_WorkSpaces_Admins` Active Directory グループのメンバーの口グインを有効にするには

1. 昇格された権限で `etc/security/access.conf` を編集します。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 次の行を追加します。

```
+:(Linux_WorkSpaces_Admins):ALL
```

Ubuntu WorkSpaces では、SSH 接続のユーザー名を指定するときにドメイン名を追加する必要はなく、デフォルトではパスワード認証が無効になっています。SSH 経由で接続するには、Ubuntu の `$HOME/.ssh/authorized_keys` に SSH パブリックキーを追加するか WorkSpace、 を編集`/etc/ssh/sshd_config`して PasswordAuthentication に設定する必要がありますyes。SSH 接続の有効化の詳細については、「Linux の SSH 接続を有効にする WorkSpaces」を参照してください。

Ubuntu のデフォルトシェルを上書きする WorkSpaces

Ubuntu のデフォルトシェルを上書きするには WorkSpaces、ユーザーの `~/.bashrc` ファイルを編集することをお勧めします。たとえば、`Z shell` シェルの代わりに `Bash` を使用するには、`/home/username/.bashrc` に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動するか、 WorkSpace から WorkSpace ログアウト (切断だけでなく) してから再度ログインする必要があります。

インターネットアクセス用のデバイスプロキシサーバー設定を構成する

デフォルトでは、 WorkSpaces クライアントアプリケーションは HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定されているプロキシサーバーを使用します。Amazon WorkSpaces クライアントアプリケーションは、更新、登録、認証に HTTPS ポートを使用します。

> **Note**
>
> サインイン認証情報を使用した認証を必要とするプロキシサーバーはサポートされていません。

Microsoft ドキュメントの「デバイスプロキシとインターネット接続の設定を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Ubuntu のデバイスプロキシサーバー設定を設定できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

WorkSpaces Windows クライアントアプリケーションでのプロキシ設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces macOS クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

WorkSpaces Web Access クライアントアプリケーションでのプロキシ設定の設定の詳細については、「Amazon ユーザーガイド」の「プロキシサーバー」を参照してください。 WorkSpaces

デスクトップトラフィックのプロキシ

PCoIP WorkSpaces の場合、デスクトップクライアントアプリケーションは、UDP のポート 4172 トラフィック (デスクトップトラフィック用) のプロキシサーバーの使用や TLS 復号化および検査をサポートしていません。ポート 4172 に直接接続する必要があります。

WSP の場合 WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート 4195 TCP トラフィックの HTTP プロキシサーバーの使用をサポートしています。TLS の復号および検査はサポートしていません。

WSP は、UDP 経由のデスクトップトラフィックに対するプロキシの使用をサポートしていません。TCP トラフィックのプロキシの使用をサポートしているのは、 WorkSpaces Windows および macOS デスクトップクライアントアプリケーションと WSP ウェブアクセスのみです。

> **Note**
>
> プロキシサーバーを使用する場合、クライアントアプリケーションが WorkSpaces サービスに対して行う API コールもプロキシされます。API コールとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイテンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket (TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響を与える可能性があります。

プロキシを使用する必要がある場合は、ストリーミングの品質と応答性に悪影響を及ぼす可能性のあるネットワークレイテンシーを追加しないように、プロキシサーバーを可能な限り WorkSpace クライアントの近く、できれば同じネットワーク内に配置してください。

Amazon WorkSpaces をリアルタイムコミュニケーションに最適化

Amazon WorkSpaces では、Microsoft Teams、Zoom、Webex などのユニファイドコミュニケーション (UC) アプリケーションの導入を容易にするさまざまな手法を提供しています。現代のアプリケーション環境では、ほとんどの UC アプリケーションに、1:1 チャットルーム、共同グループチャットチャネル、シームレスなファイルストレージと交換、ライブイベント、ウェビナー、ブロードキャスト、インタラクティブな画面共有と制御、ホワイトボード、オフラインのオーディオ/ビデオメッセージング機能などのさまざまな機能が備わっています。この機能のほとんどは、追加の微調整や機能強化を必要とせずに、 WorkSpaces 標準機能としてシームレスに利用できます。ただし、リアルタイムのコミュニケーション要素、 one-on-one 特に通話やグループ会議は、この規則の例外であることに注意してください。このような機能をうまく組み込むには、 WorkSpaces 導入プロセス中に集中的に取り組み、計画を立てることが必要になることがよくあります。

Amazon で UC アプリケーションのリアルタイム通信機能の実装を計画する場合 WorkSpaces、3 つの異なるリアルタイム通信 (RTC) 設定モードから選択できます。選択するモードは、ユーザーに提供される 1 つまたは複数の特定のアプリケーションと、使用する予定のクライアントデバイスによって異なります。

このドキュメントでは、Amazon で最も一般的な UC アプリケーションのユーザーエクスペリエンスの最適化に焦点を当てています。 WorkSpaces WorkSpaces Core 固有の最適化については、パートナー固有のドキュメントを参照してください。

トピック

- メディア最適化モードの概要
- 使用する RTC 最適化モードについて

- RTC 最適化ガイダンス

メディア最適化モードの概要

使用可能なメディア最適化オプションは次のとおりです。

オプション 1: メディア最適化リアルタイム通信 (メディア最適化 RTC)

このモードでは、サードパーティのUCおよびVoIPアプリケーションはリモートで実行され WorkSpace、メディアフレームワークはサポート対象のクライアントにオフロードされて直接通信されます。Amazon WorkSpaces では次の UC アプリケーションがこのアプローチを採用しています。

- Zoom Meetings
- Cisco Webex Meetings

メディア最適化 RTC モードが機能するためには、UC アプリケーションベンダーは DCV Extension SDK など、入手可能なソフトウェア開発キット (SDK) WorkSpaces のいずれかを使用して統合を開発する必要があります。このモードでは、UC コンポーネントをクライアントデバイスにインストールする必要があります。

このモードの設定の詳細については、「メディア最適化 RTC の設定」を参照してください。

オプション 2: セッション中最適化リアルタイム通信 (セッション中最適化 RTC)

このモードでは、変更されていない UC アプリケーションが上で動作し WorkSpace、ストリーミングプロトコルを介してオーディオとビデオのトラフィックをクライアントデバイスに伝送します。WorkSpaces マイクからのローカルオーディオと Web カメラからのビデオストリームはにリダイレクトされ WorkSpace、UC アプリケーションによって消費されます。このモードは幅広いアプリケーション互換性を実現し、UC WorkSpace アプリケーションをリモートからさまざまなクライアントプラットフォームに効率的に配信します。UC アプリケーションコンポーネントをクライアントデバイスにデプロイする必要はありません。

このモードの設定の詳細については、「セッション中最適化 RTC の設定」を参照してください。

オプション 3: 直接リアルタイム通信 (直接 RTC)

このモードでは、 WorkSpace 内で動作するアプリケーションが、ユーザのデスクまたはクライアント OS にある物理電話セットまたは仮想電話セットを制御します。これにより、音声トラフィック

は、ユーザーのワークステーションの物理電話またはクライアントデバイス上で動作する仮想電話からリモートコールピアに直接トラバースします。このモードで機能するアプリケーションの注目すべき例には以下が含まれます。

- アマゾン向けAmazon Connect 最適化 WorkSpaces
- Genesys Cloud WebRTC Media Helper
- Microsoft Teams SIP ゲートウェイ
- Microsoft Teams 卓上電話機と Teams ディスプレイ
- UC アプリケーションのダイヤルインまたは「dial my phone」機能による音声会議への参加。

このモードの設定の詳細については、「直接 RTC の設定」を参照してください。

使用する RTC 最適化モードについて

異なる RTC 最適化モードを同時に使用することも、フォールバックとして互いに補完するように設定することもできます。たとえば、Cisco Webex Meetings 向けにディア最適化 RTC を有効にするとします。この設定により、 WorkSpace ユーザーがデスクトップクライアント経由でアクセスするときの通信が最適化されます。ただし、UC 最適化コンポーネントが組み込まれていない共有インターネットキオスクから Webex にアクセスするシナリオでは、Webex はセッション中最適化 RTC モードにシームレスに移行して機能を維持します。ユーザーが複数の UC アプリケーションを使用する場合は、RTC 設定モードがユーザー固有の要件に基づいて異なる場合があります。

以下の表に UC アプリケーションの一般的な機能を示します。ここでは、どの RTC 設定モードが最良の結果をもたらすかが定義されています。

機能	直接 RTC	メディア最適化 RTC	セッション中最適化 RTC
1:1 チャット	RTC 設定は不要		
グループチャットルーム	RTC 設定は不要		
グループオーディオ会議	= ベスト	= ベスト	良好
グループビデオ会議	良好	= ベスト	良好

機能	直接 RTC	メディア最適化 RTC	セッション中最適化 RTC
1 対 1 のオーディオ通話	= ベスト	= ベスト	良好
1 対 1 のビデオ通話	良好	= ベスト	良好
ホワイトボード	RTC 設定は不要		
オーディオ/ビデオクリップ/メッセージング	該当しない	良好	= ベスト
ファイル共有	該当しない	UC アプリケーションによって異なる	= ベスト
画面の共有と制御	該当しない	UC アプリケーションによって異なる	= ベスト
ウェビナー/イベントのブロードキャスト	該当しない	良好	= ベスト

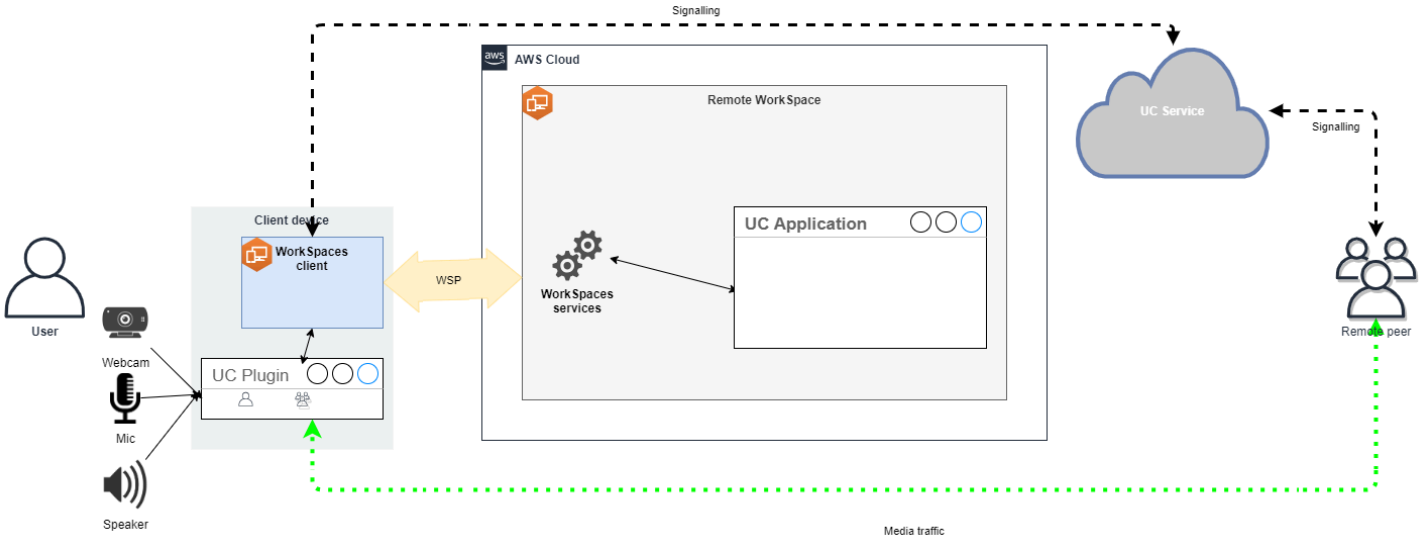
RTC 最適化ガイダンス

メディア最適化 RTC の設定

メディア最適化 RTC モードは、Amazon によって提供される SDK を使用する UC アプリケーションベンダーによって設定されます。このアーキテクチャでは、UC ベンダーが UC 固有のプラグインまたは拡張機能を開発し、それをクライアントにデプロイする必要があります。

SDK には DCV Extension SDK などの公開されているオプションやカスタマイズされたプライベートバージョンが含まれており、内で動作する UC WorkSpace アプリケーションモジュールとクライアント側のプラグインとの間の制御チャネルを確立します。通常、この制御チャネルはクライアント拡張機能に通話の開始または通話への参加を指示します。クライアント側拡張機能を通じて通話が確立されると、UC プラグインはマイクからの音声とウェブカメラからのビデオをキャプチャし、それらを UC クラウドまたはコールピアに直接送信します。受信した音声はローカルで再生され、ビデオ

はリモートクライアント UI にオーバーレイされます。制御チャネルは通話のステータスを伝達します。



Amazon WorkSpaces は現在、メディア最適化 RTC モードで以下のアプリケーションをサポートしています。

- ズームミーティング (PCoIP および WSP 用) WorkSpaces
- シスコ Webex ミーティング (WSP のみ) WorkSpaces

リストにないアプリケーションを使用している場合は、アプリケーションベンダーに連絡して、WorkSpaces Media Optimized RTC のサポートを依頼することをお勧めします。このプロセスを早めるには、@amazon .com aws-av-offloading に連絡するよう勧めてください。

メディア最適化 RTC モードは通話パフォーマンスを向上させ、 WorkSpaceリソースの使用率を最小限に抑えますが、一定の制限があります。

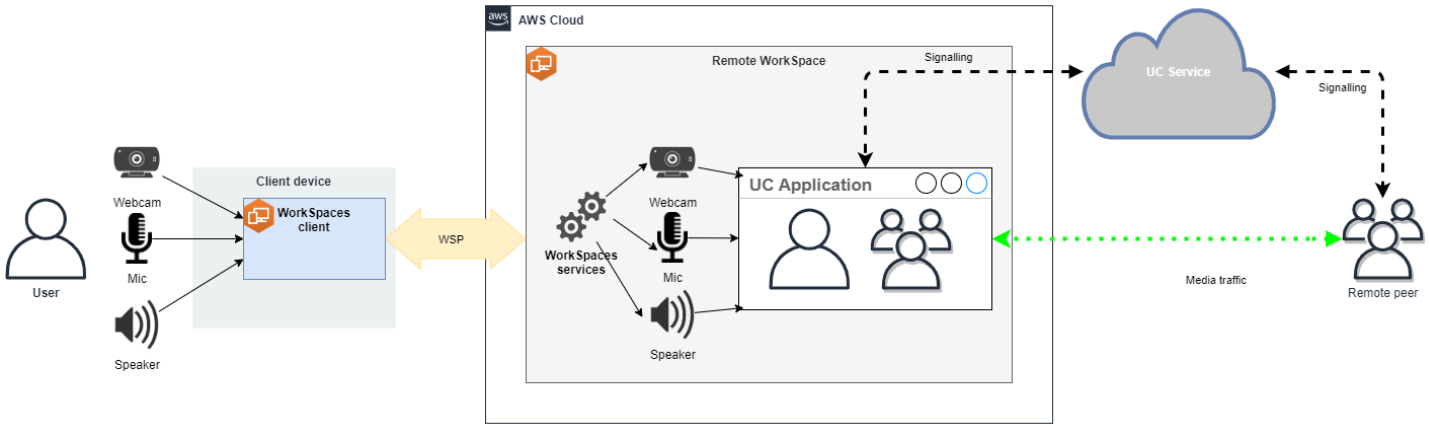
- UC クライアント拡張機能をクライアントデバイスにインストールする必要があります。
- UC クライアント拡張機能は、独立した管理と更新が必要です。
- UC クライアント拡張機能は、モバイルプラットフォームやウェブクライアントなど、特定のクライアントプラットフォームでは使用できない場合があります。
- このモードでは、画面共有の動作が異なる場合があるなど、UC アプリケーションの機能の一部が制限されることがあります。
- クライアント側拡張機能の使用は、Bring-Your-Own-Device (BYOD) や共有キオスクなどのシナリオには適さない場合があります。

メディア最適化 RTC モードがユーザーの環境に適さない場合や、特定のユーザーがクライアント拡張機能をインストールできない場合は、フォールバックオプションとしてセッション中最適化 RTC モードを設定することをお勧めします。

セッション中最適化 RTC の設定

インセッション最適化 RTC モードでは、UC WorkSpace アプリケーションは何も変更せずに上で動作するため、ローカル環境と同様の操作性が得られます。アプリケーションによって生成されたオーディオストリームとビデオストリームは、 WorkSpaces ストリーミングプロトコル (WSP) によってキャプチャされ、クライアント側に送信されます。クライアントでは、マイク (WSP と PCoIP の両方 WorkSpaces) と Web カメラ (WSP のみ WorkSpaces) の信号がキャプチャされ、にリダイレクトされ WorkSpace、UC アプリケーションにシームレスに渡されます。

特に、このオプションはレガシーアプリケーションとの互換性が非常に高く、アプリケーションのオリジンに関係なく一貫したユーザーエクスペリエンスを提供できます。セッション中最適化はウェブクライアントでも機能します。



WorkSpaces ストリーミングプロトコル (WSP) は、リモート RTC モードのパフォーマンスを向上させるために細心の注意を払って最適化されています。最適化手段には以下が含まれます。

- アダプティブ UDP ベース QUIC トランスポートを利用し、効率的なデータ転送を保証します。
- 低遅延オーディオパスを確立し、高速なオーディオ入出力を容易にします。
- 音声用に最適化されたオーディオコーデックを実装することで、CPU とネットワークの使用量を抑えながらオーディオ品質を維持します。
- ウェブカメラのリダイレクト。ウェブカメラ機能を統合できるようになります。
- パフォーマンスを最適化するためのウェブカメラの解像度の設定。
- 速度と画質のバランスをとる適応型ディスプレイコーデックの統合。

- オーディオジッター補正。スムーズなオーディオ伝送を保証します。

これらの最適化により、リモート RTC モードでの堅牢でスムーズなエクスペリエンスが実現します。

推奨サイズ

リモート RTC モードを効果的にサポートするには、Amazon のサイズを適切に設定することが重要です。 WorkSpacesリモコンは、それぞれのユニファイドコミュニケーション (UC) アプリケーションのシステム要件を満たしているか、 WorkSpace それを上回っている必要があります。次の表は、一般的な UC アプリケーションをビデオ通話と音声通話に使用する場合の、 WorkSpaces サポートされる最小構成と推奨構成の概要を示しています。

			ビデオ通話		音声通話		
アプリケーション	RTC アプリの CPU 要件	RTC アプリの RAM 要件	最低限サポート対象 WorkSpace	推奨 WorkSpace	最低限サポートされている WorkSpace	推奨 WorkSpace	リファレンス
Microsoft Teams	2 コア (必須)、4 コア (推奨)	4.0 GB RAM	Power (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	Performance (2 vCPU、8 GB メモリ)	Power (4 vCPU、16 GB メモリ)	Microsoft Teams のハードウェア要件
Zoom	2 コア (必須)、4 コア (推奨)	4.0 GB RAM	Power (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	Performance (2 vCPU、8 GB メモリ)	Power (4 vCPU、16 GB メモリ)	Zoom システム要件: Windows、macOS、Linux
Webex	2 コア (必須)	4.0 GB RAM	Power (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	Performance (2 vCPU、8 GB メモリ)	Power (4 vCPU、16 GB メモリ)	Webex サービスのシステム要件

ビデオ会議では、ビデオのエンコードとデコードに大量のリソースが使用されることに注意してください。物理マシンのシナリオでは、これらのタスクは GPU にオフロードされます。非 GPU では WorkSpaces、これらのタスクはリモートプロトコルエンコーディングとparallel CPU 上で実行されます。そのため、ビデオストリーミングやビデオ通話を定期的に行うユーザーには、 PowerProこの構成を選択することを強くお勧めします。

また、画面共有はリソースを大量に消費します。解像度が高くなると、リソースの消費量も増加します。そのため、GPU WorkSpaces 以外の環境では、画面共有は低いフレームレートに制限されることがよくあります。

UDP ベースの QUIC トランスポートをストリーミングプロトコル (WSP) WorkSpaces で活用

UDP トランスポートは、特に RTC アプリケーションの送信に適しています。効率を最大化するには、QUIC トランスポートを WSP に使用するようにネットワークを設定してください。UDP ベースのトランスポートはネイティブクライアントでしか使用できないことに注意してください。

UC アプリケーションの設定 WorkSpaces

背景ぼかし、バーチャル背景、リアクション、ライブイベントの開催などのビデオ処理機能を強化するには、最適なパフォーマンスを実現するために GPU WorkSpace 対応を選択することが不可欠です。

ほとんどの UC アプリケーションには、GPU 以外の CPU 使用率を下げるために、高度なビデオ処理を無効にするガイダンスが用意されています。 WorkSpaces

詳細については、以下のリソースを参照してください。

- Microsoft Teams: 仮想デスクトップ インフラストラクチャ用の Teams
- Zoom Meetings: Managing the user experience for incompatible VDI plugins
- Webex: Deployment guide for Webex App for Virtual Desktop Infrastructure (VDI) - Manage and troubleshoot Webex App for VDI [Webex App]
- Google Meet: Using VDI

オーディオとウェブカメラの双方向リダイレクトを有効にする

Amazon WorkSpaces は基本的に、オーディオ入力、オーディオ出力、ビデオインによるカメラリダイレクトをデフォルトでサポートしています。ただし、特定の理由でこれらの機能が無効になっている場合、提供されているガイダンスに従ってリダイレクトを再度有効にできます。詳細については、

『Amazon 管理ガイド』の「WSP のビデオインリダイレクトを有効または無効にする」を参照してください。 WorkSpacesユーザーは接続後にセッションで使用したいカメラを選択する必要があります。詳細については、Amazon WorkSpaces ユーザーガイドの「ウェブカメラとその他のビデオデバイス」を参照してください。

ウェブカメラの最大解像度を制限する

Power PowerPro WorkSpaces を使用しているユーザーやビデオ会議を行うユーザーには、リダイレクトされるウェブカメラの最大解像度を制限することを強くお勧めします。の場合 PowerPro、推奨最大解像度は幅 640 ピクセル、高さ 480 ピクセルです。Power の場合は、推奨最大解像度は幅 320 ピクセル、高さ 240 ピクセルです。

次の手順を実行して、ウェブカメラの最大解像度を設定します。

1. Windows レジストリエディタを開きます。
2. 以下のレジストリパスに移動します。

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. `max-resolution` という名前の文字列値を作成し、`(X,Y)` フォーマットで希望する解像度に設定します。このとき、`X` は水平方向のピクセル数 (幅) を表し、`Y` は垂直方向のピクセル数 (高さ) を表します。たとえば、次のように指定します。幅 640 ピクセル、高さ 480 ピクセルの解像度を表すには、`(640,480)` と指定します。

音声用に最適化されたオーディオ設定の有効化

デフォルトでは、7.1 WorkSpaces の高音質オーディオをクライアントに配信するように設定されているため、優れた音楽再生品質が保証されます。 WorkSpaces ただし、主な用途に音声会議またはビデオ会議が含まれている場合は、オーディオコーデックプロファイルを音声用に最適化された設定に変更することで、CPU とネットワークリソースを節約できます。

次の手順を実行して、オーディオプロファイルを最適化された音声に設定します。

1. Windows レジストリエディタを開きます。
2. 以下のレジストリパスに移動します。

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

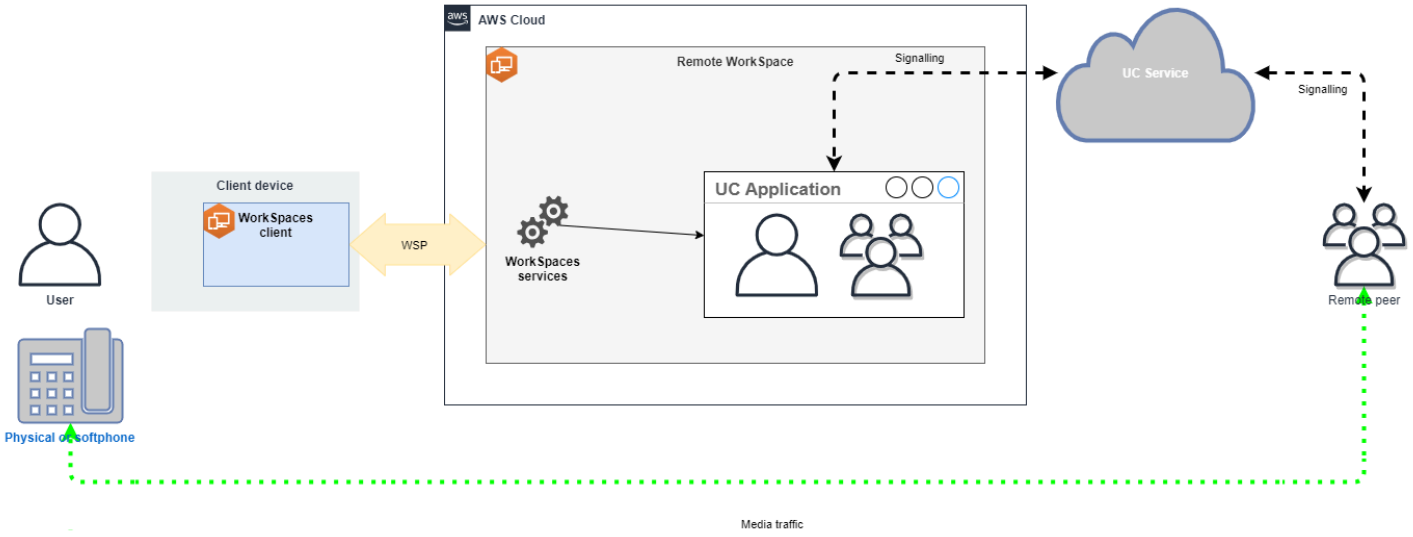
3. `default-profile` と言う名前の文字列値の名前を作成し、`voice` に設定します。

音声通話やビデオ通話には高品質のヘッドセットを使用してください。

オーディオ体験を向上させ、エコーを防ぐには、高品質のヘッドセットを使用することが重要です。デスクトップスピーカーを使用すると、通話のリモートエンドでエコーの問題が発生する可能性があります。

直接 RTC の設定

Direct RTC モードの設定は特定のユニファイドコミュニケーション (UC) アプリケーションによって異なるため、設定を変更する必要はありません。 WorkSpaces 以下のリストは、さまざまな UC アプリケーションの最適化を完全に網羅したものではありません。



- Microsoft Teams：
  - SIP ゲートウェイの計画
  - Microsoft 365 での音声会議
  - Microsoft Teams での音声ソリューションの計画
- Zoom Meetings:
  - Enabling or disabling toll call dial-in numbers
  - Using desk phone call control
  - Desk phone companion mode
- Webex:
  - Webex App | Make calls with your desk phone
  - Webex App | Supported calling options
- BlueJeans:

  - Dialing into a Meeting from a Desk Telephone
- Genesys:
  - Genesys Cloud WebRTC Media Helper
- Amazon Connect:
  - アマゾン向けAmazon Connect 最適化 WorkSpaces
- Google Meet:
  - Use a phone for audio in a video meeting

WorkSpace の実行モードを管理する

WorkSpace は、実行モードによって、すぐに使用できるかどうかとお支払い方法 (月単位または時間単位) が異なります。WorkSpace の作成時に、以下のいずれかの実行モードを選択できます。

- AlwaysOn — 固定月額料金で WorkSpaces を無制限にご利用いただけます。このモードは、WorkSpace をプライマリデスクトップとしてフルタイム使用するユーザー用に最適です。
- AutoStop — WorkSpaces のご利用に対し、時間単位で料金が発生します。このモードでは、アプリおよびデータを保存した状態と指定の長さの切断が発生した後、WorkSpaces が停止します。

詳細については、WorkSpaces の料金を参照してください。

AutoStop WorkSpaces

自動停止時間を設定するには、Amazon WorkSpaces コンソールで WorkSpace を選択し、[Actions] (アクション)、[Modify Running Mode Properties] (実行モードプロパティの変更) の順に選択し、[AutoStop Time (hours)] (自動停止時間 (時間)) を設定します。デフォルトでは、[AutoStop Time (hours)] (自動停止時間 (時間)) は 1 時間に設定されています。つまり、WorkSpace は、切断されてから 1 時間後に自動的に停止することになります。

WorkSpace が切断され、自動停止時間が経過すると、WorkSpace が自動的に停止するまでさらに数分かかる場合があります。ただし、自動停止期間が経過するとすぐに請求が停止し、その追加時間に対しては課金されません。

可能な場合は、WorkSpace のルートボリュームにデスクトップの状態が保存されます。ユーザーがログインすると WorkSpace が再開し、すべての開いていたドキュメントや実行中のプログラムが保存済みの状態に戻ります。

AutoStop Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro WorkSpaces では、停止時にデータとプログラムの状態は保持されません。これらの Autostop WorkSpaces は、作業が完了したら、作業内容をその都度保存することをお勧めします。

Bring-Your-Own-License (BYOL) AutoStop WorkSpaces では、多数の同時ログインによって、WorkSpaces が使用可能になるまでの時間が長引く可能性があります。BYOL AutoStop WorkSpaces に多くのユーザーが同時にログインすることが想定される場合は、アカウントマネージャーにご相談ください。

> **Important**
>
> AutoStop WorkSpaces は、WorkSpaces が切断されている場合にのみ自動的に停止します。

WorkSpace は、次の場合にのみ切断されます。

- ユーザーが WorkSpace から手動で切断するか、Amazon WorkSpaces クライアントアプリケーションを終了する場合。
- クライアントデバイスがシャットダウンされる場合。
- 20 分を超える時間にわたって、クライアントデバイスと WorkSpace の間に接続がない場合。

ベストプラクティスとして、AutoStop WorkSpace ユーザーは、日々、使用が終了したら、WorkSpaces から手動で切断すべきです。手動で切断するには、Linux、macOS、または Windows 用の WorkSpaces クライアントアプリケーションの Amazon WorkSpaces メニューから、[Disconnect WorkSpace] (WorkSpace を切断) または [Quit Amazon WorkSpaces] (Amazon WorkSpaces を終了) を選択します。Android または iPad の場合は、サイドバーメニューから [Disconnect] (切断) を選択します。

次のような場合、AutoStop WorkSpaces が自動的に停止しないことがあります。

- クライアントデバイスがシャットダウンされるのではなく、ロック状態、スリープ状態、またはその他の非アクティブ状態 (ノートパソコンのカバーが閉じられている、など) にある場合は、WorkSpaces アプリケーションがバックグラウンドで引き続き実行されている可能性があります。WorkSpaces アプリケーションが引き続き実行中である限り、WorkSpace は切断されない可能性があるため、自動的に停止しない場合があります。
- WorkSpaces は、ユーザーが WorkSpaces クライアントを使用している場合にのみ切断を検出できます。ユーザーがサードパーティーのクライアントを使用している場合は、WorkSpaces が切断

状態を検出できない可能性があり、WorkSpaces が自動的に停止せず、請求が中断しない場合があります。

実行モードを変更する

実行モードは、いつでも切り替えることができます。

WorkSpace の実行モードを変更するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. 変更する WorkSpace を選択し、[Actions] (アクション)、[Modify Running Mode] (実行モードの変更) の順に選択します。
4. 新しい実行モード [AlwaysOn] (常にオン) または [AutoStop] (自動停止) を選択し、次に [Save] (保存) をクリックします。

AWS CLI を使用して WorkSpace の実行モードを変更するには

modify-workspace-properties コマンドを使用します。

AutoStop WorkSpace を停止/開始する

AutoStop WorkSpaces が切断されている場合、切断されてから指定された時間が経過した後に自動的に停止し、時間単位の請求は一時停止します。コストをさらに最適化するには、AutoStop の WorkSpace に関連付けられている時間あたりの使用料金を手動で中断することができます。WorkSpace が停止し、ユーザーが次に WorkSpace にログオンする場合に備えて、すべてのアプリケーションやデータが保存されます。

停止中の WorkSpace にユーザーが再接続すると、通常は 90 秒未満で、前回の状態から再開されます。

AutoStop の WorkSpaces は、使用可能状態であってもエラー状態であっても再起動できます。

自動停止 WorkSpace を停止するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。

3. 停止する WorkSpace を選択したら、[Actions] (アクション)、[Stop WorkSpaces] (WorkSpaces の停止) の順に選択します。
4. 確認を求めるメッセージが表示されたら、[Stop] (停止) を選択します。

自動停止 WorkSpace を開始するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. 開始する WorkSpace を選択したら、[Actions] (アクション)、[Start WorkSpaces] (WorkSpaces の起動) の順に選択します。
4. 確認を求めるメッセージが表示されたら、[Start WorkSpace] (WorkSpace の起動) を選択します。

AutoStop WorkSpaces に関連付けられた固定インフラストラクチャコストを削除するには、アカウントから WorkSpace を削除します。詳細については、「WorkSpace の削除」を参照してください。

を使用して AutoStop WorkSpace を停止/開始するにはAWS CLI

stop-workspaces コマンドと start-workspaces コマンドを使用します。

アプリケーションの管理

を起動すると WorkSpace、 に関連付けられているすべてのアプリケーションバンドルのリストが WorkSpaces コンソール WorkSpace に表示されます。

に関連付けられているすべてのアプリケーションバンドルのリストを表示するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. 左側のナビゲーションペインから、 を選択しますWorkSpaces。
3. WorkSpace を選択し、詳細の表示 を選択します。
4. アプリケーション で、この に関連付けられているアプリケーションのリストと WorkSpaceインストールステータスを確認します。

のアプリケーションバンドルは、次の WorkSpace 方法で更新できます。

- にアプリケーションバンドルをインストールする WorkSpace

- からアプリケーションバンドルをアンインストールする WorkSpace
- アプリケーションバンドルをインストールし、 に別のアプリケーションバンドルのセットをアンインストールする WorkSpace

> **Note**
>
> - アプリケーションバンドルを更新するには、 のステータスが AVAILABLEまたは WorkSpace である必要がありますSTOPPED。
> - アプリケーションの管理は Windows でのみ使用できます WorkSpaces。
> - [アプリケーションの管理] は、 AWSを通じてサブスクライブされたアプリケーションバンドルでのみ使用できます。

[アプリケーションの管理] でサポートされているバンドル

アプリケーションを管理する では、 に次のアプリケーションをインストールおよびアンインストールできます WorkSpaces。Microsoft Office 2016 バンドルとMicrosoft Office 2019 の場合は、アンインストールのみが可能です。

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021

次の表は、サポートされているアプリケーションとオペレーティングシステムの組み合わせと、サポートされていない組み合わせの一覧です。

	Microsoft Office Professional Plus 2016 (32 ビット)	Microsoft Office Professional Plus 2019 (64 ビット)	Microsoft LTSC Office Professional Plus / Standard 2021 (64 ビット)	Microsoft Project Professional / Standard 2021 (64 ビット)	Microsoft LTSC Visio Professional / Standard 2021 (64 ビット)
Windows Server 2016	アンインストール	サポートされません	サポートされません	サポートされません	サポートされません
[Windows Server 2019]	サポートされていません	アンインストール	インストール/アンインストール	インストール/アンインストール	インストール/アンインストール
Windows Server 2022	サポートされていません	アンインストール	インストール/アンインストール	インストール/アンインストール	インストール/アンインストール
Windows 10	アンインストール	アンインストール	インストール/アンインストール	インストール/アンインストール	インストール/アンインストール
Windows 11	アンインストール	アンインストール	インストール/アンインストール	インストール/アンインストール	インストール/アンインストール

Important

- これらのアプリケーションは同じエディションに従う必要があります。例えば、Standard アプリケーションと Professional アプリケーションを混在させることはできません。
- これらのアプリケーションは同じバージョンに従う必要があります。例えば、2019 アプリケーションと 2021 アプリケーションを混在させることはできません。

- Microsoft Office/Visio/Project 2021 Standard/Professional は、Value、Graphics、GraphicsPro WorkSpaces バンドルではサポートされていません。
- Microsoft Office 2016 用 Plus アプリケーションバンドルを からアンインストールすると WorkSpaces、その Amazon WorkSpaces バンドルの一部として含まれていた Trend Micro ソリューションにアクセスできなくなります。Amazon で Trend Micro ソリューションを引き続き使用する場合は WorkSpaces、AWS マーケットプレイス で個別に購入できます。
- Microsoft 365 アプリケーションをインストール/アンインストールするには、独自のツールとインストーラーを用意する必要があります。[アプリケーションの管理] ワークフローでは、Microsoft 365 アプリケーションをインストール/アンインストールすることはできません。
- Manage applications を通じてインストール WorkSpaces されたアプリケーションで のカスタムイメージを作成することはできませんが、Manage applications を使用してアプリケーションバンドルをアンインストール WorkSpaces するカスタムイメージを作成できます。
- [アプリケーションの管理] を使用するには、DNS 解決を有効にする必要があります。
- アフリカ (ケープタウン) などのオプトインリージョンでは、ディレクトリレベルで WorkSpaces インターネット接続を有効にする必要があります。

でアプリケーションバンドルを更新するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. WorkSpace を選択し、アクション 、アプリケーションの管理 を選択します。
4. 現在のアプリケーションには、この WorkSpace に既にインストールされているアプリケーションバンドルのリストが表示され、アプリケーションの選択には、この にインストールできるアプリケーションバンドルのリストが表示されます WorkSpace。
5. この にアプリケーションバンドルをインストールするには WorkSpace :
   a. この にインストールするアプリケーションバンドルを選択し WorkSpace、 の関連付けを選択します。
   b. 前のステップを繰り返して、他のアプリケーションバンドルをインストールします。

c. アプリケーションバンドルのインストール中は、[現在のアプリケーション] の下に `Pending install deployment` ステータスが表示されます。

6. この からアプリケーションバンドルをアンインストールするには WorkSpace :

a. [アプリケーションの選択] で、アンインストールするアプリケーションバンドルを選択し、[関連付け解除] を選択します。

b. 前のステップを繰り返して、他のアプリケーションバンドルをアンインストールします。

c. アプリケーションバンドルのアンインストール中は、[現在のアプリケーション] の下で、`Pending uninstall deployment` 状態でバンドルが表示されます。

7. バンドルのインストールまたはインストール状態を元に戻すには、次のいずれかを実行します。

- バンドルを `Pending uninstall deployment` 状態から戻す場合は、元に戻すアプリケーションを選択し、[関連付け] を選択します。
- バンドルを `Pending install deployment` 状態から戻す場合は、元に戻すアプリケーションを選択し、[関連付け解除] を選択します。

8. インストールまたはアンインストールを選択したアプリケーションバンドルが保留状態になったら、[アプリケーションのデプロイ] を選択します。

> **Important**
>
> アプリケーションのデプロイ を選択すると、エンドユーザーセッションは終了し WorkSpaces 、アプリケーションのインストールまたはアンインストール中はアクセスできなくなります。

9. アクションを確認するには、「確認」と入力します。[強制] を選択して、[エラー] 状態のアプリケーションバンドルをインストールまたはアンインストールします。

10. アプリケーションバンドルの進行状況をモニターリングするには:

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

b. ナビゲーションペインで、 を選択しますWorkSpaces。[ステータス] には、次のようなステータスが表示されます。

- 更新中 – アプリケーションバンドルの更新はまだ進行中です。
- AVAILABLE / STOPPED - アプリケーションバンドルの更新が完了し、 WorkSpace は元の状態に戻ります。

c. アプリケーションバンドルのインストールまたはアンインストールのステータスをモニタリングするには、 WorkSpace を選択し、詳細の表示 を選択します。[アプリケーション] の [ステータス] には、`Pending install`、`Pending uninstall`、`Installed` などのステータスが表示されます。

> **Note**
>
> マネージドアプリケーションを通じて新しくインストールされたアプリケーションバンドルがライセンス有効化されていないことをユーザーが確認した場合は、手動で WorkSpace 再起動できます。ユーザーは、再起動後にこれらのアプリケーションの使用を開始できます。その他のサポートについては、AWS サポートにお問い合わせください。

Manage アプリケーションを使用した WorkSpaces 変更済み の管理

にアプリケーションバンドルをインストールまたはアンインストールすると WorkSpaces、以下のアクションが既存の設定に影響を与える可能性があります。

- を復元 WorkSpaceする - を復元すると、 が正常 WorkSpace であったときに作成されたこれらのボリュームの最新のスナップショットに基づいて、ルートボリュームとユーザーボリュームの両方が WorkSpace 再作成されます。完全な WorkSpace スナップショットは 12 時間ごとに作成されます。詳細については、「 の復元 WorkSpace」を参照してください。管理アプリケーションを使用して変更された を復元する前に WorkSpaces 、少なくとも 12 時間待ってください。アプリケーションの管理を使用して変更された次の完全なスナップショット WorkSpaces の前に を復元すると、次のようになります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して にインストールされたアプリケーションバンドルは から削除されます WorkSpaces が、ライセンスは引き続き有効になり、それらのアプリケーションに対して に課金 WorkSpaces されます。これらのアプリケーションバンドルを に戻すには、アプリケーション管理ワークフローを再度実行し、アプリケーションをアンインストールして新しく起動してから、再度インストール WorkSpaces する必要があります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して から削除されたアプリケーションバンドルは、 に戻ります WorkSpaces。ただし、ライセンスのアクティブ化が行われないため、これらのアプリケーションバンドルは正しく動作しません。これらのアプリケーションバン

ドルを削除するには、 からこれらのアプリケーションバンドルを手動でアンインストールします WorkSpaces。

- の再構築 WorkSpace - を再構築すると、ルートボリュームが WorkSpace 再作成されます。詳細については、「 の再構築 WorkSpace」を参照してください。Manage applications を使用して WorkSpaces 変更された を再構築すると、次のようになります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して にインストールされたアプリケーションバンドルは、 から削除され、非アクティブ化されます WorkSpaces。これらのアプリケーションを に戻すには、アプリケーション管理ワークフローを再度実行 WorkSpaces する必要があります。
  - アプリケーション管理ワークフロー WorkSpaces を介して から削除されたアプリケーションバンドルは、 にインストールされ、アクティブ化されます WorkSpaces。これらのアプリケーションバンドルを から削除するには WorkSpaces、アプリケーションの管理ワークフローを再度実行する必要があります。
- の移行 WorkSpace - 移行プロセス WorkSpace では、ターゲットバンドルイメージの新しいルートボリュームと、元の の最後に使用可能なスナップショットのユーザーボリュームを使用して、を再作成します WorkSpace。新しい WorkSpace ID WorkSpace を持つ新しい が作成されます。詳細については、「アプリケーションの WorkSpace管理を使用して WorkSpaces 変更された の移行」を参照してください。次の結果になります。
  - ソースからのすべてのアプリケーションバンドル WorkSpaces は削除され、非アクティブ化されます。新しい送信先 WorkSpaces は、送信先 WorkSpaces バンドルからアプリケーションを継承します。ソース WorkSpaces アプリケーションバンドルには 1 か月分の料金が請求されますが、ターゲットバンドルのアプリケーションバンドルには日割り計算された料金が請求されます。

の変更 WorkSpace

を起動したら WorkSpace、次の 3 つの方法で設定を変更できます。

- ルートボリューム (Windows の場合はドライブ C、Linux の場合は /)、およびユーザーボリューム (Windows の場合はドライブ D、Linux の場合は /home) のサイズを変更できます。
- コンピューティングタイプを変更して、新しいバンドルを選択できます。
- が PCoIP AWS バンドルで WorkSpace 作成された場合は、 CLI または Amazon WorkSpaces API を使用してストリーミングプロトコルを変更できます。

の現在の変更状態を確認するには WorkSpace、矢印を選択して、その の詳細を表示します WorkSpace。[状態] に表示される値は、[コンピューティングの変更]、[ストレージの変更]、および [なし] です。

を変更する場合は WorkSpace、ステータスが AVAILABLEまたは である必要がありますSTOPPED。ボリュームサイズとコンピューティングタイプを同時に変更することはできません。

のボリュームサイズまたはコンピューティングタイプを変更すると、 の請求レート WorkSpace が変更されます WorkSpace。

ユーザーがボリュームとコンピューティングタイプを変更できるようにするには、ユーザーのセルフサービス WorkSpace管理機能を有効にする を参照してください。

ボリュームサイズの変更

のルートボリュームとユーザーボリュームのサイズは WorkSpace、それぞれ最大 2000 GB まで増やすことができます。 WorkSpace ルートボリュームとユーザーボリュームには、変更できないセットグループが付属しています。使用可能なグループは以下のとおりです。

[ルート (GB)、ユーザー (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 ～ 2,000、100 ～ 2,000]

ルートボリュームとユーザーボリュームは、暗号化されているかどうかにかかわらず拡張できます。両方のボリュームとも、6 時間に 1 回拡張できます。ただし、ルートボリュームとユーザーボリュームのサイズを同時に増やすことはできません。詳細については、「Limitations for Increasing Volumes」を参照してください。

> **Note**
>
> のボリュームを拡張すると WorkSpace、 は Windows または Linux 内でボリュームのパーティション WorkSpaces を自動的に拡張します。プロセスが完了したら、 を再起動して WorkSpace 変更を有効にする必要があります。

データを確実に保持するために、 の起動後にルートボリュームまたはユーザーボリュームのサイズを縮小することはできません WorkSpace。代わりに、 を起動するときに、これらのボリュームの最小サイズを必ず指定してください WorkSpace。Value、Standard、Performance、Power、または を起動できます。ルートボリュームの場合は最低 PowerPro WorkSpace 80 GB、ユーザーボリュームの場合は 10 GB です。Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または を起動できます。ルートボリュームの場合は GraphicsPro WorkSpace 最低 100 GB、ユーザーボリュームの場合は最低 100 GB です。

WorkSpace ディスクサイズの増加中、ユーザーは でほとんどのタスクを実行できます WorkSpace。ただし、 WorkSpace コンピューティングタイプの変更、 WorkSpace 実行モードの切り替え、 の再構築 WorkSpace、 の再起動 (再起動) はできません WorkSpace。

> **Note**
>
> ディスクサイズの増加 WorkSpaces 中にユーザーが を使用できるようにする場合は、 のボリュームのサイズを変更するSTOPPED前に、 WorkSpaces のステータスが AVAILABLEではなく であることを確認します WorkSpaces。 WorkSpaces が の場合STOPPED、ディスクサイズの増加中は起動できません。

多くの場合、ディスクサイズの拡大プロセスには最長で 2 時間かかります。ただし、多数の のボリュームサイズを変更する場合 WorkSpaces、プロセスにかなり時間がかかることがあります。変更 WorkSpaces する の数が多い場合は、 に連絡してサポートAWS Supportを受けることをお勧めします。

ボリューム増加の制限

- サイズ変更できるのは SSD ボリュームのみです。
- を起動するときは WorkSpace、ボリュームのサイズを変更する前に 6 時間待つ必要があります。
- ルートボリュームとユーザーボリュームのサイズを同時に増やすことはできません。ルートボリュームを増やすには、まずユーザーボリュームを 100 GB に変更する必要があります。この変更を行った後、ルートボリュームを 175 ~ 2000 GB の任意の値に更新できます。ルートボリュームを 175 ~ 2000 GB の任意の値に変更した後、ユーザーボリュームを 100 ~ 2000 GB の任意の値にさらに更新できます。

> **Note**
>
> 両方のボリュームを増やす場合は、最初の操作が終了するまで 20～30 分待ってから 2 番目の操作を開始する必要があります。

- WorkSpace が Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または でない限り GraphicsPro WorkSpace、ユーザーボリュームが 100 GB の場合、ルートボリュームを 175 GB 未満にすることはできません。Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro WorkSpaces では、ルートボリュームとユーザーボリュームの両方を最小 100 GB に設定できます。
- ユーザーボリュームが 50 GB の場合、ルートボリュームを 80 GB 以外に更新することはできません。ルートボリュームが 80 GB の場合、ユーザーボリュームは 10、50、または 100 GB のみに設定できます。

のルートボリュームを変更するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. WorkSpace を選択し、アクション、ルートボリュームの変更を選択します。
4. [Root volume sizes] (ルートボリュームサイズ) でボリュームサイズを選択するか、[Custom] (カスタム) を選択してカスタムボリュームサイズを入力します。
5. [変更の保存] をクリックします。
6. ディスクサイズの増加が完了したら、 を再起動 WorkSpaceして変更を有効にする必要があります。データ損失を避けるため、 を再起動する前に、開いているファイルが必ず保存してください WorkSpace。

のユーザーボリュームを変更するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. WorkSpace を選択し、アクション、ユーザーボリュームの変更を選択します。
4. [User volume sizes] (ユーザーボリュームサイズ) でボリュームサイズを選択するか、[Custom] (カスタム) を選択してカスタムボリュームサイズを入力します。
5. [変更の保存] をクリックします。

6. ディスクサイズの増加が完了したら、 を再起動 WorkSpaceして変更を有効にする必要があります。データ損失を避けるため、 を再起動する前に、開いているファイルが必ず保存してください WorkSpace。

のボリュームサイズを変更するには WorkSpace

`RootVolumeSizeGib` または `UserVolumeSizeGib`プロパティで modify-workspace-properties コマンドを使用します。

コンピューティングタイプの変更

スタンダード、パワー、パフォーマンス、 PowerPro コンピューティングタイプ WorkSpace の間でを切り替えることができます。これらのコンピューティングタイプの詳細については、「Amazon WorkSpaces バンドル」を参照してください。

> **Note**
>
> - コンピューティングタイプは Graphics.g4dn から GraphicsPro.g4dn、または GraphicsPro.g4dn から Graphics.g4dn に変更できます。Graphics.g4dn および GraphicsPro.g4dn のコンピューティングタイプを他の値に変更することはできません。
> - 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。を WorkSpaces Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「の移行 WorkSpace」を参照してください。
> - Graphics および のコンピューティングタイプを他の値 GraphicsPro に変更することはできません。

コンピューティングの変更をリクエストすると、 は新しいコンピューティングタイプ WorkSpace を使用して WorkSpaces を再起動します。 WorkSpaces は、 のオペレーティングシステム、アプリケーション、データ、およびストレージ設定を保持します WorkSpace。

より大きなコンピューティングタイプは 6 時間に 1 回、より小さなコンピューティングタイプは 30 日に 1 回リクエストできます。新しく起動された の場合 WorkSpace、より大きなコンピューティングタイプをリクエストするには 6 時間待つ必要があります。

WorkSpace コンピューティングタイプの変更が進行中の場合、ユーザーは から切断され WorkSpace、 を使用または変更することはできません WorkSpace。 WorkSpace は、コンピューティングタイプの変更プロセス中に自動的に再起動されます。

> **Important**
>
> データ損失を避けるため、 WorkSpace コンピューティングタイプを変更する前に、開いているドキュメントやその他のアプリケーションファイルを必ず保存してください。

コンピューティングタイプの変更プロセスには、最大 1 時間かかる場合があります。

のコンピューティングタイプを変更するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. WorkSpace を選択し、アクション 、コンピューティングタイプの変更 を選択します。
4. [Compute type] (コンピューティングタイプ) で、コンピューティングタイプを選択します。
5. [変更の保存] をクリックします。

のコンピューティングタイプを変更するには WorkSpace

`ComputeTypeName` プロパティで modify-workspace-properties コマンドを使用します。

プロトコルの変更

WorkSpace が PCoIP バンドルで作成されている場合は、 CLI または Amazon WorkSpaces API AWS を使用してストリーミングプロトコルを変更できます。これにより、移行機能を使用 WorkSpace せずに、既存の を使用してプロトコルを WorkSpace 移行できます。これにより、移行プロセス中に既存の PCoIP WorkSpaces を再作成することなく、 WorkSpaces ストリーミングプロトコル (WSP) を使用してルートボリュームを維持することもできます。

- プロトコルを変更できるのは、 WorkSpace が PCoIP バンドルで作成された場合のみです。
- プロトコルを WSP に変更する前に、 WorkSpace が WSP の次の要件を満たしていることを確認してください WorkSpace。
  - WorkSpaces クライアントが WSP をサポートしている
  - がデプロイされているリージョン WorkSpace が WSP をサポート
  - WSP の IP アドレスとポートの要件が公開されている。詳細については、「 の IP アドレスとポートの要件 WorkSpaces」を参照してください。
  - 現在のバンドルが WSP で確実に利用できる。

- ビデオ会議を最大限に活用するには、Power または PowerPro バンドルのみを使用することをお勧めします。

> **Note**
>
> - プロトコルの変更 WorkSpaces を開始する前に、非本番環境でテストすることを強くお勧めします。
> - プロトコルを PCoIP から WSP に変更し、プロトコルを PCoIP に戻すと、Web Access WorkSpaces を介して に接続できなくなります。

のプロトコルを変更するには WorkSpace

1. 〔オプション] を再起動 WorkSpace し、 AVAILABLE状態になるまで待ってからプロトコルを変更します。
2. 〔オプション] describe-workspaces コマンドを使用して WorkSpace プロパティを一覧表示します。それが AVAILABLE 状態にあり、現在の Protocol が正しいことを確認します。
3. modify-workspace-properties コマンドを使用して、Protocols プロパティを PCOIP からWSP に、またはその逆に変更します。

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> Protocols プロパティは、大文字と小文字が区別されます。PCOIP または WSP を必ず使用してください。

4. コマンドを実行した後、 が WorkSpace 再起動して必要な設定を完了するまでに最大 20 分かかる場合があります。
5. describe-workspaces コマンドを再度使用してプロパティを WorkSpace一覧表示し、それが AVAILABLE状態にあり、現在のProtocolsプロパティが正しいプロトコルに変更されていることを確認します。

> **Note**
>
> - の WorkSpaceプロトコルを変更しても、コンソールのバンドルの説明は更新されません。[Launch Bundle] (バンドルの起動) という表示は変わりません。
> - 20 分経っても が UNHEALTHY状態 WorkSpace のままの場合は、コンソール WorkSpace で を再起動します。

6. これで、 に接続できます WorkSpace。

WorkSpace ブランドをカスタマイズする

Amazon WorkSpaces では、 APIs を使用して WorkSpace、独自のブランドロゴ、IT サポート情報、パスワードを忘れた場合のリンク、ログインメッセージで のログインページの外観をカスタマイズすることで、ユーザーに使い慣れた WorkSpaces エクスペリエンスを作成できます。ブランドは、デフォルトの WorkSpaces ブランドではなく WorkSpace ログインページに表示されます。

以下のクライアントをサポートしています。

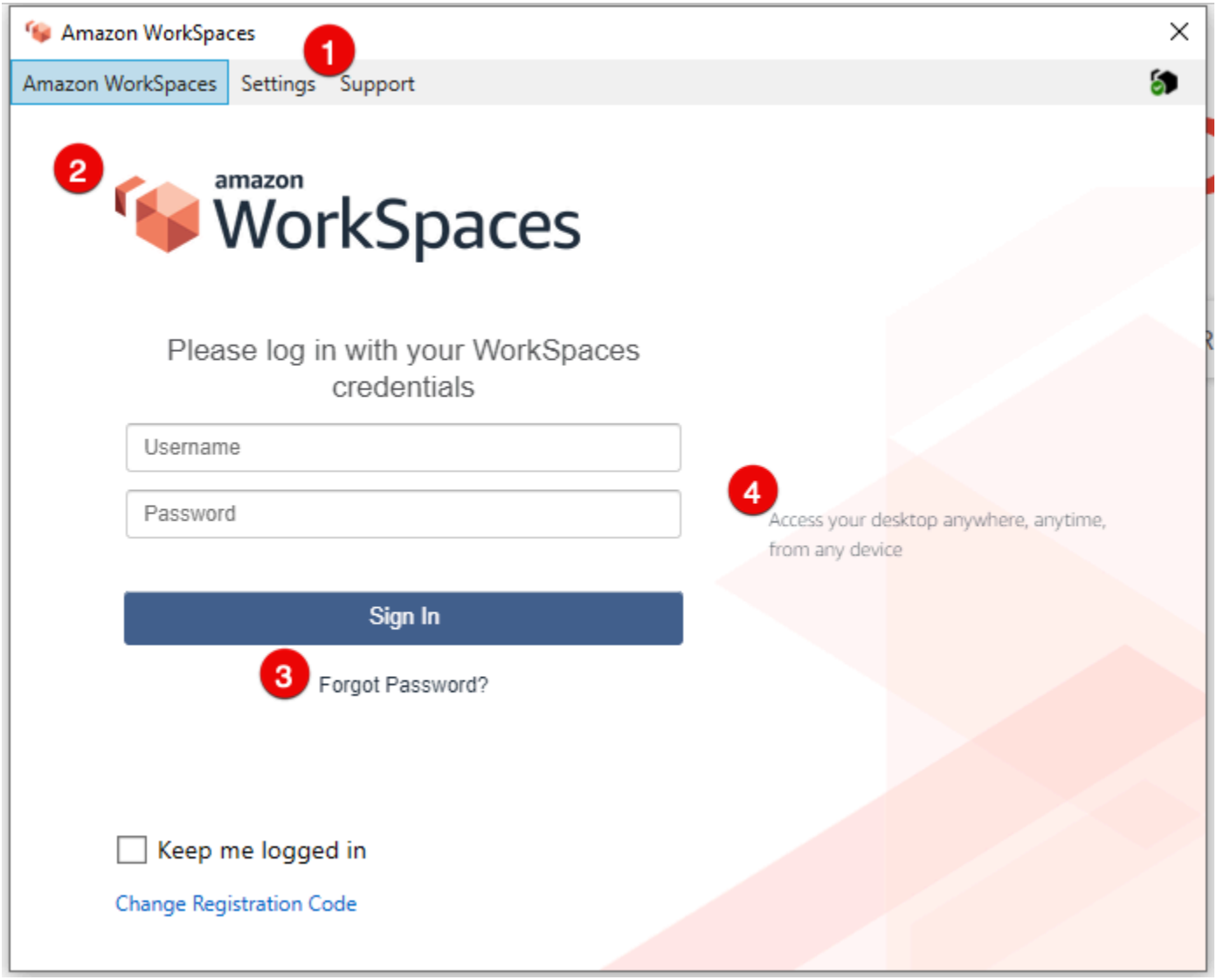
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> ClientBranding APIs を使用してブランド要素を変更するにはAWS GovCloud (US) Region、5.10.0 の WorkSpaces クライアントバージョンを使用します。

カスタムブランドのインポート

クライアントのカスタムブランドをインポートするには、`ImportClientBranding` のアクションを使用します。アクションには以下の要素が含まれます。詳細については、ImportClientBranding「 API リファレンス」を参照してください。

> **Important**
>
> クライアントのブランド属性は公開されています。機密情報が含まれないようにしてください。



1. サポートリンク

2. ロゴ

3. パスワードを忘れた場合のリンク

4. ログインメッセージ

カスタムブランドの要素

ブランド要素	説明	要件と推奨事項
サポートリンク	ユーザーが に関するヘルプを受けるためのサポート E メールリンクを指定できます WorkSpaces。SupportEmail 属性を使用するか、SupportLink 属性を使用してサポートページへのリンクを提供することで指定できます。	• 各プラットフォームタイプでは、SupportEmail と SupportLink パラメータは相互に排他的です。プラットフォームタイプごとに 1 つのパラメータを指定できますが、両方指定することはできません。 • デフォルトの E メールは workspaces-feedback@amazon.com です。 • 長さの制限: 最小長は 1 です。最大長は 200 です。

ロゴ	Logo 属性を使用して、組織のロゴをカスタマイズできます。	• イメージ形式は、.png ファイルから変換したバイナリ形式のデータオブジェクトのみ使用できます。
		• 推奨解像度:
		  • Android: 978 x 190
		  • デスクトップ: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1650 x 300

パスワードを忘れた場合のリンク	ユーザーが のパスワードを忘れた場合に移動できる ForgotPasswordLink 属性を使	長さの制限：最小長は 1 です。最大長は 200 です。

ブランド要素	説明	要件と推奨事項
	用して、ウェブアドレスを追加できます WorkSpace。	
ログインメッセージ	`LoginMessage` 属性を使用して、サインイン画面のメッセージをカスタマイズできます。	• 長さの制限: 最小長は 0 です。HTML タグおよび異なるフォントサイズを統合するための最大長は 2,000 文字です。HTML タグがないデフォルトの場合は、ログインメッセージは 600 文字未満にすることをお勧めします。 • サポートされている HTML タグ: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

以下は、 を使用するためのサンプルコードスニペットです ImportClientBranding。

AWS CLI バージョン 2

> **Warning**
> カスタムブランディングをインポートすると、カスタムデータで指定したプラットフォーム内の属性が上書きされます。また、デフォルトのカスタムブランディング属性値で指定していない属性も上書きされます。上書きしたくない属性のデータを含める必要があります。

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
```

```
--region us-west-2
```

インポート JSON ファイルは、以下のようなサンプルコードになります。

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

次のサンプル Java コードスニペットは、ロゴイメージを base64 でエンコードされた文字列に変換します。

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

次のサンプル Python コードスニペットは、ロゴイメージを base64 でエンコードされた文字列に変換します。

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> カスタムブランディングをインポートすると、カスタムデータで指定したプラットフォーム内の属性が上書きされます。また、デフォルトのカスタムブランディング属性値で指定していない属性も上書きされます。上書きしたくない属性のデータを含める必要があります。

```
// Create WS Client
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> カスタムブランディングをインポートすると、カスタムデータで指定したプラットフォーム内の属性が上書きされます。また、デフォルトのカスタムブランディング属性値で指定していない属性も上書きされます。上書きしたくない属性のデータを含める必要があります。

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)

# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))
```

```
# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

ログインページをプレビューするには、 WorkSpaces アプリケーションまたはウェブログインページを起動します。

> **Note**
>
> 変更が表示されるまでに最大 1 分程度かかる場合があります。

カスタムブランドの説明

現在使用しているクライアントブランドのカスタマイズの詳細を表示するには、DescribeCustomBranding のアクションを使用します。以下は、 を使用するためのサンプルスクリプトです DescribeClientBranding。詳細については、 DescribeClientBranding 「 API リファレンス」を参照してください。

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

カスタムブランドの削除

クライアントブランドのカスタマイズを削除するには、DeleteCustomBranding のアクションを使用します。以下は、 を使用するためのサンプルスクリプトです DeleteClientBranding。詳細については、 DeleteClientBranding 「 API リファレンス」を参照してください。

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> 変更が表示されるまでに最大 1 分程度かかる場合があります。

WorkSpaces のリソースにタグを付ける

WorkSpaces 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。タグの使用は、AWS リソースの管理やデータ (請求データなど) の整理を行うシンプルかつ強力な方法です。

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 WorkSpace にタグを追加した場合、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 Billing 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 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 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 時間後に表示されますが、こ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 リソースにその期間中に料金が発生する必要があります。[Cost Explorer] には、タグが有効化されてからそれまで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、インポートされたイメージ、および IP アクセスコントロールグループの各リソースは、作成時にタグを追加できます。
- 既存のリソースタイプ (WorkSpaces、登録されたディレクトリ、カスタムバンドル、イメージ、および IP アクセスコントロールグループ) にタグを追加できます。

タグの制限

- リソースあたりのタグの最大数 – 50
- キーの最大長 – 127 文字 (Unicode)
- 値の最大長 – 255 文字 (Unicode)
- 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。
- タグの名前または値に `aws:` または `aws:workspaces:` プレフィックスは使用しないでください。これらのプレフィックスは AWS 用に予約されています。これら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 (ディレクトリ、WorkSpaces、または IP アクセスコントロールグループ) を使用して既存のリソースのタグを更新するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、ディレクトリ、WorkSpaces、または IP アクセスコントロール のいずれかのリソースタイプを選択します。
3. リソースを選択して、詳細ページを開きます。
4. 次の 1 つ以上の操作を行います。
   - タグを更新するには、[Key] と [Value] の値を編集します。
   - 新しいタグを追加するには、[Add Tag] を選択し、[Key] と [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アイコン (X) を選択します。
5. タグの更新を完了したら、[Save] (保存) を選択します。

コンソールを使用して既存のリソースのタグを更新するには (イメージまたはバンドル)

1. WorkSpaces コンソール (https://console.aws.amazon.com/workspaces/) を開きます。
2. ナビゲーションペインで、[Bundles] (バンドル) または [Images] (イメージ) のうち、いずれかのリソースタイプを選択します。
3. リソースを選択して、詳細ページを開きます。
4. [タグ] で、[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。

- タグを更新するには、[Key] と [Value] の値を編集します。
- 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. タグの更新を完了したら、[Save changes] (変更の保存) を選択します。

を使用して既存のリソースのタグを更新するにはAWS CLI

create-tags および delete-tags コマンドを使用します。

WorkSpace のメンテナンス

WorkSpaces を定期的にメンテナンスすることをお勧めします。WorkSpaces は、WorkSpaces のデフォルトのメンテナンスウィンドウをスケジュールします。メンテナンスウィンドウ中に、WorkSpace は必要に応じて重要な更新を Amazon WorkSpaces からインストールして再起動します。オペレーティングシステムの更新プログラム (利用可能な場合) は、WorkSpace が使用するように設定されている OS アップデートサーバーからもインストールされます。メンテナンス中は、WorkSpaces が使用できないことがあります。

デフォルトでは、Windows WorkSpaces は Windows Update から更新プログラムを受信するように設定されています。ユーザー独自の Windows 自動更新メカニズムを設定する方法については、Windows Server Update Services (WSUS) および Configuration Manager のドキュメントを参照してください。

要件

オペレーティングシステムの更新をインストールしてアプリケーションをデプロイできるように、WorkSpaces はインターネットにアクセスできる必要があります。詳細については、「the section called “インターネットアクセス”」を参照してください。

AlwaysOn WorkSpaces のメンテナンスウィンドウ

AlwaysOn WorkSpaces では、メンテナンスウィンドウはオペレーティングシステムの設定によって決まります。デフォルトは、WorkSpace のタイムゾーンの、毎週日曜日午前 0:00 ~ 4:00 の 4 時間です。デフォルトでは、AlwaysOn WorkSpace のタイムゾーンは、WorkSpace の AWS リージョンのタイムゾーンです。ただし、別のリージョンから接続し、タイムゾーンリダイレクトが有効にされた後に切断した場合は、WorkSpace のタイムゾーンは、接続元リージョンのタイムゾーンに更新されます。

グループポリシーを使用して、Windows WorkSpaces のタイムゾーンリダイレクトを無効にすることができます。Linux WorkSpaces のタイムゾーンのリダイレクトを無効にするには、PCoIP エージェントの設定を使用します。

Windows WorkSpaces には、グループポリシーを使用してメンテナンスウィンドウを設定できます。「自動更新のためのグループポリシーの設定」を参照してください。Linux WorkSpaces のメンテナンスウィンドウを設定することはできません。

AutoStop WorkSpaces のメンテナンスウィンドウ

AutoStop WorkSpaces は重要な更新をインストールするために月に 1 度自動的に開始されます。その月の第 3 月曜日から開始して、2 週間、WorkSpace の AWS リージョンのタイムゾーンの毎日 0:00 ~ 5:00 に、メンテナンスウィンドウが開かれます。WorkSpace はメンテナンスウィンドウのいずれかの日に保守されます。このウィンドウでは、7 日間を超えて経過した WorkSpaces のみが保守されます。

WorkSpace のメンテナンス期間中、WorkSpace の状態は `MAINTENANCE` に設定されます。

AutoStop WorkSpaces のメンテナンスに使用するタイムゾーンを変更することはできませんが、以下のようにして AutoStop WorkSpaces のメンテナンスウィンドウを無効にすることはできます。メンテナンスモードを無効にすると、WorkSpaces は再起動されず、`MAINTENANCE` 状態になりません。

メンテナンスモードを無効にするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [メンテナンスモード] を展開します。
5. 自動更新を有効にするには、[Enabled] を選択します。更新を手動で管理する場合は、[無効] を選択します。
6. [Update and Exit] を選択します。

手動メンテナンス

必要に応じて、独自のスケジュールで WorkSpaces を管理できます。メンテナンスタスクを実行する場合は、WorkSpace の状態を [Maintenance] (メンテナンス) に変更することをお勧めします。完了したら、WorkSpace の状態を [Available] (使用可能) に変更します。

WorkSpace が [Maintenance] (メンテナンス) 状態の場合、以下の動作が発生します。

- WorkSpace は、再起動、停止、起動、再構築には対応しません。
- ユーザーは WorkSpace にログインできません。
- AutoStop WorkSpace は、休止状態ではありません。

コンソールを使用して WorkSpace の状態を変更するには

> **Note**
>
> WorkSpace の状態を変更するには、WorkSpace のステータスが [Available] (使用可能) である必要があります。WorkSpace が [Available] (使用可能) 状態ではない場合、[Modify state] (変更状態) の設定は使用できません。

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. WorkSpace を選択して、[Actions] (アクション)、[Modify state] (状態の変更) の順に選択します。
4. [Modify state] (状態の変更) で、[Available] (使用可能) または [Maintenance] (メンテナンス) を選択します。
5. [Save (保存)] を選択します。

AWS CLI を使用して WorkSpace の状態を変更するには

modify-workspace-state コマンドを使用します。

暗号化済み WorkSpaces

WorkSpaces は AWS Key Management Service () と統合されていますAWS KMS。これにより、AWS KMS キー WorkSpaces を使用して のストレージボリュームを暗号化できます。を起動すると WorkSpace、ルートボリューム (Microsoft Windows の場合は C ドライブ、Linux の場合は /) とユーザーボリューム (Windows の場合は D ドライブ、Linux の場合は /home) を暗号化できます。これにより、保管時のデータ、ボリュームへのディスク I/O、ボリュームから作成されたスナップショットを暗号化することができます。

> **Note**
>
> の暗号化に加えて WorkSpaces、特定の AWS 米国リージョンで FIPS エンドポイント暗号化を使用することもできます。詳細については、「FedRAMP 認証または DoD SRG 準拠のために Amazon WorkSpaces をセットアップする」を参照してください。

内容

前提条件

暗号化プロセスを開始する前に、 AWS KMS キーが必要です。この KMS キーは、Amazon 用の AWS マネージド KMS キー WorkSpaces （ aws/workspaces ）または対称カスタマーマネージド KMS キー のいずれかです。

- AWS マネージド KMS キー – リージョンで WorkSpaces コンソール WorkSpace から暗号化されていない を初めて起動すると、Amazon はアカウントに AWS マネージド KMS キー (aws/workspaces) WorkSpaces を自動的に作成します。この AWS マネージド KMS キーを選択して、のユーザーボリュームとルートボリュームを暗号化できます WorkSpace。詳細については、「を使用した WorkSpaces 暗号化の概要 AWS KMS」を参照してください。

  この AWS マネージド KMS キーは、ポリシーや権限を含めて表示でき、 AWS CloudTrail ログでの使用を追跡できますが、この KMS キーを使用または管理することはできません。Amazon はこの KMS キー WorkSpaces を作成および管理します。この KMS キー WorkSpaces を使用できるのは WorkSpaces Amazon のみで、アカウント内の WorkSpaces リソースの暗号化にのみ使用できます。

AWS Amazon が WorkSpaces サポートする マネージド KMS キーは、3 年ごとにローテーションされます。詳細については、「 AWS Key Management Service デベロッパーガイド」の AWS KMS 「キーのローテーション」を参照してください。

- カスタマーマネージド KMS キー – または、 を使用して作成した対称カスタマーマネージド KMS キーを選択できます AWS KMS。ポリシーの設定を含め、この KMS キーを表示、使用、管理できます。KMS キーの作成の詳細については、 AWS Key Management Service デベロッパーガイドの キーの作成 を参照してください。 AWS KMS API を使用した KMS キーの作成の詳細については、「 AWS Key Management Service デベロッパーガイド」の「キーの使用」を参照してください。

  自動キー更新を有効にしない限り、カスタマー管理の KMS キー は自動的に更新されません。詳細については、「 AWS Key Management Service デベロッパーガイド」の AWS KMS 「キーのローテーション」を参照してください。

> **Important**
>
> KMS キーを手動でローテーションするときは、元の KMS キーと新しい KMS キーの両方を有効にしたままにして、 が元の KMS キー WorkSpaces が暗号化した を復号 AWS KMS できるようにする必要があります。元の KMS キーを有効にしたくない場合は、 を再作成 WorkSpacesし、新しい KMS キーを使用して暗号化する必要があります。

AWS KMS キーを使用して を暗号化するには、次の要件を満たす必要があります WorkSpaces。

- KMS キーは対称である必要があります。Amazon WorkSpaces は非対称 KMS キーをサポートしていません。対称 KMS キーと非対称 KMS キーの区別については、「AWS Key Management Service デベロッパーガイド」の「対称および非対称 KMS キーを識別する」を参照してください。
- KMS キーを有効にする必要があります。KMS キーが有効になっているかどうかを確認する方法については、「AWS Key Management Service デベロッパーガイド」の 「コンソールで KMS キーを表示する」を参照してください。
- KMS キーに正しいアクセス権限とポリシーを関連付ける必要があります。詳細については、「パート 2: IAM ポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する」を参照してください。

制限

- 既存の を暗号化することはできません WorkSpace。を起動 WorkSpace するときに を暗号化する必要があります。
- 暗号化された からのカスタムイメージの作成 WorkSpace はサポートされていません。
- 暗号化された の暗号化の無効化 WorkSpace は現在サポートされていません。
- WorkSpaces ルートボリューム暗号化を有効にして起動すると、プロビジョニングに最大 1 時間かかる場合があります。
- 暗号化された を再起動または再構築するには WorkSpace、まず キーが有効になっていることを確認します AWS KMS 。有効でない場合、 WorkSpace は使用できなくなります。KMS キーが有効になっているかどうかを確認する方法については、「AWS Key Management Service デベロッパーガイド」の 「コンソールで KMS キーを表示する」を参照してください。

を使用した WorkSpaces 暗号化の概要 AWS KMS

暗号化されたボリューム WorkSpaces で を作成すると、 WorkSpaces は Amazon Elastic Block Store (Amazon EBS) を使用してそれらのボリュームを作成および管理します。Amazon EBS は、業界標準の AES-256 アルゴリズムを使用してデータキーでボリュームを暗号化します。Amazon EBS と Amazon はどちらも KMS キーを使用して暗号化されたボリュームを操作し WorkSpaces ます。EBS ボリュームの暗号化の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。 Amazon EC2

暗号化されたボリューム WorkSpaces で を起動すると、 end-to-end プロセスは次のように動作します。

1. 暗号化に使用する KMS キーと、 のユーザーとディレクトリを指定します WorkSpace。このアクションは、 が KMS キーをこの目的のみ、 WorkSpaceつまり指定されたユーザーとディレクトリに関連付けられた に対して WorkSpaceのみ使用 WorkSpaces できるようにする許可を作成します。
2. WorkSpaces は、 の暗号化された EBS ボリューム WorkSpace を作成し、使用する KMS キーと、ボリュームのユーザーとディレクトリを指定します。このアクションは、Amazon EBS がこの WorkSpace とボリュームにのみ、つまり指定されたユーザーとディレクトリ WorkSpace に関連付けられた と指定されたボリュームにのみ KMS キーを使用できるようにする許可を作成します。
3. Amazon EBS は、KMS キーで暗号化されたボリュームデータキーをリクエストし、WorkSpace ユーザーの Active Directory セキュリティ識別子 (SID) と AWS Directory Service

ディレクトリ ID、および暗号化コンテキスト として Amazon EBS ボリューム ID を指定します。

4. AWS KMS は新しいデータキーを作成し、KMS キーで暗号化してから、暗号化されたデータキーを Amazon EBS に送信します。
5. WorkSpaces は Amazon EBS を使用して、暗号化されたボリュームを にアタッチします WorkSpace。Amazon EBS は、暗号化されたデータキーを `Decrypt` リクエスト AWS KMS とともに に送信し、暗号化コンテキストとして使用される WorkSpace ユーザーの SID、ディレクトリ ID、ボリューム ID を指定します。
6. AWS KMS は KMS キーを使用してデータキーを復号し、プレーンテキストのデータキーを Amazon EBS に送信します。
7. Amazon EBS は、プレーンテキストデータキーを使用して、暗号化されたボリュームを出入りするすべてのデータを暗号化します。Amazon EBS は、ボリュームが にアタッチされている限り、プレーンテキストのデータキーをメモリに保持します WorkSpace。
8. Amazon EBS は、 を再起動または再構築する場合に備えて、暗号化されたデータキー (で受信Step 4) をボリュームメタデータとともに保存します WorkSpace。
9. を使用して AWS Management Console を削除する WorkSpace （ または WorkSpaces API で `TerminateWorkspaces`アクションを使用する) WorkSpaces と、Amazon EBS はその の KMS キーの使用を許可した許可を廃止します WorkSpace。

WorkSpaces 暗号化コンテキスト

WorkSpaces は、暗号化オペレーション (`Encrypt`、、 など) に KMS キーを直接使用しません。つまり`GenerateDataKey`、 WorkSpaces は暗号化コンテキスト AWS KMS を含む `Decrypt`にリクエストを送信しません。ただし、Amazon EBS が WorkSpaces （ Step 3 の を使用した WorkSpaces 暗号化の概要 AWS KMS) の暗号化されたボリュームの暗号化されたデータキーをリクエストし、そのデータキーのプレーンテキストコピー (Step 5) をリクエストすると、リクエストに暗号化コンテキストが含まれます。

暗号化コンテキストは、データの整合性を確保するために が使用する追加の認証データ (AAD) を提供します。 AWS KMS 暗号化コンテキストは AWS CloudTrail ログファイルにも書き込まれるため、特定の KMS キーが使用された理由を理解するのに役立ちます。Amazon EBS では、暗号化コンテキストとして次のものが使用されます。

- に関連付けられている Active Directory ユーザーのセキュリティ識別子 (SID) WorkSpace
- に関連付けられているディレクトリの AWS Directory Service ディレクトリ ID WorkSpace

- 暗号化されたボリュームの Amazon EBS ボリューム ID

次の例は、Amazon EBS が使用する暗号化コンテキストの JSON 表現を示しています。

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

ユーザーに代わって KMS キーを使用する WorkSpaces アクセス許可を付与する

(aws/workspaces) の AWS マネージド KMS キー WorkSpacesまたはカスタマーマネージド KMS キーで WorkSpace データを保護できます。カスタマーマネージド KMS キーを使用する場合は、アカウントの WorkSpaces 管理者に代わって KMS キーを使用する WorkSpaces アクセス許可を付与する必要があります。の WorkSpaces AWS マネージド KMS キーには、デフォルトで必要なアクセス許可があります。

カスタマーマネージド KMS キーを で使用する準備をするには WorkSpaces、次の手順を使用します。

1. KMS キーのキーポリシーのキーユーザーのリストに WorkSpaces 管理者を追加する
2. IAM ポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する

WorkSpaces 管理者には、 を使用するためのアクセス許可も必要です WorkSpaces。これらのアクセス許可の詳細については、WorkSpaces の Identity and Access Management にアクセスしてください。

パート 1: WorkSpaces 管理者をキーユーザーとして に追加する

WorkSpaces 管理者に必要なアクセス許可を付与するには、 AWS Management Console または AWS KMS API を使用できます。

KMS キーのキーユーザーとして WorkSpaces 管理者を追加するには (コンソール)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/kms で AWS Key Management Service （ AWS KMS) コンソールを開きます。

2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクタを使用します。
3. ナビゲーションペインで、[Customer managed keys] (カスタマー管理型のキー) を選択します。
4. 任意のカスタマーマネージドキーの KMS キーのキー ID またはエイリアスを選択する
5. [キーポリシー] タブを選択します。[Key users] (キーユーザー) で [Add] (追加) を選択します。
6. IAM ユーザーとロールのリストで、 WorkSpaces 管理者に対応するユーザーとロールを選択し、 の追加を選択します。

KMS キーのキーユーザーとして WorkSpaces 管理者を追加するには (API)

1. GetKeyポリシーオペレーションを使用して既存のキーポリシーを取得し、ポリシードキュメントを ファイルに保存します。
2. 任意のテキストエディタでポリシードキュメントを開きます。 WorkSpaces 管理者に対応する IAM ユーザーとロールを、キーユーザー にアクセス許可を付与するポリシーステートメントに追加します。その後、ファイルを保存します。
3. PutKeyポリシーオペレーションを使用して、キーポリシーを KMS キーに適用します。

パート 2: IAM ポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する

暗号化に使用するカスタマー管理の KMS キーを選択する場合は、暗号化された を起動するアカウントの IAM ユーザーに代わって Amazon が KMS キー WorkSpaces を使用できるようにする IAM ポリシーを確立する必要があります WorkSpaces。そのユーザーには、Amazon を使用するためのアクセス許可も必要です WorkSpaces。IAM ユーザーポリシーの作成と編集の詳細については、IAM ユーザーガイドの IAM ポリシーを管理するおよび WorkSpaces の Identity and Access Management を参照してください。

WorkSpaces 暗号化には、KMS キーへの制限付きアクセスが必要です。以下は、使用できるサンプルキーのポリシーです。このポリシーにより、 AWS KMS キーを管理できるプリンシパルと、このキーを使用できるプリンシパルが分離されます。このサンプルキーポリシーを使用する前に、サンプルアカウント ID と IAM ユーザー名を、アカウントの実際の値に置き換えてください。

最初のステートメントは、デフォルトの AWS KMS キーポリシーと一致します。これにより、IAM ポリシーを使用して KMS キーへのアクセスを制御するためのアクセス許可がアカウントに付与されます。2 番目のステートメントと 3 番目のステートメントは、キーを管理および使用できる AWS プリンシパルをそれぞれ定義します。4 番目のステートメントでは、 と統合された AWS サービスが、

指定されたプリンシパルに代わって キー AWS KMS を使用できるようにします。このステートメントは、 AWS のサービスが許可を作成、管理できるようにします。ステートメントは、KMS キーに対する許可を、アカウントのユーザーに代わって AWS のサービスによって行われた許可に制限する条件要素を使用します。

> **Note**
>
> WorkSpaces 管理者が を使用して暗号化されたボリューム WorkSpaces で AWS Management Console を作成する場合、管理者にはエイリアスとリストキー ("kms:ListAliases"および のアクセス許可) の"kms:ListKeys"アクセス許可が必要です。 WorkSpaces 管理者が (コンソールではなく) Amazon WorkSpaces API のみを使用している場合は、 "kms:ListAliases"および アクセス"kms:ListKeys"許可を省略できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

を暗号化するユーザーまたはロールの IAM ポリシーには、カスタマー管理の KMS キーの使用許可と、 へのアクセス許可が含まれている WorkSpace 必要があります WorkSpaces。IAM ユーザーまたはロールにアクセス WorkSpaces 許可を付与するには、次のサンプルポリシーを IAM ユーザーまたはロールにアタッチします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
```

```
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

ユーザーが を使用するには、次の IAM ポリシーが必要です AWS KMSこれにより、KMS キーへの読み取り専用アクセスと、許可を作成する能力がユーザーに付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

ポリシーで KMS キーを指定する場合は、次のような IAM ポリシーを使用します。サンプルKMS キー ARN を有効なものに置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

を暗号化する WorkSpace

を暗号化するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. 起動 WorkSpacesを選択し、最初の 3 つのステップを完了します。
3. WorkSpaces 設定ステップでは、次の操作を行います。
   a. 暗号化するボリュームを選択します。[Root Volume]、[User Volume]、または両方のボリュームとなります。
   b. 暗号化キー で、Amazon によって作成された AWS マネージド KMS キー WorkSpaces または作成した KMS キー AWS KMS のいずれかのキーを選択します。選択する KMS キーは対称である必要があります。Amazon WorkSpaces は非対称 KMS キーをサポートしていません。
   c. [Next Step (次のステップ)] をクリックします。
4. 起動 を選択します WorkSpaces。

暗号化された を表示する WorkSpaces

WorkSpaces コンソールから暗号化された ボリューム WorkSpaces と ボリュームを確認するには、左側のナビゲーションバーWorkSpacesから を選択します。Volume Encryption 列には、各 WorkSpace で暗号化が有効か無効かが表示されます。暗号化されている特定のボリュームを確認するには、 WorkSpace エントリを展開して Encrypted Volumes フィールドを表示します。

の再起動 WorkSpace

場合によっては、 WorkSpace を手動で再起動 (再起動) する必要があります。再起動すると、ユーザーは WorkSpace 切断され、 のシャットダウンと再起動が実行されます WorkSpace。データ損失を避けるため、 を再起動する前に、開いているドキュメントやその他のアプリケーションファイル

を必ず保存してください WorkSpace。ユーザーデータ、オペレーティングシステム、およびシステム設定には影響しません。

> **Warning**
>
> 暗号化された を再起動するには WorkSpace、まず AWS KMS キーが有効になっていることを確認します。有効でない場合、 WorkSpace は使用できなくなります。KMS キーが有効になっているかどうかを確認する方法については、「AWS Key Management Service デベロッパーガイド」の 「コンソールで KMS キーを表示する」を参照してください。

を再起動するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. 再起動 WorkSpaces する を選択し、アクション 、再起動 WorkSpacesを選択します。
4. 確認を求められたら、 の再起動 WorkSpacesを選択します。

WorkSpace を使用して を再起動するには AWS CLI

reboot-workspaces コマンドを使用します。

一括再起動するには WorkSpaces

を使用しますamazon-workspaces-admin-module。

の再構築 WorkSpace

を再構築すると、 が起動 WorkSpace されたバンドルの最新のイメージのルートボリューム、そのユーザーボリューム、およびそのプライマリ Elastic Network Interface が WorkSpace 再作成されます。を再構築すると、 を復元するよりも多くのデータが WorkSpace 削除されますが WorkSpace、必要なのはユーザーボリュームのスナップショットのみです。を復元するには、 WorkSpace「」を参照してくださいWorkSpace の復元。

を再構築 WorkSpace すると、次のようになります。

- ルートボリューム (Microsoft Windows の場合はドライブ C、Linux の場合は /) は、 WorkSpace が作成されたバンドルの最新のイメージで更新されます。インストールされたアプリケーション、または WorkSpace の作成後に変更されたシステム設定はすべて失われます。

- ユーザーボリューム (Microsoft Windows の場合は D: ドライブ、Linux の場合は /home) が、最新のスナップショットから再作成されます。ユーザーボリュームの現在の内容は上書きされます。

  の再構築時に使用する自動スナップショット WorkSpace は 12 時間ごとにスケジュールされます。ユーザーボリュームのこれらのスナップショットは、 の状態に関係なく作成されます WorkSpace。Actions 、Rebuild / Restore WorkSpaceを選択すると、最新のスナップショットの日時が表示されます。

  を再構築すると WorkSpace、再構築の完了後すぐに (多くの場合 30 分以内に) 新しいスナップショットも作成されます。
- プライマリ Elastic Network Interface が再作成されます。は新しいプライベート IP アドレス WorkSpace を受け取ります。

> **Important**
>
> 2020 年 1 月 14 日以降、パブリック Windows 7 バンドルから WorkSpaces 作成された は再構築できなくなります。Windows 7 から Windows 10 WorkSpaces への移行を検討してください。詳細については、「の移行 WorkSpace」を参照してください。

を再構築できるのは、次の条件が満たされた場合 WorkSpace のみです。

- の状態は、AVAILABLE、、ERROR、UNHEALTHY、STOPPEDまたは WorkSpace である必要がありますREBOOTING。 WorkSpace REBOOTING 状態の を再構築するには、 RebuildWorkspaces API オペレーションまたは rebuild-workspaces AWS CLI コマンドを使用する必要があります。
- ユーザーボリュームのスナップショットが存在する必要があります。

を再構築するには WorkSpace

> **Warning**
>
> 暗号化された を再構築するには WorkSpace、まず AWS KMS キーが有効になっていることを確認します。有効でない場合、 WorkSpace は使用できなくなります。KMS キーが有効になっているかどうかを確認する方法については、「AWS Key Management Service デベロッパーガイド」の 「コンソールで KMS キーを表示する」を参照してください。

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. 再構築 WorkSpace する を選択し、アクション 、再構築/復元 WorkSpaceを選択します。
4. [Snapshot] (スナップショット) で、スナップショットのタイムスタンプを選択します。
5. [Rebuild] を選択します。

WorkSpace を使用して を再構築するには AWS CLI

rebuild-workspaces コマンドを使用します。

トラブルシューティング

Active Directory でユーザーの sAMAccountName ユーザー命名属性を変更 WorkSpace した後に を再構築すると、次のエラーメッセージが表示されることがあります。

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

この問題を回避するには、元のユーザー命名属性に戻ってから再構築を再開するか、そのユーザー WorkSpace 用に新しい を作成します。

WorkSpace の復元

WorkSpace を復元すると、WorkSpace が正常であったときに作成したこれらのボリュームの最新スナップショットに基づいて、ルートボリュームとユーザーボリュームの両方が再作成されます。WorkSpace を復元すると、WorkSpace を再構築するよりも削除されるデータが少なくなります。ただし、WorkSpace の再構築にはユーザーボリュームのスナップショットのみが必要であるのに対して、ルートボリュームとユーザーボリュームの両方のスナップショットが必要になります。WorkSpace を再構築するには、「の再構築 WorkSpace」を参照してください。

WorkSpace を復元すると、次の状況が発生します。

- ルートボリューム (Microsoft Windows の場合はドライブ C、Linux の場合は /) が最新のスナップショットに復元されます。最後にスナップショットが作成された後にインストールされたアプリケーション、または変更されたシステム設定は失われます。
- ユーザーボリューム (Microsoft Windows の場合は D: ドライブ、Linux の場合は /home) が、最新のスナップショットから再作成されます。ユーザーボリュームの現在の内容は上書きされます。

スナップショットが作成される場合

ルートボリュームとユーザーボリュームのスナップショットは、次の基準で取得されます。[Actions] (アクション)、[Rebuild / Restore WorkSpace] (WorkSpace のリビルドとリストア) を選択すると、最新のスナップショットの日付と時刻が表示されます。

- WorkSpace が最初に作成された後 — 通常、ルートボリュームとユーザーボリュームの最初のスナップショットは、WorkSpace の作成後すぐに (多くの場合 30 分以内に) 作成されます。AWS リージョンによっては、WorkSpace の作成後に最初のスナップショットが作成されるまで数時間かかる場合があります。

  最初のスナップショットが作成される前に WorkSpace が異常になった場合、WorkSpace を復元することはできません。その場合は、WorkSpace の再構築を試みるか、AWS Support にお問い合わせください。
- 通常使用中 — WorkSpace の復元時に使用する自動スナップショットは、12 時間ごとにスケジュールされます。WorkSpace が正常であれば、ルートボリュームとユーザーボリュームの両方のスナップショットがほぼ同時に作成されます。WorkSpace に不具合がある場合、スナップショットはユーザーボリュームに対してのみ作成されます。
- WorkSpace が復元された後 — WorkSpace を復元すると、復元が完了した直後に (多くの場合 30 分以内に) 新しいスナップショットが作成されます。AWS リージョンによっては、WorkSpace の復元後にこれらのスナップショットが作成されるまで数時間かかる場合があります。

  WorkSpace を復元した後、新しいスナップショットを作成する前に WorkSpace が異常になった場合、WorkSpace を再び復元することはできません。その場合は、WorkSpace の再構築を試みるか、AWS Support にお問い合わせください。

WorkSpace を復元できるのは、次の条件が満たされている場合のみです。

- WorkSpace の状態は、`AVAILABLE`、`ERROR`、`UNHEALTHY`、または `STOPPED` である必要があります。
- ルートボリュームとユーザーボリュームのスナップショットが存在する必要があります。

WorkSpace を復元するには

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。

3. 復元する WorkSpace を選択したら、[Actions] (アクション)、[Rebuild / Restore WorkSpace] (WorkSpace の再ビルド / 復元) の順に選択します。
4. [Snapshot] (スナップショット) で、スナップショットのタイムスタンプを選択します。
5. [復元] を選択します。

AWS CLI を使用して WorkSpace を復元するには

restore-workspace コマンドを使用します。

Microsoft 365 Bring Your Own License (BYOL)

Amazon WorkSpaces では、Microsoft のライセンス要件を満たしている場合は、独自の Microsoft 365 ライセンスを持ち込むことができます。これらのライセンスにより、以下のオペレーティングシステム WorkSpaces を搭載した で Microsoft 365 Apps for enterprise ソフトウェアをインストールしてアクティブ化できます。

- Windows 10 (Bring Your Own License)
- Windows 11 (Bring Your Own License)
- Windows Server 2016
- [Windows Server 2019]
- Windows Server 2022

で Microsoft 365 Apps for enterprise を使用するには WorkSpaces、Microsoft 365 E3/E5、Microsoft 365 A3/A5、または Microsoft 365 Business Premium のサブスクリプションが必要です。

Amazon WorkSpaces では、Microsoft 365 ライセンスを使用して、以下を含む Microsoft 365 Apps for enterprise をインストールしてアクティブ化できます。

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

詳細については、Microsoft 365 Apps for enterprise の詳細なリストを参照してください。

Microsoft Project、Microsoft Visio、Microsoft Power Automate など、Microsoft 365 に含まれていない Microsoft アプリケーションをインストールすることもできます WorkSpaces が、独自の追加ライセンスを導入する必要があります。

WorkSpaces マルチリージョンレジリエンス を使用して、プライマリ WorkSpaces およびフェイルオーバーで Microsoft 365 およびその他の Microsoft アプリケーションをインストールして使用できます。

内容

Microsoft 365 Apps for enterprise WorkSpaces で作成する

Microsoft 365 Apps for enterprise WorkSpaces で を作成するには、アプリケーションがインストールされたカスタムイメージを作成し、それを使用してカスタムバンドルを作成する必要があります。バンドルを使用して、アプリケーションがインストールされ WorkSpaces た新しい を起動できます。 WorkSpaces ドメインは、Microsoft 365 Apps for enterprise でパブリックバンドルを提供しません。

Microsoft 365 Apps for enterprise WorkSpaces で を作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. 他の Microsoft アプリケーション のイメージ WorkSpace として使用する を起動します WorkSpaces。ここに Microsoft アプリケーションをインストールします。の起動の詳細については WorkSpace、「 を使用して仮想デスクトップを起動 WorkSpacesする」を参照してください。
3. https://clients.amazonworkspaces.com/ でクライアントアプリケーションを起動し、招待メールに記載されている登録コードを入力して、[登録] を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. Microsoft 365 Apps for enterprise をインストールして設定します。
6. からカスタムイメージを作成し WorkSpace、それを使用してカスタムバンドルを作成します。カスタムイメージとバンドルの作成の詳細については、「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。

7. 作成したカスタムバンドル WorkSpaces を使用して を起動します。これら WorkSpaces には Microsoft 365 Apps for enterprise がインストールされています。

既存の を移行 WorkSpaces して Microsoft 365 Apps for enterprise を使用する

に を通じて Microsoft Office ライセンス WorkSpaces がない場合はAWS、 に Microsoft 365 Apps for enterprise をインストールして設定できます WorkSpaces。

に を通じて Microsoft Office ライセンス WorkSpaces がある場合はAWS、Microsoft 365 Apps for enterprise をインストールする前に、まず Microsoft Office ライセンスを登録解除する必要があります。

Important

から Microsoft Office アプリケーションをアンインストールしても、ライセンスは登録解除 WorkSpaces されません。Microsoft Office ライセンスの課金を回避するには、次のいずれかを実行して、 AWSから Microsoft Office アプリケーション WorkSpaces から を登録解除します。

- アプリケーションの管理 (推奨) – Microsoft Office 2016 および 2019 を からアンインストールできます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。アンインストールしたら、Microsoft 365 Apps for enterprise を にインストールできます WorkSpaces。
- の移行 WorkSpace – ユーザーボリューム上のデータを保持しながら、あるバンドル WorkSpace から別のバンドルに を移行できます。
  - WorkSpaces を Microsoft Office サブスクリプションのないイメージを含むバンドルに移行します。移行が完了したら、Microsoft 365 Apps for enterprise を にインストールできます WorkSpaces。
  - または、イメージに Microsoft 365 Apps for enterprise が既にインストールされているカスタムイメージ WorkSpaces とバンドルを作成し、 WorkSpaces をこの新しいカスタムバンドルに移行します。移行が完了すると、 WorkSpaces ユーザーは Microsoft 365 Apps for enterprise の使用を開始できます。
  - の移行方法の詳細については WorkSpaces、「 の移行 WorkSpace」を参照してください。

で Microsoft 365 Apps for enterprise を更新する WorkSpaces

デフォルトでは、Microsoft Windows オペレーティングシステムで WorkSpaces 実行されているは、Windows Update から更新を受け取るように設定されています。ただし、Microsoft 365 Apps for enterprise の更新プログラムは Windows Update ではご利用いただけません。更新を Office CDN から自動的に実行するように設定するか、Windows Server Update Services (WSUS) を Microsoft Configuration Manager と組み合わせて使用して Microsoft 365 Apps for enterprise を更新します。詳細については、「Microsoft Configuration Manager を使用して Microsoft 365 Apps の更新プログラムを管理する」を参照してください。Microsoft 365 アプリケーションの更新の頻度を設定するには、更新チャネルを指定し、ライセンスポリシーの WorkSpaces Microsoft 365 に準拠するように現行または月次エンタープライズに設定します。

ウィンドウズ BYOL のアップグレード WorkSpaces

Windows 個人所有ライセンス (BYOL) WorkSpaces では、一括アップグレードプロセスを使用して新しいバージョンの Windows にアップグレードできます。アップグレードするには、このトピックの手順に従います。

インプレースアップグレードプロセスは Windows 10 と 11 BYOL にのみ適用されます。WorkSpaces

> **Important**
>
> アップグレードしたバージョンでは Sysprep を実行しないでください。 WorkSpaceその場合、Sysprep が終了できないエラーが発生することがあります。Sysprep を実行する予定がある場合は、まだアップグレードされていないものでのみ実行してください。 WorkSpace

> **Note**
>
> このプロセスを使用して Windows 10 と 11 WorkSpaces を新しいバージョンにアップグレードできます。ただし、このプロセスを使用して Windows 10 WorkSpaces を Windows 11 にアップグレードすることはできません。

コンテンツ

- 考慮事項
- 既知の制限事項
- レジストリキー設定の概要
- インプレースアップグレードの実行
- トラブルシューティング
- WorkSpace スクリプトを使用してレジストリを更新してください。 PowerShell

前提条件

- グループポリシーまたはシステムセンター構成マネージャー (SCCM) を使用して Windows 10 と 11 のアップグレードを延期または一時停止した場合は、Windows 10 と 11 のオペレーティングシステムのアップグレードを有効にします。 WorkSpaces
- WorkSpace がの場合は AutoStop WorkSpace、更新プログラムの適用中に自動的に停止しないように、 AlwaysOn WorkSpace一括アップグレードプロセスの前に変更してください。詳細については、「実行モードを変更する」を参照してください。 WorkSpace この設定をのままにしておきたい場合は AutoStop、 AutoStop アップグレードが実行されるまでの時間を 3 時間以上に変更してください。
- インプレースアップグレードプロセスでは、Default User (`C:\Users\Default`) という名前の特別なプロファイルのコピーを作成することで、ユーザープロファイルを再作成します。このデフォルトのユーザープロファイルを使用してカスタマイズを行わないでください。代わりに、グループポリシーオブジェクト (GPO) を使用してユーザープロファイルをカスタマイズすることをお勧めします。GPO を使用して行ったカスタマイズは変更やロールバックが容易なため、エラーが発生しにくくなります。
- インプレースアップグレードプロセスでは、1 つのユーザープロファイルだけをバックアップおよび再作成できます。ドライブ D に複数のユーザープロファイルがある場合は、必要なプロファイルを除くすべてのプロファイルを削除します。

考慮事項

インプレースアップグレードプロセスでは、2 つのレジストリスクリプト (`enable-inplace-upgrade.ps1`と`update-pvdrivers.ps1`) を使用して Windows Update プロセスを実行するために必要な変更を行います。 WorkSpaces これらの変更には、ドライブ D ではなくドライブ C に (一時的な) ユーザープロファイルを作成することが含まれます。ユーザープロファイルがドライブ D にすでに存在する場合、その元のユーザープロファイルのデータはドライブ D に残ります。

デフォルトでは、 WorkSpaces にユーザープロファイルが作成されます。D:\Users\%USERNAME%enable-inplace-upgrade.ps1 スクリプトは、C:\Users\%USERNAME% に新しいユーザープロファイルを作成するように Windows を設定し、ユーザーシェルフォルダを D:\Users\%USERNAME% にリダイレクトします。この新しいユーザープロファイルは、ユーザーが初めてログオンしたときに作成されます。

インプレースアップグレード後、ユーザープロファイルをドライブ C に残して、ユーザーが今後に Windows Update プロセスを使用してマシンをアップグレードできるようにすることが可能です。ただし、ドライブ C に保存されているプロファイルでは、データを自分でバックアップおよび復元しない限り、ユーザープロファイルのデータをすべて失わずに再構築または移行できないことに注意してください。 WorkSpaces プロファイルをドライブ C に残す場合は、このトピックの後半で説明するように、UserShellFoldersRedirectionレジストリキーを使用してユーザーシェルフォルダーをドライブ D にリダイレクトできます。

WorkSpaces を再構築または移行できるようにし、ユーザーシェルのフォルダーリダイレクトに関する潜在的な問題を回避するために、インプレースアップグレード後にユーザープロファイルをドライブ D に復元することを選択することをお勧めします。そのためには、このトピックの後半で説明するように PostUpgradeRestoreProfileOnD レジストリキーを使用します。

既知の制限事項

- ユーザープロファイルの場所がドライブ D からドライブ C に変更されるのは、 WorkSpace 再構築や移行中には発生しません。Windows 10 または 11 の BYOL WorkSpace でインプレースアップグレードを実行し、それを再構築または移行すると、新しいバージョンのユーザープロファイルはドライブ D WorkSpace に保存されます。

  > **Warning**
  >
  > インプレースアップグレード後にユーザープロファイルをドライブ C に残しておくと、ドライブ C に保存されているユーザープロファイルデータは、再構築または移行前にユーザープロファイルデータを手動でバックアップし、再構築または移行後に手動で復元しない限り、再構築または移行中に失われます。

- デフォルト BYOL バンドルに Windows 10 および 11 の以前のリリースに基づくイメージが含まれている場合は、を再構築または移行した後に、インプレースアップグレードを再度実行する必要があります。 WorkSpace

レジストリキー設定の概要

インプレースアップグレードプロセスを有効にして、アップグレード後にユーザープロファイルを配置する場所を指定するには、複数のレジストリキーを設定する必要があります。

レジストリパス:HKL M:\Software\Amazon\WorkSpacesConfig\ enable-inplace-upgrade .ps1

レジストリキー	タイプ	値
[Enabled] (有効)	DWORD	0 – (デフォルト) インプレースアップグレードを無効にする 1 – インプレースアップグレードを有効にする
PostUpgradeRestoreProfileOnD	DWORD	0 – (デフォルト) インプレースアップグレード後にユーザープロファイルパスの復元を試みない 1 — インプレースアップグレード後にユーザープロファイルパス (ProfileImagePath) を復元します
UserShellFoldersRedirection	DWORD	0 – ユーザーシェルフォルダのリダイレクトを有効にしない 1 – (デフォルト) ユーザープロファイルが `D:\Users\%USERNAME%` で再生成された後、`C:\Users\%USERNAME%` へのユーザーシェルフォルダのリダイレクトを有効にする
NoReboot	DWORD	0 – (デフォルト) ユーザープロファイルのレジストリを変更した後、再起動するタイミングを制御することを許可する

レジストリキー	タイプ	値
		1 — WorkSpace ユーザープロファイルのレジストリを変更した後に、スクリプトが再起動しないようにします。

レジストリパス:HKL M:\Software\Amazon\WorkSpacesConfig\ update-pvdrivers.ps1

レジストリキー	タイプ	値
[Enabled] (有効)	DWORD	0 — (デフォルト) PV ドライバーの更新を無効にします AWS 1 — AWS PV ドライバーの更新を有効にします。

インプレースアップグレードの実行

BYOL の Windows インプレースアップグレードを有効にするには WorkSpaces、以下の手順で説明するように、特定のレジストリキーを設定する必要があります。また、特定のレジストリキーを設定して、インプレースアップグレードの完了後にユーザープロファイルを配置するドライブ (C または D) を指定する必要があります。

これらのレジストリの変更は手動で行うことができます。 WorkSpaces 更新するスクリプトが複数ある場合は、グループポリシーまたは SCCM を使用してスクリプトをプッシュできます。PowerShell PowerShellサンプルスクリプトについては、を参照してください WorkSpace スクリプトを使用してレジストリを更新してください。 PowerShell 。

Windows 10 と 11 のインプレースアップグレードを実行するには

1. 更新中の Windows 10 および 11 BYOL WorkSpaces で現在実行されている Windows のバージョンを書き留めてから、それらを再起動します。
2. 以下の Windows システムレジストリキーを更新し、[有効] の値データを 0 から 1 に変更します。これらのレジストリの変更により、のインプレースアップグレードが可能になります。WorkSpace

- HKEY_LOCAL_MACHINE\ ソフトウェア\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
- HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ update-pvdrivers.ps1 WorkSpacesConfig

> **Note**
>
> これらのキーが存在しない場合は、を再起動してください。 WorkSpaceシステムを再起動すると、キーが追加されます。

(オプション) SCCM Task Sequences などのマネージド型ワークフローを使用してアップグレードを実行する場合は、次のキー値を 1 に設定してコンピュータが再起動しないようにします。

HKEY_LOCAL_MACHINE\ ソフトウェア\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. インプレースアップグレードプロセス後にユーザープロファイルを配置するドライブを決定し (詳細については「考慮事項」を参照)、以下のようにレジストリキーを設定します。

   - アップグレード後にドライブ C にユーザープロファイルが必要な場合の設定:

     HKEY_LOCAL_MACHINE\ ソフトウェア\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     キーネームPostUpgradeRestoreProfileOn:D

     キー値: 0

     キー名:UserShellFoldersRedirection

     キー値: 1

   - アップグレード後にドライブ D にユーザープロファイルが必要な場合の設定:

     HKEY_LOCAL_MACHINE\ ソフトウェア\ Amazon\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     キーネームPostUpgradeRestoreProfileOn:D

キー値: 1

キー名:UserShellFoldersRedirection

キー値: 0

4. 変更をレジストリに保存したら、 WorkSpace 再度再起動して変更を適用します。

> **Note**
>
> - 再起動後、 WorkSpace にログインすると新しいユーザープロファイルが作成されます。[スタート] メニューにプレースホルダーアイコンが表示される場合があります。この動作は、インプレースアップグレードが完了すると自動的に解決されます。
> - WorkSpace のブロックが解除されるまで 10 分間待ってください。

(オプション) 次のキー値が 1 に設定されていることを確認します。これにより、 WorkSpace のアップデートのブロックが解除されます。

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ 削除済み WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. インプレースアップグレードを実行します。必要に応じて、SCCM、ISO、Windows Update (WU) のいずれの方法も使用できます。Windows 10 と 11 の元のバージョンと、インストールされているアプリの数によっては、この処理に 40 分から 120 分かかる場合があります。

> **Note**
>
> インプレースアップグレードプロセスには、最低 1 時間かかる可能性があります。WorkSpace インスタンスのステータスは、UNHEALTHYアップグレード中と表示される場合があります。

6. 更新プロセスが完了したら、Windows のバージョンが更新されていることを確認します。

> **Note**
>
> 一括アップグレードが失敗した場合、Windows は、アップグレードを開始する前の Windows 10 および 11 バージョンを使用するように自動的にロールバックします。トラ

ブルシューティングの詳細については、Microsoft の関連ドキュメントを参照してください。

(オプション) 更新スクリプトが正常に実行されたことを確認するには、次のキー値が 1 に設定されていることを確認します。

HKEY_LOCAL_MACHINE\ ソフトウェア\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. の実行モードをに設定したり、 AlwaysOn AutoStop インプレースアップグレードプロセスを中断せずに実行できるように期間を変更したりして実行モードを変更した場合は、実行モードを元の設定に戻してください。 WorkSpace 詳細については、「実行モードを変更する」を参照してください。

PostUpgradeRestoreProfileOnD レジストリキーを 1 に設定していない場合、ユーザープロファイルは Windows によって再生成され、C:\Users\%USERNAME%一括アップグレード後に配置されます。これにより、future の Windows 10 および 11 のインプレースアップグレードで上記の手順をやり直す必要がなくなります。デフォルトでは、enable-inplace-upgrade.ps1 スクリプトは以下のシェルフォルダをドライブ D にリダイレクトします。

- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu

- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates`

シェルフォルダを上の他の場所にリダイレクトする場合は WorkSpaces、 WorkSpaces インプレースアップグレード後に必要な操作を実行してください。

トラブルシューティング

更新中に問題が発生した場合は、以下の項目をチェックしてトラブルシューティングに役立てます。

- Windows ログ。デフォルトでは、以下の場所にあります。

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Windows イベントビューア。

  ウィンドウズログ > アプリケーション > ソース:Amazon WorkSpaces

> **Tip**
>
> 一括アップグレード処理中に、デスクトップの一部のアイコンショートカットが機能しなくなったのは、アップグレードの準備のためにドライブ D にあるユーザープロファイルがドライブ C WorkSpaces に移動されたためです。アップグレードが完了すると、ショートカットは正常に動作します。

WorkSpace スクリプトを使用してレジストリを更新してください。PowerShell

PowerShell 次のサンプルスクリプトを使用してのレジストリを更新し、インプレースアップグレードを有効にできます WorkSpaces 。に従ってください。ただしインプレースアップグレードの実行、 WorkSpaceこのスクリプトを使用してそれぞれのレジストリを更新してください。

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
```

```
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

の移行 WorkSpace

> **Note**
>
> から を通じて Microsoft Office AWS バージョンのライセンスのサブスクリプションを解除したり、アンインストールしたりする場合は WorkSpace、アプリケーション の管理 を使用することをお勧めします。

ユーザーボリューム上のデータを保持したまま、あるバンドル WorkSpace から別のバンドルに を移行できます。サンプルシナリオを以下に示します。

- Windows 7 デスクトップエクスペリエンス WorkSpaces から Windows 10 デスクトップエクスペリエンスに移行できます。
- PCoIP プロトコル WorkSpaces から WorkSpaces ストリーミングプロトコル (WSP) に移行できます。
- Windows Server 2016 搭載の 32 ビット Microsoft Office WorkSpaces バンドル WorkSpaces から、Windows Server 2019 および Windows Server 2022 搭載の 64 ビット Microsoft Office WorkSpaces に移行できます。
- あるパブリックバンドルまたはカスタムバンドル WorkSpaces から別のバンドルに移行できます。例えば、GPU 対応 (Graphics.g4dn. GraphicsProg4dn、Graphics、) GraphicsProバンドルから GPU 対応以外のバンドル、およびその逆に移行できます。
- Windows 10 BYOL WorkSpaces から Windows 11 BYOL に移行することはできますが、Windows 11 から Windows 10 への移行はサポートされていません。
- バリューバンドルは Windows 11 ではサポートされていません。Windows 7 または 10 の値バンドル WorkSpaces を Windows 11 に移行するには、まず Value を WorkSpaces より大きなバンドルサービスに切り替える必要があります。
- Windows 7 WorkSpaces から Windows 11 に移行する前に、Windows 10 に移行する必要があります。Windows 11 に移行する前に WorkSpace 、Windows 10 に少なくとも 1 回ログインします。Windows 7 から Windows 11 への WorkSpaces 直接の移行はサポートされていません。
- Microsoft Office WorkSpaces を使用する Windows AWSは、 を通じて Microsoft 365 アプリケーションを含むカスタム WorkSpaces バンドルに移行できます。移行後、 WorkSpaces は Microsoft Office からサブスクリプション解除されます。

- Microsoft Office WorkSpaces を使用する Windows AWSを、 WorkSpacesOffice 2016/2019 サブスクリプションのないバンドルに移行できます。移行後、 WorkSpaces は Microsoft Office からサブスクリプション解除されます。

Amazon WorkSpaces バンドルの詳細については、「」を参照してくださいWorkSpace バンドルとイメージ。

移行プロセス WorkSpace では、ターゲットバンドルイメージの新しいルートボリュームと、元の の最後に利用可能なスナップショットのユーザーボリュームを使用して を再作成します WorkSpace。移行中に新しいユーザープロファイルが生成され、互換性が向上します。古いユーザープロファイルの名前が変更され、古いユーザープロファイル内の特定のファイルが新しいユーザープロファイルに移動されます (移動対象の詳細については、移行中の動作 を参照してください。)

移行プロセスには、 あたり最大 1 時間かかります WorkSpace。移行プロセスを開始すると、新しい WorkSpace が作成されます。移行の成功を妨げるエラーが発生した場合、元の WorkSpace が復旧されて元の状態に戻り、新しい WorkSpace は終了します。

目次

移行の制限

- パブリックまたはカスタムの Windows 7 デスクトップエクスペリエンスバンドルに移行することはできません。また、Bring-Your-Own-License (BYOL) Windows 7 バンドルに移行することもできません。
- BYOL は、他の BYOL バンドル WorkSpaces にのみ移行できます。PCoIP WorkSpace から WSP に BYOL を移行するには、まず WSP プロトコルで BYOL バンドルを作成する必要があります。その後、PCoIP BYOL WorkSpaces をその WSP BYOL バンドルに移行できます。

- パブリックバンドルまたはカスタムバンドルから WorkSpace 作成された を BYOL バンドルに移行することはできません。
- 現時点では、Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro バンドルは PCoIP プロトコルでのみ使用できるため、Graphics.g4dn、 GraphicsPro.g4dn、Graphics、およびはまだ WSP に移行 GraphicsPro WorkSpaces できません。
- Linux の移行 WorkSpaces は現在サポートされていません。
- 複数の言語をサポートするAWSリージョンでは、言語バンドル間で移行 WorkSpacesできます。
- ソースバンドルとターゲットバンドルは異なっている必要があります (ただし、複数の言語をサポートするリージョンでは、言語が異なる限り、同じ Windows 10 バンドルに移行できます)。同じバンドル WorkSpace を使用して を更新する場合は、代わりに を再構築 WorkSpaceします。
- リージョン WorkSpaces 間で移行することはできません。
- 場合によっては、移行が正常に完了しない場合、エラーメッセージが表示されず、移行プロセスが開始されなかったように見えることがあります。 WorkSpace バンドルが移行の試行後 1 時間同じままである場合、移行は失敗します。AWS Support センターにアクセスしてサポートをお求めください。

移行シナリオ

次の表に、可能な移行シナリオを示します。

移行元 OS	移行先 OS	使用可能
パブリックまたはカスタムバンドル Windows 7	パブリックまたはカスタムバンドル Windows 10	はい
カスタムバンドル Windows 7	パブリックバンドル Windows 7	いいえ
カスタムバンドル Windows 7	カスタムバンドル Windows 7	いいえ
パブリックバンドル Windows 7	カスタムバンドル Windows 7	いいえ
パブリックまたはカスタムバンドル Windows 10	パブリックまたはカスタムバンドル Windows 7	いいえ

移行元 OS	移行先 OS	使用可能
パブリックまたはカスタムバンドル Windows 10	カスタムバンドル Windows 10	はい
Windows 7 の BYOL バンドル	Windows 7 の BYOL バンドル	いいえ
Windows 7 の BYOL バンドル	Windows 10 の BYOL バンドル	はい
Windows 10 の BYOL バンドル	Windows 7 の BYOL バンドル	いいえ
Windows 10 の BYOL バンドル	Windows 10 の BYOL バンドル	はい
Windows Server 2016 搭載のパブリック Windows 10 バンドル	Windows Server 2019 搭載のパブリック Windows 10 バンドル 	はい
Windows Server 2019 搭載のパブリック Windows 10 バンドル 	Windows Server 2016 搭載のパブリック Windows 10 バンドル	はい
Windows 10 の BYOL バンドル	Windows 11 の BYOL バンドル	はい
Windows 11 の BYOL バンドル	Windows 10 の BYOL バンドル	いいえ

移行元 OS	移行先 OS	使用可能
Windows Server 2016 搭載のカスタム Windows 10 バンドル	Windows Server 2019 搭載のパブリック Windows 10 バンドル	はい
Windows Server 2016 搭載のカスタム Windows 10 バンドル	Windows Server 2022 搭載のパブリック Windows 10 バンドル	はい
Windows Server 2019 搭載のカスタム Windows 10 バンドル	Windows Server 2022 搭載のパブリック Windows 10 バンドル	はい

Note

Windows Server 2019 搭載のパブリック Windows 10 バンドル PCoIP ブランチでは、Web Access は使用できません。

Important

Windows Server 2016 搭載のパブリック Windows 10 プラスバンドルには、Microsoft Office 2016 と Trend Micro Worry-Free Business Security Services が含まれています。Windows Server 2019 搭載のパブリック Windows 10 プラスバンドルには、Microsoft Office 2019 のみが含まれ、Trend Micro Services は含まれません。

移行中の動作

移行中は、ユーザーボリューム (ドライブ D) 上のデータは保持されますが、ルートボリューム (ドライブ C) 上のすべてのデータは失われます。つまり、インストールされているアプリケーション、設定、およびレジストリの変更は、いずれも保持されません。古いユーザープロファイルフォルダの名前が `.NotMigrated` サフィックスで変更され、新しいユーザープロファイルが作成されます。

移行プロセスでは、元のユーザーボリュームの最後のスナップショットに基づいてドライブ D が再作成されます。新しい の最初の起動時に WorkSpace、移行プロセスによって元の`D:`

\Users\%USERNAME%フォルダが という名前のフォルダに移動されますD:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated。新しい OS によって新しい D:\Users\%USERNAME%\ フォルダが生成されます。

新しいユーザープロファイルが作成されると、次のユーザーシェルフォルダ内のファイルが古い .NotMigrated プロファイルから新しいプロファイルに移動します。

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

> **Important**
>
> 移行プロセスでは、古いユーザープロファイルから新しいプロファイルへのファイルの移動が試みられます。移行中に移動されなかったファイルは、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダ内に残ります。移行が成功すると、どのファイルが移動されたかを C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs で確認できます。自動的に移動されなかったファイルは、手動で移動できます。
>
> デフォルトでは、パブリックバンドルではローカル検索インデックス作成が無効になっています。有効にすると、デフォルトでは C:\Users ではなく D:\Users を検索する設定となるため、それも調整する必要があります。ローカル検索インデックス作成を D:\Users*username* に設定し、D:\Users に設定していない場合、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダ内のユーザーファイルの移行後にローカル検索インデックス作成が機能しないことがあります。

元の に割り当てられたタグ WorkSpace は移行中に引き継がれ、 の実行モード WorkSpace は保持されます。ただし、新しい は新しい WorkSpace ID、コンピュータ名、および IP アドレス WorkSpace を取得します。

ベストプラクティス

を移行する前に WorkSpace、次の操作を行います。

- ドライブ C の重要なデータを別の場所にバックアップします。ドライブ C 上のすべてのデータは、移行中に消去されます。
- ユーザーボリュームのスナップショットが作成されていることを確認するには、移行 WorkSpace する が 12 時間以上経過していることを確認します。Amazon WorkSpaces コンソールの移行 WorkSpacesページで、最後のスナップショットの時刻を確認できます。最後のスナップショット以降に作成されたデータは、移行中に失われます。
- データの損失を避けるため、ユーザーが WorkSpacesからログアウトし、移行プロセスが完了するまでログインし直さないようにしてください。モードの場合、 は移行 WorkSpaces できないことに注意してくださいADMIN_MAINTENANCE。
- 移行 WorkSpaces する のステータスが AVAILABLE、STOPPED、または であることを確認しますERROR。
- 移行 WorkSpaces する に十分な IP アドレスがあることを確認します。移行中、 に新しい IP アドレスが割り当てられます WorkSpaces。
- スクリプトを使用して を移行する場合は WorkSpaces、 WorkSpaces 一度に 25 以下のバッチで移行します。

トラブルシューティング

- 移行後にファイルが見つからないことについてユーザーから報告があった場合は、移行プロセス中にユーザープロファイルファイルが移動されなかったかどうかを確認します。どのファイルが移動されたかは、C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs で確認できます。移動されなかったファイルは、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダに配置されます。自動的に移動されなかったファイルは、手動で移動できます。
- API を使用して移行 WorkSpaces しても移行が成功しない場合、API から返されたターゲット WorkSpace ID は使用されず、 WorkSpaceには元の WorkSpace ID が残ります。
- 移行が正常に完了しない場合は、Active Directory で、適切にクリーンアップされたかどうかを確認します。 WorkSpaces 不要になった を手動で削除する必要がある場合があります。

請求への影響

移行が発生する月には、新しい と元の の両方に対して按分計算された金額が課金されます WorkSpaces。例えば、5 月 10 日に WorkSpace A を WorkSpace B に移行した場合、5 月 1 日から 5 月 10 日までは WorkSpace A に対して課金され、5 月 11 日から 5 月 30 日までは WorkSpace B に対して課金されます。

> **Note**
>
> WorkSpace を別のバンドルタイプに移行する場合 (パフォーマンスからパワー、値からスタンダードなど) 、移行プロセス中にルートボリューム (ドライブ C) とユーザーボリューム (ドライブ D) のサイズが増加する可能性があります。必要に応じて、ルートボリュームは、新しいバンドルのデフォルトのルートボリュームサイズに合わせて増加します。ただし、ユーザーボリュームに対して、元のバンドルのデフォルトとは異なるサイズ (高いサイズまたは低いサイズ) をすでに指定していた場合、移行プロセス中も同じユーザーボリュームサイズが保持されます。それ以外の場合、移行プロセスでは、新しいバンドルのソース WorkSpace ユーザーボリュームサイズとデフォルトのユーザーボリュームサイズのうち大きい方が使用されます。

の移行 WorkSpace

Amazon WorkSpaces コンソール、、AWS CLIまたは Amazon WorkSpaces API WorkSpaces を使用して移行できます。

を移行するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. を選択し WorkSpace 、アクション 、移行 WorkSpacesを選択します。
4. バンドル で、 を移行するバンドルを選択します WorkSpace 。

> **Note**
>
> PCoIP WorkSpace から WSP に BYOL を移行するには、まず WSP プロトコルで BYOL バンドルを作成する必要があります。その後、PCoIP BYOL WorkSpaces をその WSP BYOL バンドルに移行できます。

5. 移行を選択します WorkSpaces。

   ステータス WorkSpace が の新しい が Amazon WorkSpaces コンソールPENDINGに表示されます。移行が完了すると、元の WorkSpace が終了し、新しい のステータス WorkSpace が に設定されますAVAILABLE。

6. (オプション) 不要になったカスタムバンドルとイメージを削除する方法については、WorkSpaces カスタムバンドルまたはイメージを削除する を参照してください。

WorkSpaces を介して移行するにはAWS CLI、migrate-workspace コマンドを使用します。Amazon WorkSpaces API WorkSpaces を介して移行するには、「Amazon API リファレンス」のMigrateWorkSpace「」を参照してください。 WorkSpaces

WorkSpace の削除

不要になった WorkSpace は、削除することができます。関連リソースも削除できます。

> **Warning**
>
> WorkSpace の削除は永続的なアクションであり、元に戻すことはできません。WorkSpace ユーザーのデータは保持されず、破棄されます。ユーザーデータのバックアップに関するヘルプについては、AWS Support にお問い合わせください。

> **Note**
>
> Simple AD および AD Connector は、WorkSpaces で無料で利用できます。Simple AD または AD Connector ディレクトリで 30 日間連続使用されている WorkSpaces がない場合、そのディレクトリは Amazon WorkSpaces での使用から自動的に登録解除され、AWS Directory Service 料金の条件に従って課金されるようになります。
> 空のディレクトリを削除するには、WorkSpaces のディレクトリの削除 を参照してください。Simple AD または AD Connector ディレクトリを削除した場合、WorkSpaces を再度ご使用になる際は、いつでも Simple AD または AD Connector を新たに作成できます。

WorkSpace を削除するには

状態が [Suspended] (一時停止) 以外の WorkSpace は削除できます。

1. https://console.aws.amazon.com/workspaces/ 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] を選択します。
3. WorkSpace を選択し、[Delete] (削除) を選択します。
4. 確認を求めるメッセージが表示されたら、[Delete WorkSpace] (WorkSpace の削除) を選択します。WorkSpace が削除されるまで約 5 分かかります。削除中、WorkSpace の状態は [Terminating] (終了中) に設定されます。削除が完了すると、コンソールから WorkSpace が消えます。
5. （オプション）不要になったカスタムバンドルとイメージを削除するには、「WorkSpaces カスタムバンドルまたはイメージを削除する」を参照してください。
6. （オプション）ディレクトリのすべての WorkSpaces を削除した後で、ディレクトリを削除することができます。詳細については、「WorkSpaces のディレクトリの削除」を参照してください。
7. (オプション) ディレクトリの Virtual Private Cloud (VPC) のすべてのリソースを削除した後で、VPC を削除し、NAT ゲートウェイで使用されている Elastic IP アドレスを解放できます。詳細については、Amazon VPC ユーザーガイドの VPC の削除および Elastic IP アドレスの使用を参照してください。

を使用して WorkSpace を削除するにはAWS CLI

terminate-workspaces コマンドを使用します。

WorkSpace バンドルとイメージ

WorkSpace バンドルは、オペレーティングシステム、ストレージ、コンピューティング、ソフトウェアリソースの組み合わせです。を起動するときは WorkSpace、ニーズに合ったバンドルを選択します。で使用できるデフォルトのバンドル WorkSpaces は、パブリックバンドル と呼ばれます。で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。

Windows または Linux を起動 WorkSpace してカスタマイズした場合は、その からカスタムイメージを作成できます WorkSpace。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

カスタムイメージを作成したら、カスタム WorkSpace イメージと、選択した基盤となるコンピューティングおよびストレージ設定を組み合わせたカスタムバンドルを構築できます。その後、新しいを起動するときにこのカスタムバンドルを指定 WorkSpaces して、新しい の設定 (ハードウェアとソフトウェア) WorkSpaces の一貫性を保てるようにできます。

ソフトウェアの更新を実行したり、 に追加のソフトウェアをインストールしたりする必要がある場合は WorkSpaces、カスタムバンドルを更新して を再構築できます WorkSpaces。

WorkSpaces は、複数の異なるオペレーティングシステム (OS)、ストリーミングプロトコル、バンドルをサポートしています。次の表に、各 OS でサポートされているライセンス、ストリーミングプロトコル、バンドルに関する情報を示します。

オペレーティングシステム	ライセンス	ストリーミングプロトコル	サポート対象バンドル	ライフサイクルポリシー/廃止日
Windows Server 2016	含まれる	WSP、PCc	Value、Standard、Performance、Power PowerPro、Graphics (廃止) GraphicsPro、Graphics.g4dn、 GraphicsPro.g4dn	2027 年 1 月 12 日
[Windows Server 2019]	含まれる	WSP、PCc	Value、Standard、Performance、Power PowerPro、Graphics	2029 年 1 月 9 日

オペレーティングシステム	ライセンス	ストリーミングプロトコル	サポート対象バンドル	ライフサイクルポリシー/廃止日
			(廃止) GraphicsPro、Graphics.g4dn、 GraphicsPro.g4dn	
Windows Server 2022	含まれる	WSP、PCo	Standard、Performance、PowerPro、Graphics (非推奨) GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn	2031 年 10 月 14 日
Windows 10	Bring-Your-Own-License (BYOL)	WSP、PCo	Value、Standard、Performance、Power PowerPro、Graphics (廃止) GraphicsPro、Graphics.g4dn、 GraphicsPro.g4dn	サポート中
Windows 11	Bring-Your-Own-License (BYOL)	WSP	Standard、Performance、Power、 PowerPro	サポート中
Amazon Linux 2	含まれる	WSP、PCo	Value、Standard、Performance、Power、 PowerPro	2025 年 6 月 30 日
Ubuntu 22.04 LTS	含まれる	WSP	Value、Standard、Performance、Power PowerPro、Graphics.g4dn、 GraphicsPro.g4dn	2032 年 6 月

Note

- ベンダーがサポートしなくなったオペレーティングシステムのバージョンは動作する保証はなく、 AWS サポートによってもサポートされません。

- Windows オペレーティングシステムで WorkSpaces 実行されている場合、グラフィックスバンドルは PCoIP ストリーミングプロトコルのみをサポートします。

内容

バンドルオプション

バンドルを選択する前に、選択するバンドルが WorkSpaces のプロトコル、オペレーティングシステム、ネットワーク、およびコンピューティングタイプと互換性があることを確認します。プロトコルの詳細については、「Amazon WorkSpaces のプロトコル」を参照してください。ネットワークの詳細については、「Amazon WorkSpaces クライアントネットワーク要件」を参照してください。

Note

- PCoIP WorkSpaces の最大ネットワークレイテンシーが 250 ミリ秒を超えないようにすることをお勧めします。PCoIP WorkSpaces のユーザーエクスペリエンスを最大限に高めるには、ネットワークレイテンシーを 100 ミリ秒未満に抑えることをお勧めします。ラウンドトリップ時間 (RTT) が 375 ミリ秒を超えると、WorkSpaces クライアント接続はシャットダウンします。WorkSpaces Streaming Protocol (WSP) の最適なユーザーエクスペリエンスを実現するには、RTT を 250 ミリ秒未満に抑えることをお勧めします。RTT が 250 ms と 400 ms の間にある場合、ユーザーは WorkSpace にアクセスできますが、パフォーマンスは大きく低下します。
- テスト環境で選択するバンドルのパフォーマンスのテストでは、ユーザーの日常タスクをレプリケートするアプリケーションを実行して使用することをお勧めします。

> **Important**
>
> - 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。Graphics バンドルを使用して WorkSpaces 用の Graphics.g4dn バンドルに切り替えることをお勧めします。
> - グラフィックスおよび GraphicsPro バンドルは、現在アジアパシフィック (ムンバイ) リージョンでは利用できません。

WorkSpaces が提供するバンドルは次のとおりです。WorkSpaces でのバンドルの詳細については、「Amazon WorkSpaces バンドル」を参照してください。

Value バンドル

このバンドルは、以下に最適です。

- 基本的なテキスト編集とデータ入力
- 使用量の少ないウェブブラウジング
- インスタントメッセージング

このバンドルは、言語処理、音声およびビデオ会議、画面共有、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

Standard バンドル

このバンドルは、以下に最適です。

- 基本的なテキスト編集とデータ入力
- ウェブブラウジング
- インスタントメッセージング
- Email(メール)

このバンドルは、音声およびビデオ会議、画面共有、言語処理、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

Performance バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- インスタントメッセージング
- Email(メール)
- スプレッドシート
- オーディオ処理
- コースウェア

このバンドルは、ビデオ会議、画面共有、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

Power バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- インスタントメッセージング
- スプレッドシート
- オーディオ処理
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入
- 音声会議とビデオ会議

このバンドルは、画面共有、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

PowerPro バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- インスタントメッセージング
- スプレッドシート
- オーディオ処理
- ソフトウェア開発 (統合開発環境 (IDE))
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- 音声会議とビデオ会議

このバンドルは、機械学習モデルのトレーニング、およびグラフィックアプリケーションにはお勧めしません。

GraphicsPro バンドル

このバンドルは、WorkSpaces の基本レベルのグラフィックパフォーマンスと、高レベルの CPU パフォーマンスおよびメモリを提供します。これは、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- インスタントメッセージング
- スプレッドシート
- オーディオ会議
- ソフトウェア開発 (統合開発環境 (IDE))
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- グラフィックスデザイン
- 画像処理

このバンドルは、音声会議やビデオ会議、3D レンダリング、実写のようなリアルなデザインにはお勧めしません。

Graphics.g4dn バンドル

このバンドルは、WorkSpaces の高いレベルのグラフィックパフォーマンスと、中程度のレベルの CPU パフォーマンスおよびメモリを提供し、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- スプレッドシート
- インスタントメッセージング
- オーディオ会議
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- グラフィックスデザイン
- CAD/CAM (コンピューター支援設計/コンピューター支援製造)

このバンドルは、音声会議やビデオ会議、3D レンダリング、実写のようなリアルなデザイン、および機械学習モデルのトレーニングにはお勧めしません。

GraphicsPro.g4dn

GraphicsPro.g4dn バンドル

このバンドルは、WorkSpaces の高いレベルのグラフィックパフォーマンス、CPU パフォーマンス、およびメモリを提供し、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- スプレッドシート
- インスタントメッセージング

- オーディオ会議
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- グラフィックスデザイン
- CAD/CAM (コンピューター支援設計/コンピューター支援製造)
- 動画トランスコーディング
- 3D レンダリング
- 実写のようなリアルなデザイン
- ゲームストリーミング
- 機械学習 (ML) モデルのトレーニングと ML 推論

このバンドルは、音声会議やビデオ会議にはお勧めしません。

カスタム WorkSpaces イメージとバンドルを作成する

Windows または Linux を起動 WorkSpace し、カスタマイズした場合は、その からカスタムイメージとカスタムバンドルを作成できます WorkSpace。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

> **Note**
>
> バンドルを削除してから 2 時間以上待ってから、同じ名前の新しいバンドルを作成してください。

カスタムイメージを作成したら、カスタムイメージと、選択した基盤となるコンピューティングおよびストレージ設定を組み合わせたカスタムバンドルを構築できます。その後、新しい を起動するときにこのカスタムバンドルを指定 WorkSpaces して、新しい の設定 (ハードウェアとソフトウェア) WorkSpaces の一貫性を保てるようにできます。

バンドルごとに異なるコンピューティングオプションとストレージオプションを選択することで、同じカスタムイメージを使用してさまざまなカスタムバンドルを作成できます。

> **Important**
>
> - Windows 10 からイメージを作成する場合は WorkSpace、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows 10 システム (Windows の機能/バージョンアップグレード) では、イメージの作成はサポートされていないことに注意してください。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、 WorkSpaces イメージ作成プロセスでサポートされています。
> - 2020 年 1 月 14 日以降、パブリック Windows 7 バンドルからイメージを作成することはできません。Windows 7 から Windows 10 WorkSpaces への移行を検討してください。詳細については、「の移行 WorkSpace」を参照してください。
> - 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。 WorkSpaces を Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「の移行 WorkSpace」を参照してください。
> - 現在、アジアパシフィック (ムンバイ) リージョンではグラフィックと GraphicsPro バンドルは利用できません。
> - カスタムバンドルストレージボリュームは、イメージストレージボリュームよりも小さくすることはできません。

カスタムバンドルのコストは、作成元であるパブリックバンドルと同じです。料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

内容

Windows カスタムイメージを作成するための要件

> **Note**
>
> 現在、Windows では 1 GB を 1,073,741,824 バイトと定義しています。のイメージを作成するには、C ドライブで 12,884,901,888 バイト (または 12 GiB) を超える空きがあり、ユーザープロファイルが 10,737,418,240 バイト (または 10 GiB) 未満であることを確認する必要があります WorkSpace。

- のステータスは WorkSpace Available で、変更ステータスは None である必要があります。
- WorkSpaces イメージ上のすべてのアプリケーションとユーザープロファイルは、Microsoft Sysprep と互換性がある必要があります。
- イメージに含めるすべてのアプリケーションは、C ドライブにインストールする必要があります。
- Windows 7 の場合 WorkSpaces、およびその合計サイズ (ファイルとデータ) は 10 GB 未満である必要があります。
- Windows 7 の場合 WorkSpaces、Cドライブには少なくとも 12 GB の空き容量が必要です。
- で実行されているすべてのアプリケーションサービスは、ドメインユーザーの認証情報の代わりにローカルシステムアカウント WorkSpace を使用する必要があります。たとえば、ドメインユーザーの認証情報を使用して、インストール済みの Microsoft SQL Server Express を実行することはできません。
- は暗号化 WorkSpace しないでください。暗号化された からのイメージ作成 WorkSpace は現在サポートされていません。
- 以下のコンポーネントがイメージに必要です。これらのコンポーネントがないと、イメージから起動 WorkSpaces する が正しく機能しません。詳細については、「the section called “必要な設定”」を参照してください。
  - Windows PowerShell バージョン 3.0 以降
  - リモートデスクトップサービス
  - AWS PV ドライバー
  - Windows Remote Management (WinRM)
  - Teradici PCoIP エージェントおよびドライバー
  - STXHD エージェントおよびドライバー
  - AWS および WorkSpaces 証明書

- Skylight エージェント

Linux カスタムイメージを作成するための要件

- のステータスは WorkSpace Available で、変更ステータスは None である必要があります。
- イメージに含めるすべてのアプリケーションは、ユーザーボリューム (/home ディレクトリ) の外にインストールする必要があります。
- ルートボリューム (/) の使用率は 97% 未満である必要があります。
- は暗号化 WorkSpace しないでください。暗号化された からのイメージ作成 WorkSpace は現在サポートされていません。
- 以下のコンポーネントがイメージに必要です。これらのコンポーネントがないと、イメージから起動 WorkSpaces する が正しく機能しません。
  - Cloud-init
  - Teradici PCoIP または WSP エージェントおよびドライバー
  - Skylight エージェント

ベストプラクティス

からイメージを作成する前に WorkSpace、次の操作を行います。

- 本番稼働用環境に接続されていない別の VPC を使用します。
- プライベートサブネット WorkSpace に をデプロイし、アウトバウンドトラフィックに NAT インスタンスを使用します。
- 小さい Simple AD ディレクトリを使用します。
- ソース の最小ボリュームサイズを使用し WorkSpace、カスタムバンドルを作成するときに必要に応じてボリュームサイズを調整します。
- すべてのオペレーティングシステムの更新 (Windows の機能/バージョンの更新を除く) とすべてのアプリケーションの更新を にインストールします WorkSpace。詳細については、このトピックの冒頭にある「重要な注意点」を参照してください。
- バンドルに含めるべきではないキャッシュされたデータ (ブラウザ履歴、キャッシュされたファイル、ブラウザ WorkSpace Cookie など) を から削除します。
- バンドルに含める WorkSpace べきではない から設定を削除します (E メールプロファイルなど)。

- DHCP を使用して、動的 IP アドレス設定に切り替えます。
- リージョンで許可されている WorkSpace イメージのクォータを超えていないことを確認してください。デフォルトでは、リージョンごとに 40 個の WorkSpace イメージが許可されます。このクォータに達した場合、新しいイメージを作成しようとすると失敗します。クォータの引き上げをリクエストするには、WorkSpaces 制限フォーム を使用します。
- 暗号化された からイメージを作成しようとしていないことを確認します WorkSpace。暗号化された からのイメージ作成 WorkSpace は現在サポートされていません。
- でウイルス対策ソフトウェアを実行している場合は WorkSpace、イメージの作成中に無効にします。
- でファイアウォールが有効になっている場合は WorkSpace、必要なポートがブロックされていないことを確認してください。詳細については、「の IP アドレスとポートの要件 WorkSpaces」を参照してください。
- Windows の場合 WorkSpaces、イメージの作成前にグループポリシーオブジェクト (GPOsを設定しないでください。
- Windows の場合 WorkSpaces、イメージを作成する前にデフォルトのユーザープロファイル (`C:\Users\Default`) をカスタマイズしないでください。GPO を使用してユーザープロファイルをカスタマイズし、イメージの作成後に適用することをお勧めします。GPO を使用して行ったカスタマイズは変更やロールバックが容易なため、デフォルトのユーザープロファイルに対して行ったカスタマイズよりもエラーが発生しにくくなります。
- Linux については WorkSpaces、ホワイトペーパー「Amazon for Linux イメージを準備するためのベストプラクティス WorkSpaces 」も参照してください。
- WorkSpaces ストリーミングプロトコル (WSP) が有効になってい WorkSpaces る Linux でスマートカードを使用する場合は、イメージを作成する WorkSpace 前に Linux に対して行う必要があるカスタマイズ認証にスマートカードを使用するについて、「」を参照してください。
- ENA、NVMe、PV ドライバーなどのネットワーク依存関係ドライバーを で更新してください WorkSpaces。これは少なくとも 6 か月に 1 回行う必要があります。詳細については、「Elastic Network Adapter (ENA) ドライバー のインストールまたはアップグレードAWS NVMe ドライバー 」、「Windows インスタンス 用」、および「Windows インスタンス で PV ドライバーをアップグレードする」を参照してください。
- EC2Config, EC2Launch、および EC2Launch V2 エージェントを定期的に最新バージョンに更新してください。これは少なくとも 6 か月に 1 回行う必要があります。詳細については、EC2Config と EC2Launch の更新」を参照してください。

(オプション) ステップ 1: イメージのカスタムコンピュータ名の形式を指定する

カスタムイメージまたは Bring Your Own License (BYOL) イメージから WorkSpaces 起動した では、デフォルトのコンピュータ名形式 を使用する代わりに、コンピュータ名形式にカスタムプレフィックスを指定できます。カスタムプレフィックスを指定するには、イメージタイプに応じた適切な手順に従います。

カスタムイメージのカスタムコンピュータ名の形式を指定するには

> **Note**
>
> デフォルトでは、Windows 10 の場合はコンピュータ名の形式 WorkSpaces 、Windows 11 DESKTOP-XXXXXの場合はコンピュータ名の形式 WorkSpacesですWORKSPA-XXXXX。

1. カスタムイメージの作成に使用している WorkSpace で、メモ帳または別のテキストエディタC:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xmlで を開きます。Unattend.xml ファイルの操作の詳細については、Microsoft のドキュメントの「応答ファイル (unattend.xml)」をご参照ください。

   > **Note**
   >
   > の Windows File Explorer から C: ドライブにアクセスするには WorkSpace、アドレスバー**C:**に と入力します。

2. <settings pass="specialize"> セクションで、<ComputerName> がアスタリスク (*) に設定されていることを確認します。<ComputerName> が他の値に設定されている場合、カスタムコンピュータ名の設定は無視されます。<ComputerName> 設定の詳細については、Microsoft ドキュメントの ComputerName「」を参照してください。
3. <settings pass="specialize"> セクションで、<RegisteredOrganization> および <RegisteredOwner> を任意の値に設定します。

   Sysprep では、<RegisteredOwner> および <RegisteredOrganization> に指定した値が連結され、結合された文字列の最初の 7 文字を使用してコンピュータ名が作成されます。例えば、 **Amazon.com**に <RegisteredOrganization>を指定し、 **EC2**に を指定した場合<RegisteredOwner>、カスタムバンドルから WorkSpaces 作成された のコンピュータ名は EC2AMAZ -*xxxxxxx* で始まります。

> **Note**
>
> <RegisteredOrganization> セクション内の <RegisteredOwner> および <settings pass="oobeSystem"> の値は、Sysprep では無視されます。

4. 変更を Unattend.xml ファイルに保存します。

BYOL イメージのカスタムコンピュータ名の形式を指定するには

1. Windows 10 を使用している場合は、メモ帳または別のテキストエディタで C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml を開きます。Windows 11 を使用している場合は、C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml を開きます。
2. <settings pass="specialize"> セクションで、<ComputerName>*</ComputerName> のコメントを解除し、<ComputerName> がアスタリスク (*) に設定されていることを確認します。<ComputerName> が他の値に設定されている場合、カスタムコンピュータ名の設定は無視されます。<ComputerName> 設定の詳細については、Microsoft ドキュメントの ComputerName「」を参照してください。
3. <settings pass="specialize"> セクションで、<RegisteredOrganization> および <RegisteredOwner> を任意の値に設定します。

   Sysprep では、<RegisteredOwner> および <RegisteredOrganization> に指定した値が連結され、結合された文字列の最初の 7 文字を使用してコンピュータ名が作成されます。例えば、 **Amazon.com**に <RegisteredOrganization>を指定し、 **EC2**に を指定した場合<RegisteredOwner>、カスタムバンドルから WorkSpaces 作成された のコンピュータ名は EC2AMAZ -*xxxxxxx* で始まります。

   > **Note**
   >
   > <RegisteredOrganization> セクション内の <RegisteredOwner> および <settings pass="oobeSystem"> の値は、Sysprep では無視されます。

4. Windows 10 を使用している場合は、変更内容を Sysprep2008.xml ファイルに保存します。Windows 11 を使用している場合は、変更内容を OOBE_unattend.xml に保存します。

ステップ 2: Image Checker を実行する

> **Note**
>
> Image Checker は Windows でのみ使用できます WorkSpaces。Linux からイメージを作成する場合は WorkSpace、「」に進みますステップ 3: カスタムイメージとカスタムバンドルを作成する。

Windows がイメージ作成の WorkSpace 要件を満たしていることを確認するには、Image Checker を実行することをお勧めします。Image Checker は、イメージの作成 WorkSpace に使用する で一連のテストを実行し、検出された問題を解決する方法に関するガイダンスを提供します。

> **Important**
>
> - イメージの作成に使用する前に、 は Image Checker によって実行されるすべてのテストに合格 WorkSpace する必要があります。
> - Image Checker を実行する前に、最新の Windows セキュリティ更新プログラムと累積更新プログラムが にインストールされていることを確認します WorkSpace。

Image Checker を入手するには、以下のいずれかを実行します。

- を再起動します WorkSpace。Image Checker は再起動時に自動的にダウンロードされ、`C:\Program Files\Amazon\ImageChecker.exe` にインストールされます。
- https://tools.amazonworkspaces.com/ImageChecker.zip .zip から Amazon WorkSpaces Image Checker し、`ImageChecker.exe`ファイルを抽出します。このファイルを `C:\Program Files\Amazon\` にコピーします。

Image Checker を実行するには

1. `C:\Program Files\Amazon\ImageChecker.exe` ファイルを開きます。
2. Amazon WorkSpaces Image Checker ダイアログボックスで、「 を実行」を選択します。
3. 各テストが完了したら、テストのステータスを表示できます。

   いずれかのテストで [Failed (失敗)] ステータスが表示された場合は、[Info (情報)] を選択して、失敗の原因となった問題の解決方法に関する情報を表示します。これらの問題を解決する方法の

詳細については、Image Checker によって検出された問題を解決するためのヒント を参照してください。

いずれかのテストで [WARNING (警告)] ステータスが表示された場合は、[Fix All Warnings (すべての警告の修正)] ボタンを選択します。

このツールは、Image Checker が配置されているのと同じディレクトリに出力ログファイルを生成します。デフォルトでは、このファイルは `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` にあります。

> **Tip**
>
> このログファイルは削除しないでください。問題が発生した場合、このログファイルはトラブルシューティングに役立つことがあります。

4. 該当する場合は、テストの失敗や警告の原因となる問題を解決し、 がすべてのテストに合格するまで WorkSpace Image Checker を実行するプロセスを繰り返します。イメージを作成する前に、すべての失敗と警告が解決されている必要があります。
5. がすべてのテストに WorkSpace 合格すると、検証成功メッセージが表示されます。これで、カスタムバンドルを作成する準備ができました。

Image Checker によって検出された問題を解決するためのヒント

Image Checker によって検出された問題を解決するための以下のヒントを参照するほか、`C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` で Image Checker のログファイルも確認してください。

PowerShell バージョン 3.0 以降がインストールされている必要があります

Microsoft Windows PowerShellの最新バージョンをインストールします。

> **Important**
>
> PowerShell の実行ポリシーは、RemoteSignedスクリプトを許可するように設定 WorkSpace する必要があります。実行ポリシーを確認するには、Get-command ExecutionPolicy PowerShell を実行します。実行ポリシーが無制限または に設定されていない場合 はRemoteSigned、Set-ExecutionPolicy –ExecutionPolicy RemoteSigned コマンドを実行して

実行ポリシーの値を変更します。RemoteSigned この設定では WorkSpaces、イメージの作成に必要な Amazon でのスクリプトの実行を許可します。

C および D ドライブのみが存在できる

イメージングに使用される には WorkSpace 、 Cおよび Dドライブのみ存在できます。仮想ドライブを含め他のすべてのドライブを削除します。

Windows Update による保留中の再起動は検出できない

- Windows を再起動してセキュリティまたは累積更新プログラムのインストールが完了するまで、イメージ作成プロセスは実行できません。Windows を再起動してこれらの更新を適用し、保留中の他の Windows セキュリティまたは累積更新プログラムをインストールする必要がないことを確認します。
- イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows 10 システム (Windows の機能/バージョンのアップグレード) ではサポートされません。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、WorkSpaces イメージ作成プロセスでサポートされています。

Sysprep ファイルは存在する必要があり、空白にすることはできない

Sysprep ファイルに問題がある場合は、AWS Support センターに連絡して EC2Config または EC2Launch の修復を依頼します。

ユーザープロファイルのサイズは 10 GB 未満であることが必要

Windows 7 の場合 WorkSpaces、ユーザープロファイル (`D:\Users\username`) の合計は 10 GB 未満である必要があります。必要に応じてファイルを削除して、ユーザープロファイルのサイズを小さくします。

ドライブ C には十分な空き容量が必要

Windows 7 では WorkSpaces、ドライブ に 12 GB 以上の空き容量が必要ですC。必要に応じてファイルを削除し、ドライブ C の空き容量を増やします。Windows 10 では WorkSpaces、FAILEDメッセージを受信し、ディスク容量が 2GB を超える場合は無視します。

ドメインアカウントで実行できるサービスがない

イメージの作成プロセスを実行するには、ドメインアカウントで 上のサービス WorkSpace を実行できません。すべてのサービスがローカルアカウントで実行されている必要があります。

ローカルアカウントでサービスを実行するには

1. `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` を開き、ドメインアカウントで実行されているサービスのリストを見つけます。
2. Windows の検索ボックスに「**`services.msc`**」と入力して、Windows サービスマネージャーを開きます。
3. [ログオン方法] で、ドメインアカウントで実行されているサービスを探します。([ローカルシステム]、[ローカルサービス]、または [ネットワークサービス] として実行されているサービスは、イメージの作成を妨げません)
4. ドメインアカウントで実行されているサービスを選択し、[操作]、[プロパティ] の順に選択します。
5. [ログオン] タブを開きます。[ログオン方法] で、[ローカルシステムアカウント] を選択します。
6. [OK] をクリックします。

DHCP を使用するように を設定 WorkSpace する必要があります

静的 IP アドレスの代わりに DHCP を使用する WorkSpace ように、 上のすべてのネットワークアダプタを設定する必要があります。

DHCP を使用するようにすべてのネットワークアダプターを設定するには

1. Windows の検索ボックスに「**`control panel`**」と入力して、コントロールパネルを開きます。
2. [ネットワークとインターネット] を選択します。
3. [ネットワークと共有センター] を選択します。
4. [アダプター設定の変更] を選択し、アダプターを選択します。
5. [この接続の設定を変更する] を選択します。
6. [ネットワーク] タブで、[インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択し、[プロパティ] を選択します。
7. [インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティ] ダイアログボックスで、[IP アドレスを自動的に取得する] を選択します。
8. [OK] をクリックします。
9. 上のすべてのネットワークアダプタに対してこのプロセスを繰り返します WorkSpace。

リモートデスクトップサービスを有効にすることが必要

イメージ作成プロセスでは、リモートデスクトップサービスを有効にする必要があります。

リモートデスクトップサービスを有効にするには

1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[リモートデスクトップサービス] を見つけます。
3. [リモートデスクトップサービス] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] をクリックします。

ユーザープロファイルが存在することが必要

イメージの作成 WorkSpace に使用する には、ユーザープロファイル () が必要ですD:\Users*username*。このテストに失敗した場合は、AWS Support センターにお問い合わせください。

環境変数のパスを適切に設定することが必要

ローカルマシンの環境変数パスに、System32 および Windows の エントリがありません PowerShell。これらのエントリは、[イメージの作成] を実行するために必要です。

環境変数のパスを設定するには

1. Windows の検索ボックスに「**environment variables**」と入力し、[システム環境変数の編集] を選択します。
2. [システムのプロパティ] ダイアログボックスで、[詳細設定] タブを開き、[環境変数] を選択します。
3. [環境変数] ダイアログボックスの [システム変数] で、[パス] エントリを選択し、[編集] を選択します。
4. [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32
   ```
5. もう一度 [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```

6. [OK] をクリックします。
7. を再起動します WorkSpace。

> **Tip**
>
> 環境変数のパスに項目が表示される順序が重要です。正しい順序を決定するには、 の環境変数パス WorkSpace を、新しく作成された Windows インスタンス WorkSpace または新しい Windows インスタンスの環境変数パスと比較します。

Windows モジュールインストーラーを有効にすることが必要

イメージ作成プロセスでは、Windows モジュールインストーラーサービスを有効にする必要があります。

Windows モジュールインストーラーサービスを有効にするには

1. Windows の検索ボックスに「**`services.msc`**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[Windows モジュールインストーラー] を見つけます。
3. [Windows モジュールインストーラー] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] をクリックします。

Amazon SSM Agent を無効にすることが必要

イメージの作成プロセスでは、Amazon SSM Agent サービスを無効にする必要があります。

Amazon SSM Agent サービスを無効にするには

1. Windows の検索ボックスに「**`services.msc`**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[Amazon SSM Agent] を見つけます。
3. [Amazon SSM Agent] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[無効] を選択します。
5. [OK] をクリックします。

SSL3 および TLS バージョン 1.2 を有効にすることが必要

Windows に SSL/TLS を設定するには、Microsoft Windows ドキュメントの「How to Enable TLS 1.2」を参照してください。

には 1 つのユーザープロファイルしか存在できません WorkSpace

イメージの作成に使用している には WorkSpaces 、ユーザープロファイル (`D:\Users\username`) WorkSpace を 1 つだけ使用できます。の目的のユーザーに属さないユーザープロファイルをすべて削除します WorkSpace。

イメージ作成が機能するように、 WorkSpace には 3 つのユーザープロファイルしか設定できません。

- (`D:\Users\username`) の対象ユーザーの WorkSpaceユーザープロファイル
- デフォルトのユーザープロファイル (デフォルトプロファイルとも呼ばれます)
- 管理者ユーザープロファイル

追加のユーザープロファイルがある場合は、Windows コントロールパネルの詳細システムプロパティを使用して削除できます。

ユーザープロファイルを削除するには

1. 詳細システムプロパティにアクセスするには、以下のいずれかを実行します。
   - Windows + Pause Break キーを押し、[コントロールパネル] > [システムとセキュリティ] > [システム]ダイアログボックスの左側のペインで [システムの詳細設定]を選択します。
   - Windows の検索ボックスに「**`control panel`**」と入力します。コントロールパネルで、[システムとセキュリティ]、[システム] の順に選択し、[コントロールパネル] > [システムとセキュリティ] > [システム] ダイアログボックスの左側のペインで [システムの詳細設定] を選択します。
2. [システムのプロパティ] ダイアログボックスの [詳細設定] タブで、[ユーザープロファイル] の [設定] を選択します。
3. 管理者プロファイル、デフォルトプロファイル、および目的の WorkSpacesユーザーのプロファイル以外のプロファイルが一覧表示されている場合は、その追加プロファイルを選択し、削除を選択します。
4. プロファイルを削除するかどうか尋ねられたら、[はい] を選択します。

5. 必要に応じて、ステップ 3 と 4 を繰り返して、 に属していない他のプロファイルを削除します WorkSpace。
6. [OK] を 2 回選択し、コントロールパネルを閉じます。
7. を再起動します WorkSpace。

AppX パッケージがステージング状態になることはない

1 つ以上の AppX パッケージがステージング状態になっています。これにより、イメージの作成中に Sysprep エラーが発生する可能性があります。

ステージングされたすべての AppX パッケージを削除するには

1. Windows の検索ボックスに「**powershell**」と入力します。[管理者として実行] を選択します。
2. 「このアプリがデバイスに変更を加えることを許可しますか?」と尋ねられたら、[はい] を選択します。
3. Windows PowerShell ウィンドウで、次のコマンドを入力してステージングされたすべての AppX パッケージを一覧表示し、それぞれの後に Enter キーを押します。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. 以下のコマンドを入力して、ステージングされたすべての AppX パッケージを削除し、Enter キーを押します。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Image Checker を再度実行します。それでもこのテストに失敗する場合は、以下のコマンドを入力して、すべての AppX パッケージを削除し、それぞれの後に Enter キーを押します。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows が以前のバージョンからアップグレードされていないこと

イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows システム (Windows の機能/バージョンのアップグレード) ではサポートされません。

イメージを作成するには、Windows の機能/バージョンのアップグレードが行われ WorkSpace ていない を使用します。

Windows リアームカウントが 0 でないこと

リアーム機能を使用すると、Windows の試用バージョンのアクティベーション期間を延長できます。イメージ作成プロセスでは、リアームカウントを 0 以外の値にする必要があります。

Windows リアームカウントを確認するには

1. Windows の [スタート] メニューで [Windows システム] を選択し、[コマンドプロンプト] を選択します。
2. [コマンドプロンプト] ウィンドウで、以下のコマンドを入力し、Enter キーを押します。

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

リアームカウントを 0 以外の値にリセットするには、Microsoft Windows ドキュメントの「Sysprep (Generalize) a Windows installation」を参照してください。

トラブルシューティングに関するその他のヒント

が Image Checker によって実行されるすべてのテストに WorkSpace 合格しても、 からイメージを作成できない場合は WorkSpace、次の点を確認してください。

- WorkSpace がドメインゲストグループ内のユーザーに割り当てられていないことを確認します。ドメインアカウントがあるかどうかを確認するには、次の PowerShellコマンドを実行します。

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- Windows 7 WorkSpaces のみ: イメージの作成中にユーザープロファイルのコピー中に問題が発生した場合は、次の点を確認してください。
  - プロファイルパスが長いと、イメージ作成エラーが発生する可能性があります。ユーザープロファイル内のすべてのフォルダのパスが 261 文字未満であることを確認します。
  - システムとすべてのアプリケーションパッケージに、プロファイルフォルダに対する完全なアクセス許可を必ず付与してください。
  - ユーザープロファイルのファイルがプロセスによってロックされているか、イメージの作成中に使用されている場合、プロファイルのコピーが失敗する可能性があります。
- 一部のグループポリシーオブジェクト (GPO) では、Windows インスタンスの設定中に EC2Config サービスまたは EC2Launch スクリプトによって RDP 証明書のサムプリントへのアクセスがリクエストされると、そのアクセスは制限されます。イメージを作成する前に、継承がブロックされ、GPOs WorkSpace に を移動します。
- Windows Remote Management (WinRM) サービスが自動的に開始するように設定されていることを確認します。次の作業を行います。
  1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
  2. [名前] 列で、[Windows リモート管理 (WS-Management)] を見つけます。
  3. [Windows リモート管理 (WS-Management)] を選択し、[操作]、[プロパティ] の順に選択します。
  4. [全般] タブの [スタートアップの種類] で、[自動] を選択します。
  5. [OK] をクリックします。

ステップ 3: カスタムイメージとカスタムバンドルを作成する

WorkSpace イメージを検証したら、カスタムイメージとカスタムバンドルの作成に進むことができます。

カスタムイメージとカスタムバンドルを作成するには

1. にまだ接続している場合は WorkSpace、 WorkSpaces クライアントアプリケーションで Amazon WorkSpaces と Disconnect を選択して切断します。
2. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
3. ナビゲーションペインで、 を選択しますWorkSpaces。
4. を選択して詳細ページ WorkSpace を開き、イメージの作成 を選択します。のステータス WorkSpace が Stopped の場合、アクション 、イメージの作成 を選択する前に、まずそのステータスを開始する必要があります (アクション 、開始 WorkSpacesを選択) 。

   > **Note**
   >
   > プログラムでイメージを作成するには、 CreateWorkspaceImage API アクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceImage」の「」を参照してください。

5. 続行する前に を再起動 (再起動) WorkSpaceするように求めるメッセージが表示されます。Amazon WorkSpaces ソフトウェアを再起動すると、最新バージョンに WorkSpace 更新されます。

   メッセージ WorkSpace を閉じて の手順に従って、 を再起動しますの再起動 WorkSpace。完了したら、この手順の Step 4 を繰り返します。ただし、再起動メッセージが表示されたら、[次へ] を選択します。イメージを作成するには、 のステータスが WorkSpace Available で、その変更ステータスが None である必要があります。
6. イメージを識別するのに役立つイメージの名前と説明を入力し、[イメージの作成] を選択します。イメージの作成中、 のステータス WorkSpace は一時停止になり、 WorkSpace は使用できません。

   > **Note**
   >
   > イメージの説明を入力するときは、特殊文字「-」を使用しないようにしてください。使用しないと、エラーが発生します。

7. ナビゲーションペインで [Images] を選択します。イメージは、ステータスが Available に WorkSpace 変わると完了します (これには最大 45 分かかる場合があります) 。
8. イメージを選択し、[Actions] (アクション)、[Create bundle] (バンドルの作成) を選択します。

> **Note**
>
> プログラムによりバンドルを作成するには、CreateWorkspaceBundle API アクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceBundle」の「」を参照してください。

9. バンドル名と説明を入力し、次の操作を行います。

   - バンドルハードウェアタイプ で、このカスタムバンドル WorkSpaces から起動するときに使用するハードウェアを選択します。
   - [Storage settings] (ストレージ設定) で、ルートボリュームとユーザーボリュームサイズのデフォルトの組み合わせのいずれかを選択するか、[Custom] (カスタム) を選択し、[Root volume size] (ルートボリュームサイズ) と [User volume size] (ユーザーボリュームサイズ) に値 (最大 2000 GB) を入力します。

     デフォルトのルートボリューム (Microsoft Windows の場合は C ドライブ、Linux の場合は /) およびユーザーボリューム (Windows の場合は D ドライブ、Linux の場合は /home) で使用できるサイズの組み合わせは以下のとおりです。

     - ルート: 80 GB、ユーザー: 10 GB、50 GB、または 100 GB
     - ルート: 175 GB、ユーザー: 100 GB
     - Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro WorkSpaces のみ: ルート: 100 GB、ユーザー: 100 GB

     または、ルートボリュームとユーザーボリュームをそれぞれ 2,000 GB まで拡張できます。

     > **Note**
     >
     > データを確実に保持するために、 の起動後にルートボリュームまたはユーザーボリュームのサイズを小さくすることはできません WorkSpace。代わりに、 を起動するときに、これらのボリュームの最小サイズを必ず指定してください WorkSpace。ルートボリュームの場合は 80 GB、ユーザーボリュームの場合は 10 GB PowerPro WorkSpace 以上の値、標準、パフォーマンス、パワー、または を起動できます。Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または を起動できます。ルートボリュームの場合は GraphicsPro WorkSpace 100 GB、ユーザーボリュームの場合は 100 GB 以上です。

10. [Create bundle] (バンドルの作成) を選択します。

11. バンドルが作成されたことを確認するには、[Bundles] (バンドル) を選択し、バンドルが表示されていることを確認します。

Windows WorkSpaces カスタムイメージに含まれるもの

Windows 7、Windows 10、または Windows 11 からイメージを作成すると WorkSpace、Cドライブの内容全体が含まれます。

Windows 10 または 11 の場合 WorkSpaces、 のユーザープロファイルD:\Users*username*はカスタムイメージに含まれません。

Windows 7 では WorkSpaces、以下を除き、 のユーザープロファイルの内容全体D:\Users*username*が含まれます。

- 連絡先
- ダウンロード
- 音楽
- 画像
- ゲームのセーブデータ
- 動画
- ポッドキャスト
- 仮想マシン
- .virtualbox
- トレース
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\

- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary internet files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Linux WorkSpace カスタムイメージに含まれるもの

Amazon Linux からイメージを作成すると WorkSpace、ユーザーボリューム (/home) の内容全体が削除されます。ルートボリューム (/) の内容は含まれますが、以下に該当するフォルダとキーは削除されます。

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg

- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/libAccountsService//users

以下のキーは、カスタムイメージの作成中に破棄されます。

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

カスタム WorkSpaces バンドルの更新

既存のカスタム WorkSpaces バンドルを更新するには、バンドルに基づいて WorkSpace を変更し、WorkSpace からイメージを作成し、新しいイメージでバンドルを更新します。更新されたバンドルを使用して新しい WorkSpaces を起動できます。

> **Important**
>
> 既存の WorkSpaces は、基になっているバンドルを更新しても自動的に更新されません。更新済みのバンドルに基づく既存の WorkSpaces を更新するには、WorkSpaces を再構築するか、一旦削除してから再作成する必要があります。

コンソールを使用してバンドルを更新するには

1. バンドルに基づく WorkSpace に接続し、必要な変更を加えます。たとえば、最新のオペレーティングシステムとアプリケーションのパッチを適用し、追加のアプリケーションをインストールすることができます。

   または、バンドルの作成や変更に使用したイメージと同じ基本ソフトウェアパッケージ (Plus または Standard) を使用して新しい WorkSpace を作成することもできます。
2. まだ WorkSpace に接続している場合は、WorkSpaces クライアントアプリケーションで [Amazon Workspaces]、[Disconnect] (切断) の順に選択して切断します。
3. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
4. ナビゲーションペインで [WorkSpaces] を選択します。
5. WorkSpace を選択し、[Actions]、[Create Image] を選択します。WorkSpace のステータスが STOPPED の場合、[Actions] (アクション)、[Create Image] (イメージの作成) を選択する前に、まずそれを開始する必要があります ([Actions] (アクション)、[Start WorkSpaces] (WorkSpaces の起動) の順に選択)。
6. イメージ名と説明を入力して、[イメージの作成] を選択します。イメージが作成されている間、WorkSpace は使用できません。イメージ作成プロセスの詳細については、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。
7. ナビゲーションペインで [Bundles] を選択します。
8. バンドルを選択して詳細ページを開き、[Source image] (ソースイメージ) で [Edit] (編集) を選択します。
9. [Update source image] (ソースイメージの更新) ページで、作成したイメージを選択し、[Update bundle] (バンドルの更新) を選択します。
10. 必要に応じて、バンドルに基づく既存の WorkSpaces を更新します。更新するには、WorkSpaces を再構築するか、これを削除してから再作成します。詳細については、「の再構築 WorkSpace」を参照してください。

プログラムによりバンドルを更新するには

プログラムによりバンドルを更新するには、UpdateWorkspaceBundle API アクションを使用します。詳細については、Amazon WorkSpaces API リファレンスの UpdateWorkspaceBundle を参照してください。

WorkSpaces のカスタムイメージのコピー

AWS リージョン内、またはリージョン間でカスタム WorkSpaces イメージをコピーできます。イメージをコピーすると、独自の識別子の付いた同一のイメージを作成したことになります。

コピー先のリージョンで BYOL が有効になっている限り、自分のライセンス使用 (BYOL) イメージを別のリージョンにコピーできます。関係するすべてのアカウントとリージョンで BYOL が有効になっていることを確認してください。

> **Note**
>
> 中国 (寧夏) リージョンでは、同じリージョン内でのみイメージをコピーできます。
> AWS GovCloud (US) Regionで他の AWS リージョンとの間でイメージをコピーするには、AWS サポートにお問い合わせください。
> オプトインリージョンで、他のリージョンにイメージをコピーするには、AWS サポートにお問い合わせください。オプトインリージョンの詳細については、「利用できるリージョン」を参照してください。

別の AWS アカウントによって共有されたイメージをコピーすることもできます。共有イメージの詳細については、WorkSpaces のカスタムイメージの共有または共有解除 を参照してください。

リージョン間のイメージのコピーに追加料金はかかりません。ただし、コピー先リージョンでのイメージ数のクォータは適用されます。Amazon WorkSpaces クォータの詳細については、 Amazon WorkSpaces クォータ を参照してください。

イメージをコピーするための IAM 許可

IAM ユーザーを使用してイメージをコピーする場合、ユーザーには `workspaces:DescribeWorkspaceImages` および `workspaces:CopyWorkspaceImage` のアクセス許可が必要です。

次のポリシー例では、指定したイメージを、指定したリージョンの指定したアカウントにコピーすることをユーザーに許可します。

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

```
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

イメージを所有していないアカウントの共有イメージをコピーするための IAM ポリシーを作成する場合は、ARN でアカウント ID を指定できません。代わりに、次のポリシー例に示すように、アカウント ID には * を使用する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

ARN でアカウント ID を指定できるのは、コピーするイメージをそのアカウントが所有している場合だけです。

IAM の操作方法の詳細については、WorkSpaces の Identity and Access Management を参照してください。

イメージの一括コピー

コンソールを使用して、イメージを 1 つずつコピーできます。イメージを一括コピーするには、CopyWorkspaceImage API オペレーションまたは AWS Command Line Interface (AWS CLI) 内の copy-workspace-image コマンドを使用します。詳細については、Amazon WorkSpaces API リファレンスの CopyWorkspaceImage または AWS CLI コマンドリファレンスの copy-workspace-image を参照してください。

> **Important**
>
> 共有イメージをコピーする前に、正しい AWS アカウントから共有されていることを確認します。イメージが共有されているかどうかを判断し、イメージを所有している AWS アカウント ID を確認するには、DescribeWorkSpaceImages および DescribeWorkspaceImagePermissions API オペレーションを使用するか、AWS CLI で describe-workspace-images および describe-workspace-image-permissions コマンドを使用します。

コンソールを使用してイメージをコピーするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. イメージを選択し、[Actions] (アクション)、[Copy image] (イメージをコピー) の順に選択します。
4. [Select destination] (対象を選択する) で、イメージのコピー先の AWS リージョンを選択します。
5. [Name of the copy] (コピーの名前) で、コピーしたイメージの新しい名前を入力し、[Description] (説明) で、コピーしたイメージの説明を入力します。
6. (オプション) [Tags] (タグ) で、コピーしたイメージのタグを入力します。詳細については、「WorkSpaces のリソースにタグを付ける」を参照してください。
7. [Copy image] (イメージのコピー) を選択します。

WorkSpaces のカスタムイメージの共有または共有解除

WorkSpaces のカスタムイメージは、同じ AWS リージョン内の AWS アカウント間で共有できます。イメージの共有後、受取人アカウントは、必要に応じてイメージを他の AWS リージョンにコピーできます。イメージのコピーの詳細については、WorkSpaces のカスタムイメージのコピー を参照してください。

> **Note**
>
> 中国 (寧夏) リージョンでは、同じリージョン内でのみイメージをコピーできます。AWS GovCloud (US) Regionで他の AWS リージョンとの間でイメージをコピーするには、AWS サポートにお問い合わせください。

イメージの共有に追加料金はかかりません。ただし、AWS リージョンでのイメージ数のクォータは適用されます。共有イメージは、受信者がイメージをコピーするまで、受信者アカウントのクォータにはカウントされません。Amazon WorkSpaces クォータの詳細については、 Amazon WorkSpaces クォータ を参照してください。

共有イメージを削除するには、そのイメージを削除する前に共有を解除する必要があります。

ライセンス持ち込みのイメージを共有する

Bring-Your-Own-License (BYOL) イメージは、BYOL が有効になっている AWS アカウントとのみ共有できます。BYOL イメージを共有する先の AWS アカウントも、同じ組織の一部である (同じ支払いアカウントに属する) 必要があります。

> **Note**
>
> AWS GovCloud (米国西部) および AWS GovCloud (米後東部) リージョンでは、AWS アカウント間での BYOL イメージの共有は、現時点ではサポートされていません。AWS GovCloud (米国西部) および AWS GovCloud (米国東部) リージョンのアカウント間で BYOL イメージを共有する場合は、AWS サポートにお問い合わせください。

自分に共有されたイメージ

自分にイメージが共有された場合は、コピーできます。その後、共有イメージのコピーを使用して、新しい WorkSpaces を起動するためのバンドルを作成できます。

> **Important**
>
> 共有イメージをコピーする前に、正しい AWS アカウントから共有されていることを確認します。イメージが共有されているかどうかをプログラムで判断するには、DescribeWorkSpaceImages および DescribeWorkspaceImagePermissions API オペレー

ションを使用するか、 AWS Command Line Interface (CLI) で describe-workspace-images および describe-workspace-image-permissions コマンドを使用します。

自分に共有されたイメージに対して表示される作成日は、イメージが最初に作成された日付であり、イメージが自分に共有された日付ではありません。

自分にイメージが共有されている場合、そのイメージを他のアカウントと共有することはできません。

イメージを共有するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. イメージを選択して、詳細ページを開きます。
4. イメージの詳細ページの [Shared accounts (共有アカウント)] セクションで、[Add account (アカウントの追加)] を選択します。
5. [Add account (アカウントの追加)] ページの [Add account to share with (共有するアカウントの追加] で、イメージの共有先のアカウントのアカウント ID を入力します。

   Important

   イメージを共有する前に、共有先の AWS アカウントの ID が正しいことを確認してください。

6. [Share image (イメージの共有)] を選択します。

   Note

   共有イメージを使用するには、まず受信者アカウントでイメージをコピーする必要があります。その後、受取人アカウントは、共有イメージのコピーを使用して新しい WorkSpaces を起動するためのバンドルを作成できます。

イメージの共有を停止するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。

3. イメージを選択して、詳細ページを開きます。
4. イメージの詳細ページの [Shared accounts (共有アカウント)] セクションで、共有を停止する AWS アカウントを選択し、[Unshare (共有解除)] を選択します。
5. イメージの共有解除を確認するメッセージが表示されたら、[Unshare (共有解除)] を選択します。

> **Note**
>
> 共有を解除した後にイメージを削除する場合、まず共有されているすべてのアカウントからそのイメージの共有を解除する必要があります。

イメージの共有を解除すると、受信者アカウントはイメージのコピーを作成できなくなります。ただし、受取人アカウント内に既に存在する共有イメージのコピーは、このアカウント内に残り、これらのコピーから新しい WorkSpaces を起動できます。

プログラムによりイメージを共有または共有解除するには

プログラムによりイメージを共有または共有を解除するには、UpdateWorkspaceImagePermission APIオペレーションまたは update-workspace-image-permission AWS Command Line Interface (AWS CLI) コマンドを使用します。イメージが共有されているかどうかを確認するには、DescribeWorkspaceImagePermissions API オペレーションまたは describe-workspace-image-permissions CLI コマンドを使用します。

WorkSpaces カスタムバンドルまたはイメージを削除する

必要に応じて、未使用のカスタムバンドルまたはカスタムイメージを削除できます。

バンドルを削除する

バンドルを削除するには、 WorkSpaces まずそのバンドルをベースにしたものをすべて削除する必要があります。

コンソールを使用してバンドルを削除するには

1. https://console.aws.amazon.com/workspaces/ WorkSpaces でコンソールを開きます。
2. ナビゲーションペインで [Bundles] を選択します。

3. バンドルを選択し、[Delete] (削除) を選択します。
4. 確認を求めるメッセージが表示されたら、[Delete] を選択します。

プログラムによりバンドルを削除するには

プログラムによりバンドルを削除するには、DeleteWorkspaceBundle API アクションを使用します。詳細については、Amazon WorkSpaces API DeleteWorkspaceBundleリファレンスのを参照してください。

> **Note**
>
> バンドルを削除してから 2 時間以上待ってから、同じ名前の新しいバンドルを作成してください。

イメージを削除します。

カスタムバンドルを削除した後で、バンドルの作成または更新に使用したイメージを削除できます。

イメージを削除するには、まずそのイメージに関連付けられているバンドルを削除するか、別のソースイメージを使用するようにそれらのバンドルを更新する必要があります。また、他のアカウントと共有されている場合は、イメージの共有を解除する必要があります。また、イメージは [Pending] (保留中) または [Validating] (検証中) 状態になることもできません。

コンソールを使用してイメージを削除するには

1. https://console.aws.amazon.com/workspaces/ WorkSpaces でコンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. イメージを選択し、[Delete] (削除) を選択します。
4. 確認を求めるメッセージが表示されたら、[Delete] を選択します。

プログラムによりイメージを削除するには

プログラムによりイメージを削除するには、DeleteWorkspaceImage API アクションを使用します。詳細については、Amazon WorkSpaces API DeleteWorkspaceImageリファレンスのを参照してください。

自分の Windows デスクトップライセンスを使用する

Microsoft とのライセンス契約で許可されている場合は、Windows 10 または 11 デスクトップを に持ち込んでデプロイできます WorkSpaces。そのためには、Bring Your Own License (BYOL) を有効にして、以下の要件を満たす Windows 10 または 11 ライセンスを用意する必要があります。での Microsoft ソフトウェアの使用の詳細については AWS、「Amazon Web Services と Microsoft 」を参照してください。

Microsoft のライセンス条項に準拠するために、 は AWS クラウド専用のハードウェアで BYOL WorkSpaces AWS を実行します。独自のライセンスを持ち込むことで、ユーザーに一貫したエクスペリエンスを提供できます。詳細については、「 のWorkSpaces 料金」を参照してください。

> **Important**
>
> イメージの作成は、Windows 10 または 11 の 1 つのバージョンから Windows 10 または 11 の新しいバージョンにアップグレードされた Windows 10 または 11 システムではサポートされていません (Windows の機能/バージョンアップグレード)。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、 WorkSpaces イメージ作成プロセスでサポートされています。

内容

- BYOL アカウントをリンクする

要件

開始する前に、以下の点を確認してください。

- Microsoft の使用許諾契約書では、仮想ホスト環境で Windows を実行できます。
- GPU 対応ではないバンドル (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および 以外のバンドル GraphicsPro) を使用する場合は、リージョン WorkSpaces ごとに 100 個以上を使用することを確認します。これらの 100 は、 AlwaysOn と の任意の組み合わせ WorkSpaces にすることができます AutoStop WorkSpaces。専用ハードウェアで を実行するには、リージョン WorkSpaces ごとに 100 WorkSpaces 個以上を使用する必要があります。Microsoft のライセンス要件に準拠するには、専用ハードウェア WorkSpaces で を実行する必要があります。専用ハードウェアは AWS 側でプロビジョニングされるため、VPC はデフォルトのテナンシーを維持できます。

  GPU 対応 (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro) バンドルを使用する場合は、専用ハードウェアでリージョン WorkSpaces で 1 か月あたり 4 AlwaysOn つ以上の 20 AutoStop GPU 対応 を実行することを確認します。

> **Note**
>
> - Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro バンドルは、現時点では PCoIP プロトコルに対してのみ作成できます。
> - 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。を WorkSpaces Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「の移行 WorkSpace」を参照してください。
> - 現在、アジアパシフィック (ムンバイ) リージョンではグラフィックと GraphicsPro バンドルは利用できません。
> - Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro バンドルは現在、アフリカ (ケープタウン) リージョンでは利用できません。
> - をアフリカ (ケープタウン) リージョン WorkSpaces で実行するには、アフリカ (ケープタウン) リージョン WorkSpaces で 400 以上を実行する必要があります。
> - Windows 11 バンドルは WSP プロトコルのためにのみ作成できます。
> - Graphics.g4dn および GraphicsPro.g4dn バンドルは現在 Windows 11 では使用できません。
> - グラフィックと GraphicsPro バンドルは Windows 11 ではサポートされていません。

  - バリューバンドルは Windows 11 で使用できません。既存の値バンドル WorkSpaces の移行の詳細については、「」を参照してくださいの移行 WorkSpace。
  - 最高のビデオ会議エクスペリエンスを得るには、パワーまたは PowerPro バンドルの使用をお勧めします。
  - Windows 11 では、統合拡張ファームウェアインターフェイス (UEFI) ブートモードが機能する必要があります。VM を正常にインポートするには、オプションの `--boot-mode`パラメータを UEFI として指定してください。

- WorkSpaces は、/16 IP アドレス範囲内の管理インターフェイスを使用できます。管理インターフェイスは、インタラクティブストリーミングに使用される安全な WorkSpaces 管理ネットワークに接続されます。これにより、 WorkSpaces は を管理できます WorkSpaces。詳細については、「ネットワークインターフェイス」を参照してください。この目的のために、次の IP アドレス範囲のうち少なくとも 1 つから /16 ネットマスクを予約する必要があります。
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

  > **Note**
  >
  > - WorkSpaces サービスを採用すると、使用可能な管理インターフェイスの IP アドレス範囲が頻繁に変更されます。現在使用可能な範囲を確認するには、 list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) コマンドを実行します。
  > - 選択した /16 CIDR ブロックに加えて、54.239.224.0/20 IP アドレス範囲がすべての AWS リージョンの管理インターフェイストラフィックに使用されます。

- BYOL の Microsoft Windows および Microsoft Office KMS アクティベーションに必要な管理インターフェイスポートが開いていることを確認します WorkSpaces。詳細については、「管理インターフェイスポート」を参照してください。
- サポートされている 64 ビットバージョンの Windows を実行する仮想マシン (VM) があります。サポートされているバージョンのリストについては、このトピックの BYOL でサポートされる Windows のバージョン セクションを参照してください 。VM は、以下の条件も満たす必要があります。

- Windows オペレーティングシステムは、キー管理サーバーに対してアクティブにする必要があります。
- Windows オペレーティングシステムのメイン言語が [英語 (米国)] であることを確認してください。
- Windows に付属していないソフトウェアを VM にインストールすることはできません。後でカスタムイメージを作成するときに、ウイルス対策ソリューションなどのソフトウェアを追加することができます。
- イメージを作成する前に、デフォルトのユーザープロファイル (`C:\Users\Default`) をカスタマイズしたり、他のカスタマイズを行ったりしないでください。すべてのカスタマイズは、イメージの作成後に行う必要があります。グループポリシーオブジェクト (GPO) を使用してユーザープロファイルをカスタマイズし、イメージの作成後に適用することをお勧めします。これは、GPO を使用して行われたカスタマイズは簡単に変更またはロールバックでき、デフォルトのユーザープロファイルに対して行われたカスタマイズよりもエラーが発生しにくいためです。
- イメージを共有する前に、ローカル管理者アクセス権を持つ WorkSpaces_BYOL アカウントを作成する必要があります。このアカウントのパスワードは後で必要になる可能性があるため、メモしておいてください。
- VM は、最大サイズが 70 GB、空き容量が 10 GB 以上の 1 つのボリューム上にあることが必要です。また、BYOL イメージの Microsoft Office へのサブスクライブを計画している場合は、VM は最大サイズが 70 GB で、20 GB 以上の空き容量を持つ 1 つのボリューム上に存在する必要があります。ルートボリュームがある DISK は 70 GB を超えることはできません。
- VM は Windows PowerShell バージョン 4 以降を実行する必要があります。

- ステップ 3: Windows VM で BYOL Checker PowerShell スクリプトを実行する で BYOL チェッカースクリプトを実行する前に、最新の Microsoft Windows パッチがインストールされていることを確認してください。

> **Note**
>
> - BYOL では AutoStop WorkSpaces、多数の同時ログインにより、 が使用可能 WorkSpaces になるまでの時間が大幅に長くなる可能性があります。多数のユーザーが AutoStop WorkSpaces 同時に BYOL にログインすることが予想される場合は、アカウントマネージャーにアドバイスを求めてください。

- 暗号化された AMI はインポートプロセスではサポートされません。EC2 AMI の作成に使用したインスタンスが EBS 暗号化を無効にしていることを確認してください。暗号化は、最終的な WorkSpaces がプロビジョニングされた後に有効にできます。

BYOL でサポートされる Windows のバージョン

VM は、次のいずれかの Windows バージョンで実行する必要があります。

- Windows 10 バージョン 21H2 (2021 年 12 月更新)
- Windows 10 バージョン 22H2 (2022 年 11 月更新)
- Windows 10 Enterprise LTSC 2019 (1809)
- Windows 10 Enterprise LTSC 2021 (21H2)
- Windows 11 Enterprise 23H2 (2023 年 10 月リリース)
- Windows 11 Enterprise 22H2 (2022 年 10 月リリース)

サポートされているすべての OS バージョンは、 を使用している AWS リージョンで利用可能なすべてのコンピューティングタイプをサポートしています WorkSpaces。Microsoft でサポートされなくなった Windows のバージョンは動作が保証されず、 AWS サポートでもサポートされません。

> **Note**
>
> 現時点では BYOL での Windows 10 N および Windows 11 N バージョンはサポートされていません。

BYOL イメージに Microsoft Office を追加する

BYOL イメージの取り込みプロセス中に Windows 10 を使用している場合は、 から Microsoft Office Professional 2016 (32 ビット) または 2019 (64 ビット) をサブスクライブできます AWS。Windows 11 を使用している場合は、Microsoft Office Professional 2019 (64 ビット) にサブスクライブできます。これらのオプションのいずれかを選択すると、Microsoft Office は BYOL イメージにプリインストールされ、このイメージから起動 WorkSpaces するすべての に含まれます。

を通じて Office にサブスクライブすることを選択した場合は AWS、追加料金が適用されます。詳細については、「 のWorkSpaces 料金」を参照してください。

Important

- BYOL イメージの作成に使用している VM に Microsoft Office が既にインストールされている場合は、 を通じて Office にサブスクライブする場合は、VM からアンインストールする必要があります AWS。
- を通じて Office にサブスクライブする場合は AWS、VM に少なくとも 20 GB の空きディスク容量があることを確認してください。
- イメージのインポート中は、Office 2016 または 2019 にサブスクライブできますが、Office 2021 にはサブスクライブできません。Office 2021 および他のアプリケーション (Microsoft Visio 2021 や Microsoft Project 2021 など) については、「アプリケーションの管理」を参照してください。
- Amazon でブラウザベースのアプリケーションとデスクトップアプリケーションの両方に独自の Microsoft 365 ライセンスを持ち込むには WorkSpaces、BYOL イメージの取り込みプロセスが完了した後に、BYOL イメージに Microsoft 365 アプリケーションをインストールします。

Note

Graphics.g4dn および GraphicsPro.g4dn BYOL イメージは Office 2019 のみをサポートし、Office 2016 はサポートしていません。

Office のサブスクライブを選択した場合、BYOL イメージの取り込み処理には最低 3 時間かかります。

BYOL 取り込みプロセス中の Office へのサブスクライブの詳細については、ステップ 6: WorkSpaces コンソールを使用して BYOL イメージを作成する を参照してください。

オフィスの言語設定

Office サブスクリプションに使用される言語は、BYOL イメージの取り込みを実行している AWS リージョンに基づいて選択されます。例えば、アジアパシフィック (東京) リージョンで BYOL イメージの取り込みを実行している場合、Office サブスクリプションの言語は日本語になります。

デフォルトでは、頻繁に使用する Office 言語パックがいくつか にインストールされます WorkSpaces。目的の言語パックがインストールされていない場合は、Microsoft から追加の言語パッ

クをダウンロードできます。詳細については、Microsoft のドキュメントの「Office 用言語アクセサリパック」を参照してください。

Office の言語を変更するには、いくつかのオプションがあります。

オプション 1: 個々のユーザーが Office の言語設定をカスタマイズできるようにする

個々のユーザーは、 の Office 言語設定を調整できます WorkSpaces。詳細については、Microsoft ドキュメントの「Office で編集言語または作成言語を追加する、または言語の基本設定を設定する」を参照してください。

オプション 2: GPO 管理テンプレート (.admx/.adml) を使用して、すべての WorkSpaces ユーザーにデフォルトの Office 言語設定を適用する

グループポリシーオブジェクト (GPO) 設定を使用して、 WorkSpaces ユーザーにデフォルトの Office 言語設定を適用できます。

> **Note**
>
> WorkSpaces ユーザーは GPO を通じて適用される言語設定を上書きすることはできません。

GPO を使用して Office の言語を設定する方法の詳細については、Microsoft のドキュメントの「Office の言語設定と設定をカスタマイズする」を参照してください。Office 2016 と Office 2019 では、同じ GPO 設定が使用されます (Office 2016 とラベル付けされています)。

GPO を使用するには、Active Directory 管理ツールをインストールする必要があります。Active Directory 管理ツールを使用して GPO を操作する方法については、WorkSpaces の Active Directory 管理ツールを設定する を参照してください。

Office 2016 または Office 2019 のポリシー設定を設定する前に、Microsoft ダウンロードセンターから Office の管理用テンプレートファイル (.admx/.adml) をダウンロードする必要があります。管理テンプレートファイルをダウンロードしたら、 WorkSpaces ディレクトリのドメインコントローラーのセントラルストアに `office16.admx`および `office16.adml` ファイルを追加する必要があります。(`office16.admx` および `office16.adml` ファイルは、Office 2016 と Office 2019 の両方に適用されます)。`.admx` および `.adml` ファイルの操作の詳細については、Microsoft のドキュメントの「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。 WorkSpaces ディレクトリ管理 WorkSpace またはディレクトリに結合されている Amazon EC2 インスタンスで次の手順を実行します。

Office のグループポリシー管理用テンプレートファイルをインストールするには

1. Microsoft ダウンロードセンターから Office の管理用テンプレートファイル (.admx/.adml) をダウンロードします。
2. ディレクトリ管理 WorkSpace またはディレクトリに参加している WorkSpaces Amazon EC2 インスタンスで Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します`\\example.com`。
3. SYSVOL フォルダを開きます。
4. *FQDN* という名前のフォルダを開きます。
5. Policies フォルダを開きます。今、`\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies` に入っているはずです。
6. まだ存在しない場合は、PolicyDefinitions という名前のフォルダを作成します。
7. PolicyDefinitions フォルダを開きます。
8. office16.admx ファイルを `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions` フォルダにコピーします。
9. PolicyDefinitions フォルダに en-US という名前のフォルダを作成します。
10. en-US フォルダを開きます。
11. office16.adml ファイルを `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions\en-US` フォルダにコピーします。

Office の GPO 言語設定を設定するには

1. ディレクトリ管理 WorkSpace またはディレクトリに参加している Amazon EC2 インスタンスで WorkSpaces 、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト ([フォレスト:***FQDN***]) を展開します。
3. [ドメイン] を展開します。
4. FQDN を展開します (example.com など)。
5. FQDN を選択し、コンテキスト (右クリック) メニューを開くか、[アクション] メニューを開き、[このドメインに GPO を作成し、ここにリンクする] を選択します。

6. GPO に名前を付けます (**`Office`** など)。
7. GPO を選択し、コンテキスト (右クリック) メニューを開くか、[アクション] メニューを開き、[編集] を選択します。
8. [グループポリシー管理エディタ] で、[ユーザー設定]、[ポリシー]、[ローカルコンピュータから取得した管理用テンプレートポリシー定義 (ADMX ファイル)]、[Microsoft Office 2016]、[言語設定] の順に選択します。

   > **Note**
   >
   > Office 2016 と Office 2019 では、同じ GPO 設定が使用されます (Office 2016 とラベル付けされています)。 [User Configuration] (ユーザー設定) で、[Administrative Template Policy definitions (ADMX files) retrieved from the local computer] (ローカルコンピュータから取得した管理用テンプレートポリシー定義 (ADMX ファイル)) が表示されない場合は、[ポリシー]、`office16.admx` ファイル、および `office16.adml` ファイルがドメインコントローラーに正しくインストールされていません。

9. [言語設定] で、次の設定で使用する言語を指定します。各設定を [有効] に設定し、[オプション] で目的の言語を選択します。[OK] を選択して各設定を保存します。

   - [表示言語] > [ヘルプを表示]
   - [表示言語] > [メニューとダイアログボックスを表示]
   - [編集言語] > [主要編集言語]

10. 終了したら、グループポリシー管理ツールを閉じます。
11. グループポリシー設定の変更は、 の次のグループポリシー更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

    - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します) 。
    - 管理コマンドプロンプトから、gpupdate /force と入力します。

オプション 3: の Office 言語レジストリ設定を更新する WorkSpaces

レジストリを使用して Office の言語設定を設定するには、次のレジストリ設定を更新します。

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResourcesUILanguage

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\HelpLanguage

これらの設定では、適切な Office ロケール ID (LCID) を持つ DWORD キー値を追加します。たとえば、英語 (米国) の LCID は 1033 です。LCID は 10 進数であるため、DWORD 値の [基本] オプションを [10 進数] に設定する必要があります。OfficeLCIDs、Microsoft ドキュメントの「Office 2016 の言語識別子と OptionState ID 値」を参照してください。

これらのレジストリ設定は、GPO 設定またはログオンスクリプト WorkSpaces を使用して に適用できます。

Office の言語設定の操作の詳細については、Microsoft のドキュメントの「Office の言語設定と設定をカスタマイズする」を参照してください。

既存の BYOL に Office を追加する WorkSpaces

また、次の手順 WorkSpaces を実行して、Office にサブスクリプションを既存の BYOL に追加することもできます。

- アプリケーションの管理 (推奨) - 既存の に Microsoft Office、Microsoft Visio、または Microsoft Project 2021 をインストールして設定できます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace - Office がインストールされた BYOL バンドルをインストールしたら、WorkSpaces 移行機能を使用して、既存の BYOL を Office WorkSpaces にサブスクライブしている BYOL バンドルに移行できます。詳細については、「の移行 WorkSpace」を参照してください。

> **Note**
>
> アプリケーション管理オプションは、Microsoft Office 2021 および Microsoft Visio 2021 や Microsoft Project 2021 などの他のアプリケーションを にインストールするために使用できます WorkSpaces。に Microsoft Office 2016 または 2019 をインストールするには WorkSpaces、 を使用しますの移行 WorkSpace。

Microsoft Office のバージョン間で移行する

Microsoft Office の 1 つのバージョンを別のバージョンに移行する際には、次のオプションがあります。

- アプリケーションの管理 (推奨) – 元の Office バージョンをアンインストールし、Office 2021 および Microsoft Visio 2021 や Microsoft Project 2021 などの他のアプリケーションを既存の にインストールできます WorkSpaces。例えば、Microsoft Office 2019 から Microsoft Office 2021 に移行するには、アプリケーションの管理ワークフローを使用して Microsoft Office 2019 をアンインストールし、Microsoft Office 2021 をインストールします。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace – Microsoft Office 2016 から Microsoft Office 2019 または Microsoft Office 2019 から Microsoft Office 2016 に移行するには、移行先の Office のバージョンにサブスクライブされている BYOL バンドルを作成する必要があります。次に、 WorkSpaces 移行機能を使用して、Office に WorkSpaces サブスクライブされている既存の BYOL を、移行先の Office のバージョンにサブスクライブされている BYOL バンドルに移行します。例えば、Microsoft Office 2016 から Microsoft Office 2019 に移行するには、Microsoft Office 2019 にサブスクライブされている BYOL バンドルを作成します。次に、 WorkSpaces 移行機能を使用して、Office 2016 に WorkSpaces サブスクライブされている既存の BYOL を、Office 2019 にサブスクライブされている BYOL バンドルに移行します。詳細については、「 の移行 WorkSpace」を参照してください。

これらのオプションを使用して、 を介して Microsoft Office に WorkSpaces サブスクライブされている AWS を Microsoft 365 アプリケーションに移行できます。ただし、アプリケーションの管理は、 からの Microsoft Office のアンインストールに限定されます WorkSpace。に Microsoft 365 アプリケーションをインストールするには、独自のツールとインストーラーを導入する必要があります WorkSpaces。

> **Note**
>
> 管理アプリケーションを使用すると、 に Microsoft Office、Microsoft Visio、または MicrosoftProject 2021 をインストールまたはアンインストールできます WorkSpaces。Microsoft Office 2016 または 2019 バージョンでは、 からのみ削除できます WorkSpaces。に Microsoft Office 2016 または 2019 をインストールするには WorkSpaces、を移行します WorkSpace。

移行プロセスの詳細については、の移行 WorkSpace を参照してください。

Office からサブスクリプションを解除する

Office のサブスクリプションを解除する場合は、次のオプションがあります。

- アプリケーションの管理 (推奨) - Microsoft Office や、Microsoft Visio や Microsoft Project などの他のアプリケーションを からアンインストールできます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace - Office にサブスクライブしていない BYOL バンドルを作成できます。次に、WorkSpaces 移行機能を使用して、既存の BYOL WorkSpaces を Office にサブスクライブしていない BYOL バンドルに移行します。詳細については、「の移行 WorkSpace」を参照してください。

Office のアップデート

を通じて Office にサブスクライブしている場合 AWS、Office の更新は通常の Windows 更新プログラムの一部として含まれます。セキュリティパッチおよび更新プログラムを最新の状態に保つには、BYOL のベースイメージを定期的にアップデートすることをお勧めします。

ステップ 1: Amazon WorkSpaces コンソールを使用して BYOL のアカウントの適格性を確認する

BYOL のアカウントを有効にする前に、検証プロセスを経て BYOL 適格性を確認する必要があります。このプロセスが完了するまで、BYOL を有効にするオプションは Amazon WorkSpaces コンソールでは使用できません。

> **Note**
>
> 検証プロセスには少なくとも 1 営業日かかります。既存のアカウントの CIDR 範囲と BYOL 設定を別の AWS アカウントに適用する場合は、それらをリンクして同じ基盤となるハードウェアを使用できます。 AWS アカウントをリンクするには、サポートチケットを送信する必要はありません。 CreateAccountLinkInvitations や などの APIsを使用して AWS 、アカウントをAcceptAccountLinkInvitation接続できます。詳細については、「BYOL アカウントをリンクする」を参照してください。

Amazon WorkSpaces コンソールを使用して BYOL のアカウントの適格性を確認するには

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

2. ナビゲーションペインでアカウント設定 を選択し、「自分のライセンスを使用 (BYOL)」で WorkSpaces 「BYOL 設定を表示」を選択します。アカウントが現在 BYOL の対象になっていない場合は、次のステップに関するガイダンスがメッセージに表示されます。開始するには、AWS アカウントマネージャーまたは販売担当者に問い合わせるか、 AWS Support センターにお問い合わせください。担当者が BYOL 適格性を検証します。

   BYOL 適格性を判断するには、お客様から特定の情報を担当者にご提供いただく必要があります。例えば、次の質問への回答を求められる場合があります。

   - 前述の BYOL 要件を確認して承諾しましたか?
   - BYOL でアカウントを有効にする必要がある AWS リージョン
   - AWS リージョンごとにデプロイする予定の BYOL の数 WorkSpaces はいくつですか ?
   - ランプアップ計画はどのような内容ですか?
   - リセラー WorkSpaces から購入していますか ?
   - BYOL にはどのようなバンドルタイプが必要ですか?
   - 同じ リージョンで BYOL が有効になっている他の AWS アカウントはありますか ? ある場合、同じ基盤となるハードウェアを使用するように、これらのアカウントをリンクしますか?

     アカウントがリンクされている場合、BYOL の適格性を判断するために、これらのアカウントに WorkSpaces デプロイされた の合計数が集計されます。これらの質問の両方に対する回答が「はい」の場合は、アカウントをリンクできます。 CreateAccountLinkInvitations や などの APIsを使用して AWS 、アカウントをAcceptAccountLinkInvitation接続できます。他の BYOL 対応アカウントをリンクしたいが、別の BYOL 設定 (CIDR 範囲とイメージ) を使用する場合は、 AWS サポートに連絡して BYOL の新しいアカウントを有効にします。

3. BYOL の適格性が確認されたら、次のステップに進み、Amazon WorkSpaces コンソールでアカウントの BYOL を有効にします。

ステップ 2: Amazon WorkSpaces コンソールを使用して BYOL のアカウントで BYOL を有効にする

アカウントの BYOL を有効にするには、管理ネットワークインターフェイスを指定する必要があります。このインターフェイスは安全な Amazon WorkSpaces 管理ネットワークに接続されています。これは、Amazon WorkSpaces クライアントへの WorkSpace デスクトップのインタラクティブストリーミング、および Amazon WorkSpaces が を管理できるようにするために使用されます WorkSpace。

> **Note**
>
> この手順をリージョン別に 1 回のみ実行することで、アカウントの BYOL を有効にできます。

Amazon WorkSpaces コンソールを使用してアカウントの BYOL を有効にするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインでアカウント設定 を選択し、自分のライセンスを使用 (BYOL) で WorkSpaces BYOL 設定を表示 を選択します。
3. [Account Settings] (アカウント設定) ページの [Bring Your Own License (BYOL)] で、[Enable BYOL] (BYOL の有効化) を選択します。

   [Enable BYOL] (BYOL の有効化) オプションが表示されない場合は、お客様のアカウントは現在 BYOL 適格ではありません。詳細については、「ステップ 1: Amazon WorkSpaces コンソールを使用して BYOL のアカウントの適格性を確認する」を参照してください。
4. [Bring Your Own License (BYOL)] の [管理ネットワークインターフェイス IP アドレス範囲] エリアで、IP アドレス範囲を選択し、[使用可能な CIDR ブロックを表示] を選択します。

   Amazon WorkSpaces は、使用可能な IP アドレス範囲を検索し、指定した範囲内の IPv4 クラスレスドメイン間ルーティング (CIDR) ブロックとして表示します。特定の IP アドレス範囲が必要な場合は、検索範囲を編集することができます。

   > **Important**
   >
   > IP アドレス範囲を指定すると、変更することはできません。内部ネットワークによって使用される範囲と競合しない IP アドレス範囲が指定されていることを確認します。指定する範囲について質問がある場合は、先に進む前に AWS アカウントマネージャーまたは販売担当者に問い合わせるか、 AWS Support センターにお問い合わせください。
5. 結果のリストから必要な CIDR ブロックを選択し、[BYOL を有効にする] を選択します。

   このプロセスには数時間かかることがあります。 WorkSpaces が BYOL のアカウントを有効にしている間、次のステップに進みます。

ステップ 3: Windows VM で BYOL Checker PowerShell スクリプトを実行する

アカウントの BYOL が有効になったら、VM が BYOL の要件を満たしていることを確認する必要があります。そのためには、以下の手順を実行して WorkSpaces BYOL Checker PowerShell スクリプトをダウンロードして実行します。このスクリプトでは、使用する VM 上で一連のテストを実行してイメージを作成します。

> **Important**
>
> BYOL で使用する前に、VM がすべてのテストにパスする必要があります。

BYOL Checker スクリプトをダウンロードするには

BYOL Checker スクリプトをダウンロードして実行する前に、Windows の最新セキュリティアップデートが VM にインストールされていることを確認してください。このスクリプトの実行中、Windows Update サービスは無効化されます。

1. BYOL Checker スクリプトの .zip ファイルを https://tools.amazonworkspaces.com/BYOLChecker.zip からDownloadsフォルダにダウンロードします。
2. Downloads フォルダに、BYOL フォルダを作成します。
3. BYOLChecker.zip からファイルを抽出し、Downloads\BYOL フォルダにコピーします。
4. Downloads\BYOLChecker.zip フォルダを削除して、抽出されたファイルのみが残るようにします。

以下のステップで、BYOL Checker スクリプトを実行します。

BYOL Checker スクリプトを実行するには

1. Windows デスクトップから Windows を開きます PowerShell。Windows 開始ボタンを選択し、Windows PowerShellを右クリックし、管理者として実行 を選択します。デバイスに変更 PowerShell を加えるかどうかを選択するようにユーザーアカウントコントロールから求められた場合は、はい を選択します。
2. PowerShell コマンドプロンプトで、BYOL Checker スクリプトがあるディレクトリに変更します。たとえば、スクリプトが Downloads\BYOL ディレクトリにある場合は、以下のコマンドを入力し、Enter キーを押します。

```
cd C:\Users\username\Downloads\BYOL
```

3. 次のコマンドを入力して、コンピュータ PowerShell の実行ポリシーを更新します。これにより、BYOL Checker スクリプトで以下を実行できるようになります。

```
Set-ExecutionPolicy AllSigned
```

4. PowerShell 実行ポリシーを変更するかどうかを確認するプロンプトが表示されたら、「はいA」と「すべて」と指定します。
5. 次のコマンドを入力して、BYOL Checker スクリプトを実行します。

```
.\BYOLChecker.ps1
```

6. セキュリティ通知が表示されたら、R キーを押して 1 回実行します。
7. WorkSpaces 画像検証ダイアログボックスで、テストの開始 を選択します。
8. 各テストが完了したら、テストのステータスを表示できます。いずれかのテストで [Failed (失敗)] ステータスが表示された場合は、[Info (情報)] を選択して、失敗の原因となった問題の解決方法に関する情報を表示します。いずれかのテストで [WARNING (警告)] ステータスが表示された場合は、[Fix All Warnings (すべての警告の修正)] ボタンを選択します。
9. 該当する場合は、テストのエラーや警告の原因となる問題を解消し、VM がすべてのテストにパスするまで Step 7 と Step 8 を繰り返します。VM をエクスポートする前に、エラーや警告はすべて解消する必要があります。
10. BYOL スクリプトチェッカーによって 2 種類のログファイル (`BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` および `ImageInfo.text`) が生成されます。これらのファイルは、BYOL Checker スクリプトファイルを含むディレクトリにあります。

> **Tip**
>
> これらのファイルを削除しないでください。問題が発生した場合、それらのファイルはトラブルシューティングに役立つことがあります。

11. VM がすべてのテストに合格すると、「Validation Successful (検証に成功しました)」というメッセージが表示されます。ツールに表示される VM のロケール設定を確認します。ロケール設定を更新するには、Microsoft ドキュメントのこちらの手順に従って、BYOL Checker スクリプトを再実行します。
12. VM をシャットダウンし、そのスナップショットを作成します。
13. 仮想マシンを再起動します。[Run Sysprep] を選択します。Sysprep が成功した場合、Step 12 の後にエクスポートした VM を Amazon Elastic Compute Cloud (Amazon EC2) にインポートで

きます。それ以外の場合は、Sysprep ログを確認し、Step 12 で作成したスナップショットにロールバックして、レポートされた問題を解決します。その後、新しいスナップショットを作成して、BYOL Checker スクリプトを再度実行します。

Sysprep が失敗する代表的な原因は、Modern Appx Packages が一部のユーザーにインストールされていないことです。Remove-AppxPackage PowerShell コマンドレットを使用して AppX パッケージを削除します。

14. イメージが正常に作成されたら、WorkSpaces_BYOL アカウントを削除できます。

エラーメッセージとエラー修正のリスト

BYOL のインポートには Powershell 4.0 以降が必要です。インストールされている のバージョン PowerShell はサポートされていません。

PowerShell バージョン 4.0 以降がインストールされている必要があります。詳細については、「Microsoft Windows PowerShell」を参照してください。

BYOL のインポートは、アクティブな Microsoft Office がインストールされているシステムをサポートしていません。

インポートする前に Microsoft Office をアンインストールする必要があります。詳細については、「PC から Office をアンインストールする」を参照してください。

BYOL のインポートには、PCoIP エージェントがないシステムが必要です。

PCoIP エージェントをアンインストールします。PCoIP エージェントのアンインストールについては、「Uninstalling the Teradici PCoIP Software Client for Mac」を参照してください。

BYOL のインポートには、Windows Update を無効にする必要があります。

次の手順に従って Windows Update を無効にします。

1. Windows キー + R キーを押します。`services.msc` を入力し、Enter を押します。
2. [Windows Update] を右クリックして、[プロパティ] を選択します。
3. [全般] タブの下で、[スタートアップのタイプ] を [無効] に設定します。
4. [Stop] (停止) を選択します。
5. [適用]、[OK] の順に選択します。
6. コンピュータを再起動します。

BYOL のインポートには、自動マウントが有効になっている必要があります。

自動マウントを有効にする必要があります。管理者として PowerShell で次のコマンドを実行します。

```
C:\> diskpart
DISKPART> automount enable
```

新しいボリュームの自動マウントが有効になります。

BYOL インポートでは、 WorkSpaces_BYOL アカウントを有効にする必要があります

WorkSpaces_BYOL アカウントを有効にする必要があります。詳細については、「Amazon WorkSpaces コンソール を使用して BYOL のアカウントで BYOL を有効にする」を参照してください。

BYOL のインポートでは、ネットワークインターフェイスが DHCP を使用して IP アドレスを自動的に割り当てる必要があります。ネットワークインターフェイスでは現在、固定 IP アドレスを使用しています。

DHCP を使用するには、ネットワークインターフェイスを変更する必要があります。詳細については、Change TCP/IP settings を参照してください。

BYOL のインポートには、ローカルディスクに 20 GB を超えるスペースが必要です。

ローカルディスクには十分なスペースが必要で、20 GB 以上解放する必要があります。

BYOL のインポートには、1 つのローカルドライブを搭載したシステムが必要です。他に、ローカルドライブ、リムーバブルドライブ、またはネットワークドライブがあります。

イメージのインポートに使用される には WorkSpace 、C および D ドライブのみ存在できます。仮想ドライブを含め他のすべてのドライブを削除します。

BYOL のインポートには、Windows 10 または Windows 11 が必要です。

Windows 10 または Windows 11 オペレーティングシステムを使用してください。

BYOL のインポートには、AD ドメインに参加していないシステムが必要です。

システムを AD ドメインから参加解除する必要があります。詳細については、Azure Active Directory device management FAQ を参照してください。

BYOL のインポートには、Azure ドメインに参加していないシステムが必要です。

システムを Azure ドメインから参加解除する必要があります。詳細については、Azure Active Directory device management FAQ を参照してください。

BYOL のインポートでは、Windows パブリックファイアウォールを無効にする必要があります。

パブリックファイアウォールプロファイルを無効にする必要があります。詳細については、「Microsoft Defender ファイアウォールを有効または無効にする」を参照してください。

BYOL のインポートには、VMware ツールがないシステムが必要です。

VMware ツールはアンインストールする必要があります。詳細については、「VMware Fusion での VMware Tools のアンインストールと手動インストール (1014522)」を参照してください。

BYOL のインポートでは、ローカルディスクが 80 GB 未満である必要があります。

ディスクは 80 GB より小さくなければなりません。ディスクサイズを縮小してください。

BYOL のインポートでは、ローカルドライブ上のパーティションが 2 つ未満である必要があります。さらに、Windows 10 のパーティションはすべて MBR パーティションで、Windows 11 のパーティションはすべて GPT でパーティション化されている必要があります。

ボリュームは Windows 10 の場合は MBR パーティション化され、Windows 11 の場合は GPT パーティション化されている必要があります。詳細については、「ディスクの管理」を参照してください。

BYOL インポートでは、再起動を必要とする保留中の更新がすべて完了している必要があります。

すべての更新プログラムをインストールし、オペレーティングシステムを再起動します。

BYOL インポートでは、 AutoLogon が無効になっている必要があります。

AutoLogon レジストリを無効にするには：

1. Windows キー + R を押して、コマンドプロンプトに `Regedit.exe` を入力します。
2. `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon` まで下にスクロールします。
3. `DontDisplayLastUserName` に値を追加します。
4. [タイプ] に `REG_SZ` を入力します。
5. [値] に「`0`」と入力します。

> **Note**
>
> - 値 DontDisplayLastUserName は、ログオンダイアログボックスに、PC に最後にログオンしたユーザーのユーザー名を表示するかどうかを決定します。
> - この値はデフォルトでは存在しません。存在する場合は、 に設定する必要があります。設定0しないと、 の値がDefaultUser消去され、失敗 AutoLogon します。

BYOL のインポートでは **RealTimeIsUniversal** が有効である必要があります。

RealTimeUniversal レジストリキーを有効にする必要があります。詳細については、「Windows Server 2008 以降の時刻設定の構成」を参照してください。

BYOL のインポートには、ブート可能なパーティションが 1 つあるシステムが必要です。

ブート可能なパーティションの数は 1 を超えてはなりません。

追加のパーティションを削除するには

1. Windows ロゴキー + R キーを押して、[実行] ボックスを開きます。msconfig を入力して、キーボードで Enter キーを押して [システム構成] ウィンドウを開きます。
2. ウィンドウから [ブート] タブを選択して、使用する OS が [現在の OS; デフォルト OS] に設定されているか確認してください。設定されていない場合は、ウィンドウから目的の OS を選択し、同じウィンドウで [デフォルトとして設定] を選択します。
3. 別のパーティションを削除するには、そのパーティションを選択し、[削除]、[適用]、[OK] の順に選択します。

それでもエラーが表示される場合は、インストールディスクまたは修復ディスクからコンピュータを起動し、次の手順に従います。

1. 最初の言語画面をスキップして、メインインストール画面で [コンピュータを修復する] を選択します。
2. [オプションを選択] 画面で、[トラブルシューティング] を選択します。
3. [詳細オプション] 画面で、[コマンドプロンプト] を選択します。
4. コマンドプロンプトで、bootrec.exe /fixmbr を入力し、Enter を押します。

BYOL のインポートには 64 ビットシステムが必要です。

64 ビット OS イメージを使用する必要があります。詳細については、「BYOL でサポートされる Windows のバージョン」を参照してください。

BYOL のインポートには、リアームされていないシステムが必要です。

イメージのリアームカウントが 0 であってはなりません。リアーム機能を使用すると、Windows の試用バージョンのアクティベーション期間を延長できます。イメージ作成プロセスでは、リアームカウントを 0 以外の値にする必要があります。

Windows リアームカウントを確認するには

1. Windows の [スタート] メニューで [Windows システム] を選択し、[コマンドプロンプト] を選択します。
2. コマンドプロンプトで、`cscript C:\Windows\System32\slmgr.vbs /dlv` を入力し、Enter を押します。
3. リアームカウントを 0 以外の値にリセットするには。詳細については、「Windows インストールに対する Sysprep (一般化) の実行」を参照してください。

BYOL のインポートには、インプレースアップグレードされていないシステムが必要です。このシステムはインプレースアップグレードされています。

Windows が以前のバージョンからアップグレードされていてはなりません。

BYOL のインポートでは、ウイルス対策がシステムにインストールされていないことが必要です。

ウイルス対策ソフトウェアをアンインストールする必要があります。BYOLChecker を実行して、アンインストールするウイルス対策ソフトウェアの詳細を取得します。

BYOL のインポートでは、Windows 10 システムにレガシーブートモードが必要です。

Windows 10 ではレガシー BIOS BootMode を使用する必要があります。詳細については、「ブートモード」を参照してください。

ステップ 4: VM を仮想化環境からエクスポートする

BYOL のイメージを作成するには、まず仮想化環境から VM をエクスポートします。VM は、最大サイズが 70 GB、空き容量が 10 GB 以上の 1 つのボリューム上にあることが必要です。詳細について

は、仮想化環境に関するドキュメント、およびVM Import/Export ユーザーガイドの VM をその仮想化環境からエクスポートするを参照してください。

Windows 11 では、Unified Extensible Firmware Interface (UEFI)、トラステッドプラットフォームモジュール (TPM) 2.0、およびセキュアブートのサポートに関する新しいハードウェア要件を設定しています。Windows 11 のインポートに固有の VM Import/Export は、Microsoft キーと NitroTPM を使用して UEFI セキュアブートを自動的に有効にします。詳細については、「VM Import/Export を使用した Windows 11 イメージ AWS の への取り込み」を参照してください。

ステップ 5: イメージとして VM を Amazon EC2 にインポートする

VM をエクスポートしたら、VM から Windows オペレーティングシステムをインポートするための要件を確認します。必要に応じてアクションを実行します。詳細については、VM Import/Export 要件を参照してください。

> **Note**
>
> 暗号化されたディスクを持つ VM のインポートはサポートされていません。Amazon Elastic Block Store (Amazon EBS) ボリュームのデフォルトの暗号化を選択した場合は、VM をインポートする前にこのオプションの選択を解除する必要があります。

Amazon マシンイメージ (AMI) として VM を Amazon EC2 にインポートします。次のいずれかの方法を使用します。

- AWS CLIで import-image コマンドを使用します。詳細については、AWS CLI コマンドリファレンスの import-image を参照してください。
- ImportImage API オペレーションを使用します。詳細については、Amazon EC2 API リファレンスImportImage」の「」を参照してください。

詳細については、VM Import/Export ユーザーガイドのイメージとして VM をインポートするを参照してください。

ステップ 6: WorkSpaces コンソールを使用して BYOL イメージを作成する

WorkSpaces BYOL イメージを作成するには、以下の手順を実行します。

> **Note**
>
> この手順を実行するには、 AWS Identity and Access Management 以下の (IAM) アクセス許可があることを確認します。
>
> - を呼び出します WorkSpaces **`ImportWorkspaceImage`**。
> - BYOL イメージの作成に使用する Amazon EC2 イメージでの AmazonEC2 **`DescribeImages`** の呼び出し。
> - BYOL イメージの作成に使用する Amazon EC2 イメージでの AmazonEC2 **`ModifyImageAttribute`** の呼び出し。Amazon EC2 イメージの起動のためのアクセス許可が制限されていないことを確認します。イメージは、BYOL イメージ作成プロセスを通じて共有可能である必要があります。
>
> BYOL に固有の IAM ポリシーの例については WorkSpaces、「」を参照してくださいWorkSpaces の Identity and Access Management。IAM アクセス許可の使用の詳細については、IAM ユーザーガイドの IAM ユーザーのアクセス許可の変更を参照してください。イメージから Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または GraphicsPro バンドルを作成するには、 AWS Support センターに連絡してアカウントを許可リストに追加してもらいます。アカウントが許可リストに登録されたら、 import-workspace-image コマンドを使用して AWS CLI Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または GraphicsPro Image を取り込むことができます。詳細については、 AWS CLI コマンドリファレンスの import-workspace-image を参照してください。

Windows VM からイメージを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. [Create BYOL image] (BYOL イメージの作成) を選択します。
4. [Create BYOL image] (BYOL イメージの作成) ページで、次の操作を行います。
   - [AMI ID] で、EC2 コンソールへのリンクをクリックし、前のセクション (ステップ 5: イメージとして VM を Amazon EC2 にインポートする) の説明に従ってインポートした Amazon EC2 イメージを選択します。イメージ名は `ami-` で始まり、AMI の識別子が続いている必要があります (例: `ami-1234567e`)。
   - [Image name] (イメージ名) で、イメージの一意の名前を入力します。

- [Description] (説明) で、イメージをすばやく識別できるような説明を入力します。
- インスタンスタイプ で、PCoIP または WorkSpaces ストリーミングプロトコル (WSPGraphicsPro) のいずれかのイメージに使用するプロトコルに応じて、適切なバンドルタイプ (通常の 、Graphics.g4dn 、Graphics 、または) を選択します。 GraphicsPro.g4dn バンドルを作成する場合は、Graphics.g4dn を選択します。GPU 対応ではないバンドル (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または 以外のバンドル GraphicsPro) の場合は、通常の を選択します。

  > **Note**
  >
  > - 現時点では、Graphics.g4dn、 GraphicsPro.g4dn、Graphics、 GraphicsPro イメージは PCoIP プロトコルに対してのみ作成できます。
  > - Windows 11 イメージは WSP プロトコルのためにのみ作成できます。
  > - Graphics.g4dn および GraphicsPro.g4dn バンドルは現在 Windows 11 では使用できません。
  > - Windows 11 では、グラフィックスと GraphicsPro イメージはサポートされていません。

- (オプション) [Select applications] (アプリケーションの選択) で、購読する Microsoft Office のバージョンを選択します。詳細については、「BYOL イメージに Microsoft Office を追加する」を参照してください。
- (オプション) [Tags] (タグ) で、[Add new tag] (新しいタグの追加) を選択して、このイメージにタグを関連付けます。詳細については、「WorkSpaces のリソースにタグを付ける」を参照してください。

5. [Create BYOL image] (BYOL イメージの作成) を選択します。

   イメージの作成中、イメージのステータスは、コンソールの [Images] (イメージ) ページで [Pending] (保留中) と表示されます。BYOL の取り込みプロセスには、最低 90 分かかります。Office にもサブスクライブしている場合は、プロセスに最低 3 時間かかります。

   イメージの検証が成功しない場合は、エラーコードがコンソールに表示されます。イメージの作成が完了すると、ステータスは [Available] に変わります。

ステップ 7: BYOL イメージからカスタムバンドルを作成する

BYOL イメージが作成されたら、イメージを使用してカスタムバンドルを作成できます。詳細については、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。

ステップ 8: の専用ディレクトリを登録する WorkSpaces

に BYOL イメージを使用するには WorkSpaces、この目的のためにディレクトリを登録する必要があります。

のディレクトリを登録するには WorkSpaces

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択後、[アクション]、[登録] の順に選択します。
4. ディレクトリの登録ダイアログボックスで、専有 を有効にする WorkSpaces で、はい を選択します。
5. [登録] を選択します。

専用ハードウェアで実行 WorkSpaces されていない の AWS Managed Microsoft AD ディレクトリまたは AD Connector ディレクトリを既に登録している場合は、この目的のために新しい AWS Managed Microsoft AD ディレクトリまたは AD Connector ディレクトリを設定できます。ディレクトリを登録解除し、専用 のディレクトリとして再登録することもできます WorkSpaces。そのためには、以下の手順を実行します。

> **Note**
>
> この手順は、 ディレクトリに関連付けられ WorkSpaces ていない場合にのみ実行できます。

ディレクトリを登録解除して専用に再登録するには WorkSpaces

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. 既存の を終了します WorkSpaces。
3. ナビゲーションペインで [Directories] を選択します。
4. ディレクトリを選択し、[Actions]、[Deregister] の順に選択します。

5. 確認を求めるメッセージが表示されたら、[Deregister] を選択します。
6. ディレクトリを再度選択後、[アクション]、[登録] の順に選択します。
7. ディレクトリの登録ダイアログボックスで、専有 を有効にする WorkSpaces で、はい を選択します。
8. [登録] を選択します。

ステップ 9: BYOL を起動する WorkSpaces

専用 のディレクトリを登録したら WorkSpaces、このディレクトリ WorkSpaces で BYOL を起動できます。を起動する方法については、 WorkSpaces「」を参照してくださいWorkSpaces を使用して仮想デスクトップを起動します。。

BYOL アカウントをリンクする

BYOL リンクを使用してアカウントをリンクし、BYOL 設定を共有できます。BYOL 設定には、 アカウントで使用される CIDR 範囲と、Windows ライセンス WorkSpaces での作成に使用するイメージが含まれます。リンクされているすべてのアカウントは、同じ基盤となるハードウェアインフラストラクチャを共有します。

BYOL リンクが有効になっているアカウントは、基盤となるハードウェアインフラストラクチャのプライマリ所有者であり、ソースアカウントと呼ばれます。ソースアカウントは、基盤となるハードウェアインフラストラクチャへのアクセスを管理します。ターゲットアカウントは、ソースアカウントにリンクされているアカウントです。

> **Important**
>
> BYOL アカウントリンクの APIs は、現在 では使用できません AWS GovCloud (US) Region。

> **Note**
>
> リンクする AWS アカウントは、組織の一部であり、同じ支払者アカウントに属する必要があります。同じリージョン内のアカウントのみをリンクできます。

ソースアカウントとターゲットアカウントをリンクするには

1. CreateAccountLinkInvitation API を使用して、ソースアカウントからターゲットアカウントに招待リンクを送信します。
2. AcceptAccountLinkInvitation API を使用して、ターゲットアカウントからの保留中のリンクを受け入れます。
3. GetAccountLink または ListAccountLinks API を使用して、リンクが確立されていることを確認します。

のモニタリング WorkSpaces

次の機能を使用して をモニタリングできます WorkSpaces。

CloudWatch メトリクス

Amazon は、 CloudWatch に関するデータポイントを Amazon に WorkSpaces 公開します WorkSpaces。 CloudWatch では、これらのデータポイントに関する統計情報を、メトリクス と呼ばれる時系列データの順序付けられたセットとして取得できます。これらのメトリクスを使用して、 WorkSpaces が期待どおりに動作していることを確認できます。詳細については、「CloudWatch メトリクス WorkSpaces を使用して をモニタリングする」を参照してください。

CloudWatch イベント

ユーザーが にログインすると、Amazon WorkSpaces は Amazon CloudWatch Events にイベントを送信できます WorkSpace。その結果、イベント発生時に応答できるようになります。詳細については、「Amazon WorkSpaces ンを利用してモニタリングする EventBridge」を参照してください。

CloudTrail ログ

AWS CloudTrail は、 WorkSpaces のユーザー、ロール、または AWS のサービスによって実行されたアクションのレコードを提供します。で収集された情報を使用して CloudTrail、 に対するリクエスト WorkSpaces、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「 を使用した API コールのログ記録 WorkSpaces」を参照してください CloudTrail。 は、スマートカードユーザーの成功したサインインイベントと失敗したサインインイベントをAWS CloudTrailログに記録します。詳細については、「スマートカードユーザーの AWS サインインイベントを理解する」を参照してください。

CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor は、 でホストされているアプリケーションとエンドユーザー間のインターネットの問題がパフォーマンスAWSと可用性にどのように影響するかを可視化します。 CloudWatch Internet Monitor を使用して以下を行うこともできます。

- 1 つ以上の WorkSpace ディレクトリのモニターを作成します。
- インターネットのパフォーマンスをモニタリングする。
- エンドユーザーの都市ネットワーク間の場所や ASN、通常はインターネットサービスプロバイダー (ISP) とその WorkSpace リージョンなどの問題に対するアラームを取得します。

Internet Monitor では、AWS のグローバルネットワークのフットプリントから接続データを取得します。そして、インターネット向けトラフィックのパフォーマンスと可用性に関するベースラインの計算に使用します。現在のところ、Internet Monitor は個々のエンドユーザーにインターネットパフォーマンスを提供することはできませんが、都市レベルや ISP レベルでは提供できます。

CloudWatch 自動ダッシュボードを使用して WorkSpaces ヘルスをモニタリングする

CloudWatch 自動ダッシュボード WorkSpaces を使用して をモニタリングすることで、raw データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。メトリクスは、履歴情報にアクセスし、ウェブアプリケーションまたはサービスのパフォーマンスをモニタリングするために 15 か月間保持されます。また、特定のしきい値をモニタリングするアラームを設定し、しきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

AWS アカウントを使用して を設定すると、 CloudWatch ダッシュボードが自動的に作成されます WorkSpaces。ダッシュボードでは、リージョン全体でヘルスやパフォーマンスなどの WorkSpaces メトリクスをモニタリングできます。ダッシュボードは以下の目的にも使用できます。

- 異常な WorkSpace インスタンスを特定します。
- 異常な WorkSpace インスタンスがある実行モード、プロトコル、オペレーティングシステムを特定します。
- 時間の経過に伴う重要なリソース使用率を表示します。
- トラブルシューティングに役立つ異常を特定します。

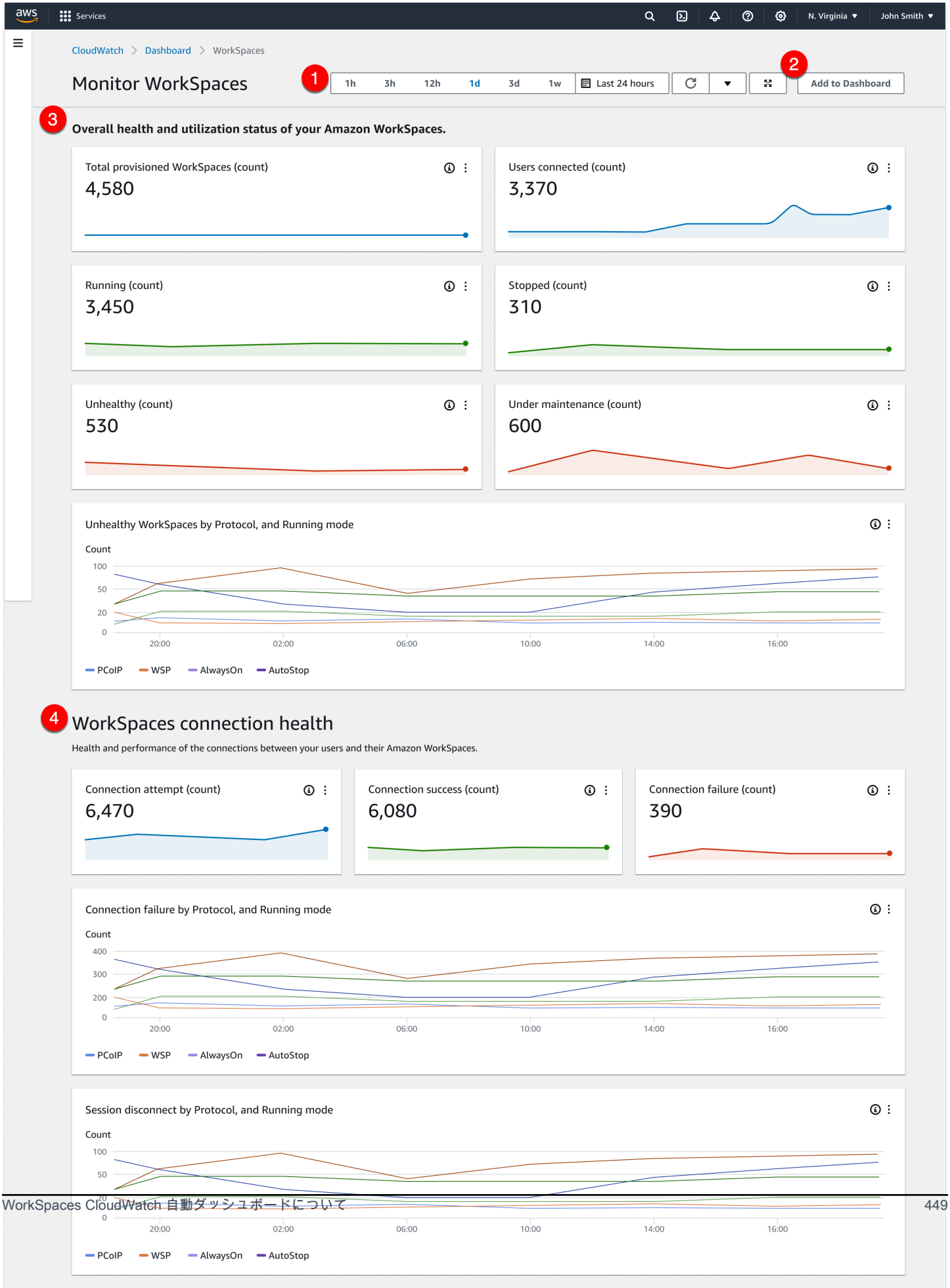
WorkSpaces CloudWatch 自動ダッシュボードは、すべてのAWS商用リージョンで利用できます。

WorkSpaces CloudWatch 自動ダッシュボードを使用するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、ダッシュボードを選択します。
3. 自動ダッシュボードタブを選択します。
4. を選択しますWorkSpaces。

WorkSpaces CloudWatch 自動ダッシュボードについて

CloudWatch 自動ダッシュボードを使用すると、 WorkSpaces リソースのパフォーマンスを把握し、パフォーマンスの問題を特定できます。


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

ダッシュボードは以下の機能で構成されています。

1. 時間範囲と日付範囲の制御を使用して履歴データを表示します。
2. カスタマイズされたダッシュボードビューを CloudWatch カスタムダッシュボードに追加します。
3. 次の操作 WorkSpaces を実行して、 の全体的なヘルスと使用状況をモニタリングします。

    a. プロビジョニングされた の総数 WorkSpaces、接続されているユーザーの数、異常および正常な WorkSpace インスタンスの数を表示します。

    b. プロトコル WorkSpaces やコンピューティングモードなど、異常のある変数やさまざまな変数を表示します。

    c. 折れ線グラフにカーソルを合わせると、特定のプロトコルと実行モードの正常または異常な WorkSpace インスタンスの数を一定期間表示します。

    d. 省略記号メニューを選択し、メトリクスの表示を選択してタイムスケールチャートにメトリクスを表示します。
4. 接続メトリクスと、接続試行回数、成功した接続、失敗した接続など、特定の時点で WorkSpaces の環境内のさまざまな変数を表示します。
5. ラウンドトリップタイム (RTT) など、ユーザーエクスペリエンスに影響する InSession レイテンシーを表示して、ネットワークの状態をモニタリングするための接続状態とパケット損失を判断します。
6. ホストのパフォーマンスとリソースの使用率を表示して、潜在的なパフォーマンスの問題を特定してトラブルシューティングします。

CloudWatch メトリクス WorkSpaces を使用して をモニタリングする

WorkSpaces と Amazon CloudWatch は統合されているため、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、 CloudWatch コマンドラインインターフェイス、または CloudWatch API を使用してプログラムでモニタリングできます。 CloudWatch また、 では、メトリクスの指定されたしきい値に達したときにアラームを設定することもできます。

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

前提条件

CloudWatch メトリクスを取得するには、us-east-1 リージョンのAMAZONサブセットでポート 443 へのアクセスを有効にします。詳細については、「の IP アドレスとポートの要件 WorkSpaces」を参照してください。

内容

WorkSpaces メトリクス

AWS/WorkSpaces 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
Available [1]	正常なステータスを返した WorkSpaces の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
Unhealthy [1]	異常なステータスを返した WorkSpaces の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
		UserName		
ConnectionAttempt [2]	接続試行の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
ConnectionSuccess [2]	成功した接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
ConnectionFailure [2]	失敗した接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
SessionLaunchTime [2、6]	WorkSpaces セッションの開始にかかる時間。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	秒 (時間)
InSession Latency [2、6]	WorkSpaces クライアントと の間の往復時間 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	ミリ秒 (時間)

メトリクス	説明	ディメンション	統計	単位
SessionDisconnect [2、6]	ユーザーが開始して失敗した接続を含む、閉じられた接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
UserConnected [3]	ユーザーが接続 WorkSpaces されている の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
Stopped	停止 WorkSpaces されている の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
Maintenance [4]	メンテナンス WorkSpaces 中の の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
TrustedDeviceValidationAttempt [5、6]	デバイス認証シグニチャ検証の試行回数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	カウント
TrustedDeviceValidationSuccess [5、6]	成功したデバイス認証シグニチャ検証の数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	カウント
TrustedDeviceValidationFailure [5、6]	失敗したデバイス認証シグニチャ検証の数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	カウント
TrustedDeviceCertificateDaysBeforeExpiration [6]	ディレクトリに関連付けられたルート証明書の有効期限が切れるまでの日数。	CertificateId	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
CPUUsage	使用されている CPU リソースの割合。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小	割合 (%)
MemoryUsage	使用されているマシンメモリの割合。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小	割合 (%)
RootVolumeDiskUsage	使用されているルートディスクボリュームの割合。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小	割合 (%)

メトリクス	説明	ディメンション	統計	単位
UserVolumeDiskUsage	使用されているユーザーディスクボリュームの割合。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小	割合 (%)
UDPPacketLossRate [7]	クライアントとゲートウェイの間でドロップされたパケットの割合。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小、データサンプル	割合 (%)
UpTime	の前回の再起動からの時間 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均、最大、最小、データサンプル	[秒]

[1] WorkSpaces はステータスリクエストを に定期的に送信します WorkSpace。 WorkSpace は、これらのリクエストに応答Availableしたとき、およびこれらのリクエストに応答できなかったUnhealthyときにマークされます。これらのメトリクスは、粒度WorkSpace レベルごとに使用でき、組織 WorkSpaces 内のすべての に対して集計されます。

[2] WorkSpaces 各 に対して行われた接続に関するメトリクスを記録します WorkSpace。これらのメトリクスは、ユーザーが WorkSpaces クライアント経由で正常に認証され、クライアントがセッションを開始した後に出力されます。メトリクスは粒度WorkSpace レベルごとに使用でき、ディレクトリ WorkSpaces 内のすべての に対して集計されます。

[3] WorkSpaces は、接続ステータスリクエストを に定期的に送信します WorkSpace。ユーザーは、能動的にセッションを使用している場合、接続済みとしてレポートされます。このメトリクスは、粒度WorkSpace レベルごとに使用でき、組織 WorkSpaces 内のすべての に対して集計されます。

[4] このメトリクス WorkSpaces は、 AutoStop 実行モードで設定された に適用されます。のメンテナンスが有効になっている場合 WorkSpaces、このメトリクス WorkSpaces は、現在メンテナンス中の の数をキャプチャします。このメトリクスは、 がメンテナンス WorkSpace を開始したタイミングと削除されたタイミングを記述する、粒度WorkSpace レベルごとに使用できます。

[5] ディレクトリで信頼されたデバイス機能が有効になっている場合、Amazon は証明書ベースの認証 WorkSpaces を使用して、デバイスが信頼されているかどうかを判断します。ユーザーが にアクセスしようとすると WorkSpaces、信頼されたデバイス認証が成功または失敗したことを示すために、これらのメトリクスが発行されます。これらのメトリクスは、Amazon WorkSpaces Windows および macOS クライアントアプリケーションに対してのみ、ディレクトリごとの粒度レベルで使用できます。

[6] WorkSpaces Web Access では使用できません。

[7] このメトリクスは、平均パケット損失を測定します。

- PCoIP の場合: クライアントからのゲートウェイの平均パケット損失を測定します。
- WSP の場合: クライアントからゲートウェイへの平均パケット損失を測定します。

WorkSpaces メトリクスのディメンション

メトリクスデータをフィルタリングするために以下のディメンションを使用します。

ディメンション	説明
DirectoryId	指定されたディレクトリの にメトリクスデータをフィルタリング WorkSpaces します。ディレクトリ ID の形式は d-XXXXXXXXXX です。
WorkspaceId	指定された にメトリクスデータをフィルタリングします WorkSpace。 WorkSpace ID の形式は ですws-XXXXXXXXXX 。
CertificateId	メトリクスデータをフィルタリングして、ディレクトリに関連付けられている指定されたルート証明書にします。証明書 ID の形式は wsc-XXXXXXXXX です。
RunningMode	メトリクスデータを実行モードで にフィルタリング WorkSpaces します。実行モードの形式は AutoStop または です AlwaysOn。
BundleId	プロトコル WorkSpaces によってメトリクスデータを にフィルタリングします。バンドルの形式は ですwsb-XXXXXXXXXX 。
ComputeType	コンピューティングタイプ WorkSpaces でメトリクスデータを にフィルタリングします。
Protocol	プロトコルタイプ WorkSpaces でメトリクスデータを にフィルタリングします。
UserName	ユーザー名 WorkSpaces でメトリクスデータを にフィルタリングします。

モニタリングの例

次の例は、 を使用して CloudWatch アラームに AWS CLI 応答し、ディレクトリ WorkSpaces 内のどの で接続障害が発生したかを判断する方法を示しています。

CloudWatch アラームに応答するには

1. describe-alarms コマンドを使用して、アラームの対象になっているディレクトリを特定します。

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. describe-workspaces コマンドを使用して WorkSpaces 、指定されたディレクトリ内の のリストを取得します。

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
```

```
    }
  ]
}
```

3. get-metric-statistics コマンドを使用して、ディレクトリ WorkSpace 内の各 の CloudWatch メトリクスを取得します。 https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Amazon WorkSpaces ンを利用してモニタリングする EventBridge

Amazon WorkSpaces からのイベントを使用して、閲覧、検索、ダウンロード、アーカイブ、分析を行い、ログインに成功した場合の対応を行うことができます。 WorkSpacesたとえば、次の目的でイベントを使用できます。

- future WorkSpaces 参照できるようにログインイベントをログとして保存またはアーカイブし、ログを分析してパターンを探し、それらのパターンに基づいてアクションを実行します。

- WAN IP アドレスを使用してユーザーがどこからログインしているかを判断し、次にポリシーを使用して、イベントタイプの「」 WorkSpaces `WorkSpaces Access` に記載されているアクセス条件を満たすファイルまたはデータへのアクセスのみをユーザーに許可します。
- を使用してログインデータを分析し、自動アクションを実行します AWS Lambda。
- ポリシー制御を使用して、権限のない IP アドレスからのファイルやアプリケーションへのアクセスをブロックします。
- WorkSpaces 接続に使用したクライアントのバージョンを調べてください WorkSpaces。

Amazon WorkSpaces はこれらのイベントをベストエフォート方式で配信します。 EventBridge イベントはほぼリアルタイムで配信されます。を使用すると EventBridge、イベントに応じてプログラムによるアクションをトリガーするルールを作成できます。例えば、SNS トピックを呼び出して E メール通知を送信するルールや、Lambda 関数を呼び出して何らかのアクションを実行するルールを設定できます。詳細については、Amazon EventBridge ユーザーガイドを参照してください。

WorkSpaces アクセスイベント

WorkSpaces クライアントアプリケーションは、`WorkSpaces Access` WorkSpaceユーザがに正常にログインするとイベントを送信します。 WorkSpaces すべてのクライアントがこれらのイベントを送信します。

WorkSpaces ストリーミングプロトコル (WSP) WorkSpaces を使用して発生するイベントには、WorkSpaces クライアントアプリケーションのバージョン 4.0.1 以降が必要です。

イベントは、JSON オブジェクトとして表されます。以下は `WorkSpaces Access` イベントのサンプルデータです。

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
```

```
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

イベント固有のフィールド

`clientIpAddress`

クライアントアプリケーションの WAN IP アドレス。PCoIP ゼロクライアントの場合は、Teradici auth クライアントの IP アドレスを表します。

`actionType`

この値は常に `successfulLogin` です。

`workspacesClientProductName`

次の値では大文字と小文字が区別されます。

- `WorkSpaces Desktop client` Windows、MacOS、Linux クライアント
- `Amazon WorkSpaces Mobile client` iOS クライアント
- `WorkSpaces Mobile Client` Android クライアント
- `WorkSpaces Chrome Client` Chromebook クライアント
- `WorkSpacesWebClient` Web Access クライアント
- `AmazonWorkSpacesThinClient`— Amazon WorkSpaces シンクライアントデバイス
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` ゼロクライアント

`loginTime`

ユーザがにログインした時刻 WorkSpace。

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`

- OSX
- Windows
- Teradici PCoIP Zero Client and Tera2
- Web

`directoryId`

のディレクトリの識別子 WorkSpace。domain/ にはディレクトリ識別子を前置する必要があります。たとえば、"domain/d-123456789" と指定します。

`clientVersion`

接続に使用したクライアントバージョン WorkSpaces。

`workspaceId`

WorkSpace の識別子。

WorkSpaces イベントを処理するルールを作成します。

以下の手順に従って、 WorkSpaces イベントを処理するルールを作成します。

前提条件

E メール通知を受信するには、Amazon Simple Notification Service トピックを作成します。

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. [Create topic] (トピックの作成) を選択します。
4. [Type (タイプ)] で、[Standard (標準)] を選択します。
5. [Name] (名前) で、トピックの名前を入力します。
6. [Create topic] (トピックの作成) を選択します。
7. [サブスクリプションを作成] を選択します。
8. [Protocol (プロトコル)] として [Email (E メール)] を選択します。
9. [Endpoint] (エンドポイント) で、通知を受信するメールアドレスを入力します。
10. [サブスクリプションを作成] を選択します。
11. 次の件名の E メールメッセージが届きます: AWS Notification - Subscription Confirmation。指示に沿って操作し、登録を確認します。

WorkSpaces イベントを処理するルールを作成するには

1. https://console.aws.amazon.com/events/ で Amazon EventBridge コンソールを開きます。
2. [ルールの作成] を選択します。
3. [Name] (名前) に、ルールの名前を入力します。
4. ルールタイプ では、イベントパターンを持つルール] を選択します。
5. 次へ をクリックします。
6. [Event pattern] (イベントパターン) の場合は、次のいずれかを実行します。
   a. イベントソース で AWS のサービス を選択します。
   b. についてはAWS のサービス、を選択しますWorkSpaces。
   c. [イベントタイプ] で [WorkSpacesアクセス] を選択します。
   d. デフォルトでは、すべてのイベントに通知が送信されます。必要に応じて、特定のクライアントまたはワークスペースのイベントをフィルタリングするイベントパターンを作成できます。
7. [次へ] を選択します。
8. 次のようにターゲットを指定します。
   a. [Target types] (ターゲットタイプ) には、[AWS のサービス] を選択します。
   b. [Select a target] (ターゲットの選択) には、[SNS topic] (SNS トピック) を選択します。
   c. [トピック] で、通知用に作成した SNS トピックを選択します。
9. [次へ] を選択します。
10. (オプション) ルールにタグを追加します。
11. [次へ] を選択します。
12. [Create rule] (ルールの作成) を選択します。

スマートカードユーザーの AWS サインインイベントを理解する

AWS CloudTrail は、スマートカードユーザーの成功したサインインイベントと失敗したサインインイベントを記録します。これには、ユーザーが特定の資格情報のチャレンジや要素を解決するよう求められるたびにキャプチャされるサインインイベントに加えて、その特定の認証情報の検証リクエストのステータスが含まれます。必要な認証情報のチャレンジをすべて完了したユーザーだけがサインインを許可され、`UserAuthentication` イベントがログに記録されます。

次の表は、サインインの CloudTrail イベント名とその目的を示します。

イベント名	イベントの目的
CredentialChallenge	ユーザーは AWS サインインで特定の認証情報のチャレンジを解決するように要求されたことを示し、必要な CredentialType (スマートカードなど) を指定します。
CredentialVerification	ユーザーが特定の CredentialChallenge リクエストの解決を試みたことを通知し、その認証情報が成功したか失敗したかを指定します。
UserAuthentication	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知します。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、UserAuthentication イベントはログに記録されません。

次の表は、特定のサインイン CloudTrail イベント内に含まれる追加の有用なイベントデータフィールドを示します。

イベント名	イベントの目的	サインインイベントの適用性	値の例
AuthWorkflowID	サインインシーケンス全体で発生するすべてのイベントを相関させます。各ユーザーサインインで、AWS サインインによって複数のイベントが送信されることがあります。	CredentialChallenge , CredentialVerification , UserAuthentication	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
CredentialType	ユーザーが特定の CredentialChallenge リクエストの解決を試みたことを通知し、その認証情報が成功したか失敗したかを指定します。	CredentialChallenge , CredentialVerification , UserAuthentication	CredentialType": "SMARTCARD" (possible values today: SMARTCARD)

イベント名	イベントの目的	サインインイベントの適用性	値の例
LoginTo	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知します。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、UserAuthentication イベントは口グに記録されません。	UserAuthentication	"LoginTo": "https://skylight.local“

AWS サインインシナリオのイベント例

以下の例は、さまざまなサインインシナリオで予想される CloudTrail イベントのシーケンスを示します。

目次

スマートカードを使用した認証での正常なサインイン

次の一連のイベントは、正常に完了したスマートカードサインインの例を示します。

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
```

```
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```


正常に完了した CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
```

```
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

正常に完了した UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

スマートカードを使用した認証での失敗したサインイン

次の一連のイベントは、正常に完了しなかったスマートカードサインインの例を示します。

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

失敗した CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
```

```
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Amazon のビジネス継続性 WorkSpaces

Amazon WorkSpaces は、 AWSリージョンとアベイラビリティーゾーンに整理された AWS グローバルインフラストラクチャ上に構築されています。これらのリージョンとアベイラビリティーゾーンは、物理的な分離とデータの冗長性の両方の観点から回復力を提供します。詳細については、「Amazon WorkSpaces の耐障害性」を参照してください。

Amazon は、ドメインネームシステム (DNS) ルーティングポリシーと連携して、プライマリが利用できない WorkSpaces 場合に WorkSpaces ユーザーを別の にリダイレクトする機能 WorkSpaces であるクロスリージョンリダイレクト WorkSpaces も提供します。例えば、DNS フェイルオーバールーティングポリシーを使用すると、プライマリリージョン WorkSpaces の にアクセスできないときに、指定したフェイルオーバーリージョンの WorkSpaces にユーザーを接続できます。

リージョン間リダイレクトを使用すると、リージョンの復元性と高可用性を実現できます。また、トラフィックの分散やメンテナンス WorkSpaces 期間中の代替手段の提供など、他の目的でも使用できます。DNS 設定に Amazon Route 53 を使用する場合は、Amazon CloudWatch アラームをモニタリングするヘルスチェックを利用できます。

Amazon WorkSpaces マルチリージョンレジリエンスは、セカンダリ WorkSpace リージョンに自動的で冗長な仮想デスクトップインフラストラクチャを提供し、停止によりプライマリリージョンに到達できない場合にユーザーをセカンダリリージョンにリダイレクトするプロセスを効率化します。

マルチ WorkSpaces リージョンレジリエンスとクロスリージョンリダイレクトを使用して、冗長仮想デスクトップインフラストラクチャをセカンダリ WorkSpace リージョンにデプロイし、破壊的なイベントに備えてクロスリージョンフェイルオーバー戦略を設計できます。このソリューションは、トラフィックの分散やメンテナンス WorkSpaces 期間中の代替手段の提供など、他の目的にも使用できます。DNS 設定に Route 53 を使用する場合は、 CloudWatch アラームをモニタリングするヘルスチェックを利用できます。

内容

- Amazon のクロスリージョンリダイレクト WorkSpaces
- Amazon のマルチリージョンレジリエンス WorkSpaces

Amazon のクロスリージョンリダイレクト WorkSpaces

Amazon のクロスリージョンリダイレクト機能を使用すると WorkSpaces、 の登録コードとして完全修飾ドメイン名 (FQDN) を使用できます WorkSpaces。クロスリージョンリダイレクトは、ドメイ

ンネームシステム (DNS) ルーティングポリシーと連携して、プライマリ WorkSpaces が利用できない WorkSpaces 場合に WorkSpaces ユーザーを別の にリダイレクトします。例えば、DNS フェイルオーバールーティングポリシーを使用すると、プライマリAWSリージョン WorkSpaces の にアクセスできないときに、指定したフェイルオーバーリージョンの WorkSpaces にユーザーを接続できます。

リージョン間のリダイレクトを DNS フェイルオーバールーティングポリシーとともに使用して、リージョンの耐障害性と高可用性を実現できます。この機能は、トラフィックの分散やメンテナンス WorkSpaces 期間中の代替手段の提供など、他の目的でも使用できます。DNS 設定に Amazon Route 53 を使用する場合は、Amazon CloudWatch アラームをモニタリングするヘルスチェックを利用できます。

この機能を使用するには、2 つ (またはそれ以上) のAWSリージョンでユーザー WorkSpaces 用に を設定する必要があります。また、接続エイリアスと呼ばれる特別な FQDN ベースの登録コードを作成する必要があります。これらの接続エイリアスは、 WorkSpaces ユーザーのリージョン固有の登録コードを置き換えます。(リージョン固有の登録コードは有効なままです。ただし、リージョン間リダイレクトが機能するためには、ユーザーは登録コードとして代わりに FQDN を使用する必要があります)。

接続エイリアスを作成するには、`www.example.com` または `desktop.example.com` などの FQDN である接続文字列を指定します。このドメインをクロスリージョンリダイレクトで使用するには、ドメインレジストラに登録し、ドメインの DNS サービスを構成する必要があります。

接続エイリアスを作成したら、それらを異なるリージョンの WorkSpaces ディレクトリに関連付けて、関連付けペア を作成します。関連付けペアごとに、プライマリリージョンと 1 つ以上のフェイルオーバーリージョンがあります。プライマリリージョンで停止が発生した場合、DNS フェイルオーバールーティングポリシーは、フェイルオーバーリージョンで WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。

プライマリリージョンとフェイルオーバーリージョンを指定するには、DNS フェイルオーバールーティングポリシーを設定するときに、リージョンの優先順位 (プライマリまたはセカンダリ) を定義します。

内容

前提条件

- 接続エイリアスで FQDN として使用するドメインを所有し、登録する必要があります。別のドメインレジストラをまだ使用していない場合は、Amazon Route 53 を使用してドメインを登録できます。詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 を使用したドメイン名の登録を参照してください。

> **Important**
>
> Amazon と組み合わせて使用するドメイン名を使用するには、必要なすべての権限が必要です WorkSpaces。お客様は、ドメイン名が第三者の法的権利を侵害または侵害しないこと、または適用法に違反しないことに同意するものとします。

ドメイン名の長さの合計は 255 文字を超えることはできません。ドメイン名の詳細については、Amazon Route 53 デベロッパーガイドの DNS ドメイン名の形式を参照してください。

クロスリージョンリダイレクトは、パブリックドメイン名とプライベート DNS ゾーンのドメイン名の両方で機能します。プライベート DNS ゾーンを使用している場合は、 を含む仮想プライベートクラウド (VPC) への仮想プライベートネットワーク (VPN) 接続を提供する必要がありますWorkSpaces。 WorkSpaces ユーザーがパブリックインターネットからプライベート FQDN を使用しようとすると、 WorkSpaces クライアントアプリケーションは次のエラーメッセージを返します。

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- DNS サービスをセットアップし、必要な DNS ルーティングポリシーを設定する必要があります。クロスリージョンリダイレクトは、DNS ルーティングポリシーと組み合わせて動作し、必要に応じて WorkSpaces ユーザーをリダイレクトします。
- クロスリージョンリダイレクトを設定するプライマリリージョンとフェイルオーバーリージョンごとに、ユーザー WorkSpaces 用に を作成します。各リージョンの各 WorkSpaces ディレクトリで、必ず同じユーザー名を使用してください。Active Directory ユーザーデータを同期させるには、AD Connector を使用して、ユーザー WorkSpaces 用に設定した各リージョンで同じ Active Directory を指すことをお勧めします。の作成の詳細については WorkSpaces、「 の起動 WorkSpaces」を参照してください。

> **Important**
>
> マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを Amazon で使用するために登録できます WorkSpaces。Amazon で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗 WorkSpaces します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用はサポートされていません。

クロスリージョンリダイレクトの設定が完了したら、 WorkSpaces ユーザーがプライマリリージョンのリージョンベースの登録コード (などWSpdx+ABC12D) ではなく FQDN ベースの登録コードを使用していることを確認する必要があります。これを行うには、ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する の手順を使用して、FQDN 接続文字列を含む E メールを送信する必要があります。

> **Note**
>
> Active Directory でユーザーを作成するのではなく、 WorkSpaces コンソールでユーザーを作成すると、新しい を起動するたびに、 によってリージョンベースの登録コードが記載された招待メールがユーザー WorkSpaces に自動的に送信されます WorkSpace。つまり、フェイルオーバーリージョンのユーザー WorkSpaces 用に を設定すると、ユーザーにはこれらのフェイルオーバー の E メールも自動的に送信されます WorkSpaces。リージョ

ンベースの登録コードを含む E メールを無視するようにユーザーに指示する必要があります。

制限事項

- クロスリージョンリダイレクトは、プライマリリージョンへの接続が失敗したかどうかを自動的にチェックせず、 を別のリージョンにフェイル WorkSpaces オーバーします。つまり、自動フェイルオーバーは発生しません。

  自動フェイルオーバーシナリオを実装するには、リージョン間リダイレクトと組み合わせて他のメカニズムを使用する必要があります。例えば、Amazon Route 53 フェイルオーバー DNS ルーティングポリシーと、プライマリリージョンの CloudWatch アラームをモニタリングする Route 53 ヘルスチェックを組み合わせることができます。プライマリリージョンの CloudWatch アラームがトリガーされると、DNS フェイルオーバールーティングポリシーは、フェイルオーバーリージョンで WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。
- クロスリージョンリダイレクトを使用している場合、ユーザーデータは異なるリージョン WorkSpaces の 間で保持されません。ユーザーが異なるリージョンからファイルにアクセスできるように、プライマリリージョンとフェイルオーバーリージョンで Amazon WorkDocs がサポートされている場合は、 WorkSpaces ユーザー WorkDocs 用に Amazon を設定することをお勧めします。Amazon の詳細については WorkDocs、「Amazon WorkDocs 管理ガイド」の「Amazon WorkDocs Drive」を参照してください。ユーザーに対して Amazon を有効にする方法の詳細については、 WorkDocs WorkSpace WorkSpaces でディレクトリを登録する「」および「」を参照してくださいAWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする。 WorkSpaces ユーザーが WorkDocs で Amazon をセットアップする方法については WorkSpaces、「Amazon WorkSpaces ユーザーガイド」の「 との統合 WorkDocs」を参照してください。
- クロスリージョンリダイレクトは、Linux、macOS、および Windows WorkSpaces クライアントアプリケーションのバージョン 3.0.9 以降でのみサポートされています。ウェブアクセスでクロスリージョンリダイレクトを使用することもできます。
- クロスリージョンリダイレクトは、 AWS GovCloud (US) Regionおよび中国 (寧夏) AWS リージョンを除く、Amazon WorkSpaces が利用可能なすべてのリージョンで使用できます。

ステップ 1: 接続エイリアスを作成する

同じ AWS アカウントを使用して、クロスリージョンリダイレクトを設定するプライマリリージョンとフェイルオーバーリージョンごとに、接続エイリアスを作成します。

接続エイリアスを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリAWSリージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクト] で、[接続エイリアスの作成] を選択します。
5. [接続文字列] に、`www.example.com` または `desktop.example.com` などの FQDN を入力します。接続文字列は最大 255 文字です。使用できる文字は、文字 (A ~ Z および a ~ z)、数字 (0 ~ 9)、および次の文字のみです: .-

   > **Important**
   >
   > 接続文字列を作成すると、その文字列は常に AWS アカウントに関連付けられます。元のアカウントからすべてのインスタンスを削除しても、同じ接続文字列を別のアカウントで再作成することはできません。接続文字列は、アカウント用にグローバルに予約されています。

6. (オプション) [タグ] で、接続エイリアスと関連付けるタグを指定します。
7. [接続エイリアスの作成] を選択します。
8. これらのステップを繰り返しますが、 ではStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、フェイルオーバーリージョンごとにこれらのステップを繰り返します。必ず同じ AWS アカウントを使用して、各フェイルオーバーリージョンで接続エイリアスを作成してください。

(オプション) ステップ 2: 接続エイリアスを別のアカウントと共有する

接続エイリアスは、同じ AWS リージョン内の別の AWS アカウントと共有できます。接続エイリアスを別のアカウントと共有すると、そのエイリアスを同じリージョン内のそのアカウントが所有するディレクトリに関連付けたり、関連付けを解除したりするアクセス許可がそのアカウントに付与されます。接続エイリアスを所有するアカウントだけが、エイリアスを削除できます。

> **Note**
>
> 接続エイリアスは、AWS リージョンごとに 1 つのディレクトリにのみ関連付けることができます。接続エイリアスを別の AWS アカウントと共有する場合、そのエイリアスをその

リージョンのディレクトリに関連付けることができるのは 1 つのアカウント (自分のアカウントまたは共有アカウント) のみです。

接続エイリアスを別の AWS アカウントと共有するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、接続エイリアスを別の AWS アカウントと共有する AWS リージョンを選択します。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[アクション]、[接続エイリアスの共有/共有解除] を選択します。

   接続エイリアスの詳細ページからエイリアスを共有することもできます。これを行うには、[共有アカウント] で、[接続エイリアスの共有] を選択します。
5. [接続エイリアスの共有/共有解除] ページの [アカウントとの共有] で、この AWS リージョンで接続エイリアスを共有する AWS アカウント ID を入力します。
6. [Share] を選択します。

ステップ 3: 接続エイリアスを各リージョンのディレクトリに関連付ける

同じ接続エイリアスを 2 つ以上のリージョンの WorkSpaces ディレクトリに関連付けると、ディレクトリ間に関連付けペアが作成されます。関連付けペアごとに、プライマリリージョンと 1 つ以上のフェイルオーバーリージョンがあります。

例えば、プライマリリージョンが米国西部 (オレゴン) リージョンの場合、米国西部 (オレゴン) リージョンの WorkSpaces ディレクトリと米国東部 (バージニア北部) リージョンの WorkSpaces ディレクトリをペアリングできます。プライマリリージョンで停止が発生した場合、クロスリージョンリダイレクトは DNS フェイルオーバールーティングポリシーおよび米国西部 (オレゴン) リージョンで行ったヘルスチェックと連携して動作し、米国東部 (バージニア北部) WorkSpaces リージョンで設定した にユーザーをリダイレクトします。クロスリージョンリダイレクトのエクスペリエンスの詳細については、クロスリージョンリダイレクト時の動作 を参照してください。

> **Note**
>
> WorkSpaces ユーザーがフェイルオーバーリージョンからかなり離れている (例えば、何千マイルも離れている) 場合、通常よりも応答性が低くなる WorkSpaces 可能性があります。

ロケーションからさまざまなAWSリージョンへのラウンドトリップタイム (RTT) を確認するには、Amazon WorkSpaces Connection Health Check を使用します。

接続エイリアスをディレクトリに関連付けるには

接続エイリアスは、AWS リージョンごとに 1 つのディレクトリにのみ関連付けることができます。接続エイリアスを別の AWS アカウントと共有している場合、そのエイリアスをそのリージョンのディレクトリに関連付けることができるのは 1 つのアカウント (自分のアカウントまたは共有アカウント) のみです。

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリAWSリージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[アクション]、[関連付け/関連付け解除] を選択します。

   接続エイリアスの詳細ページから、接続エイリアスをディレクトリに関連付けることもできます。これを行うには、[関連付けられたディレクトリ] で、[ディレクトリを関連付ける] を選択します。
5. [関連付け/関連付け解除] ページの [ディレクトリに関連付ける] で、この AWS リージョンで接続エイリアスを関連付けるディレクトリを選択します。

   > **Note**
   >
   > マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを Amazon で使用できます WorkSpaces。Amazon でレプリケートされたリージョンのディレクトリを使用しようとすると失敗 WorkSpaces します。AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内での Amazon WorkSpaces での使用はサポートされていません。
6. [関連付ける] を選択します。
7. これらの手順を繰り返しますが、 でStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、フェイルオーバーリージョンごとにこれらのステップを繰り返します。各フェイルオーバーリージョンのディレクトリに、同じ接続エイリアスを関連付けてください。

ステップ 4: DNS サービスを設定し、DNS ルーティングポリシーを設定する

接続エイリアスと接続エイリアスの関連付けのペアを作成したら、接続文字列で使用したドメインの DNS サービスを設定できます。この目的には、任意の DNS サービスプロバイダーを使用できます。優先 DNS サービスプロバイダーをまだお持ちでない場合は、Amazon Route 53 を使用できます。詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 を DNS サービスとして設定するを参照してください。

ドメインの DNS サービスを設定したら、クロスリージョンリダイレクトに使用する DNS ルーティングポリシーを設定する必要があります。例えば、Amazon Route 53 ヘルスチェックを使用して、ユーザーが特定のリージョン WorkSpaces の に接続できるかどうかを判断できます。ユーザーが接続できない場合は、DNS フェイルオーバーポリシーを使用して、あるリージョンから別のリージョンに DNS トラフィックをルーティングできます。

DNS ルーティングポリシーの選択の詳細については、Amazon Route 53 デベロッパーガイドのルーティングポリシーの選択を参照してください。Amazon Route 53 ヘルスチェックの詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 によるリソースのヘルスチェック方法を参照してください。

DNS ルーティングポリシーを設定するときは、接続エイリアスとプライマリリージョンのディレクトリ間の関連付けの接続識別子が必要です。 WorkSpaces また、フェイルオーバーリージョンまたはリージョン内の接続エイリアスと WorkSpaces ディレクトリ間の関連付けの接続識別子も必要です。

> **Note**
>
> 接続識別子が接続エイリアス ID と同じではありません。接続エイリアス ID は `wsca-` で始まります。

接続エイリアスの関連付けの接続識別子を見つけるには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリAWSリージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列テキスト (FQDN) を選択し、接続エイリアスの詳細ページを表示します。

5. 接続エイリアスの詳細ページの [関連付けられたディレクトリ] で、[接続識別子] に表示される値をメモします。
6. これらの手順を繰り返しますが、 ではStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、これらのステップを繰り返して、各フェイルオーバーリージョンの接続 ID を調べます。

例: Route 53 を使用して DNS フェイルオーバールーティングポリシーを設定するには

次の例では、ドメインのパブリックホストゾーンを設定します。ただし、パブリックホストゾーンまたはプライベートホストゾーンを設定できます。ホストゾーンの設定の詳細については、Amazon Route 53 デベロッパーガイドのホストゾーンの使用を参照してください。

この例では、フェイルオーバールーティングポリシーも使用します。クロスリージョンリダイレクト戦略には、他のルーティングポリシータイプを使用できます。DNS ルーティングポリシーの選択の詳細については、Amazon Route 53 デベロッパーガイドのルーティングポリシーの選択を参照してください。

Route 53 でフェイルオーバールーティングポリシーを設定する場合、プライマリリージョンのヘルスチェックが必要です。Route 53 でのヘルスチェックの作成の詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 ヘルスチェックの作成と DNS フェイルオーバーの設定および ヘルスチェックの作成、更新、および削除を参照してください。

Route 53 ヘルスチェックで Amazon CloudWatch アラームを使用する場合は、プライマリリージョンのリソースをモニタリングするアラームも設定 CloudWatch する必要があります。の詳細については CloudWatch、「Amazon ユーザーガイド」の「Amazon CloudWatchとは」を参照してください。 CloudWatch Route 53 がヘルスチェックで CloudWatch アラームを使用する方法の詳細については、「Amazon Route 53 デベロッパーガイド」の「Route 53 が CloudWatch アラームをモニタリングするヘルスチェックのステータスを決定する方法」および CloudWatch 「アラームのモニタリング」を参照してください。

Route 53 で DNS フェイルオーバールーティングポリシーを設定するには、まずドメインのホストゾーンを作成する必要があります。

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで、[ホストゾーン] を選択し、[ホストゾーンの作成] を選択します。
3. [作成されたホストゾーン] ページで、[ドメイン名] にドメイン名 (`example.com` など) を入力します。

4. [タイプ] で、[パブリックホストゾーン] を選択します。
5. [ホストゾーンの作成] を選択します。

次に、プライマリリージョンのヘルスチェックを作成します。

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで、[ヘルスチェック] を選択し、[ヘルスチェックの作成] を選択します。
3. [ヘルスチェックの設定] ページで、ヘルスチェックの名前を入力します。
4. のモニタリング対象 で、エンドポイント 、他のヘルスチェックのステータス (計算されたヘルスチェック) 、または CloudWatch アラームの状態 を選択します。
5. 前のステップで選択した内容に応じて、ヘルスチェックを設定し、[次へ] を選択します。
6. [ヘルスチェックが失敗したときに通知を受け取る] ページの [アラームの作成] で、[はい] または [いいえ] を選択します。
7. [ヘルスチェックの作成] を選択します。

ヘルスチェックを作成したら、DNS フェイルオーバーレコードを作成できます。

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ナビゲーションペインで [Hosted zones] を選択します。
3. [ホストゾーン] ページで、ドメイン名を選択します。
4. ドメイン名の詳細ページで、[レコードの作成] を選択します。
5. [ルーティングポリシーの選択] ページで、[フェイルオーバー] を選択し、[次へ] を選択します。
6. [レコードの設定] ページの [基本設定] で、[レコード名] にサブドメイン名を入力します。たとえば、FQDN が `desktop.example.com` の場合は、**`desktop`** と入力します。

   > **Note**
   >
   > ルートドメインを使用する場合は、[レコード名] を空白のままにします。ただし、 専用にドメインを設定していない`workspaces`限り、 `desktop`や などのサブドメインを使用することをお勧めします WorkSpaces。

7. [レコードのタイプ] で、[TXT – E メールの送信者の確認およびアプリケーション固有の値の確認に使用します] を選択します。
8. [TTL 秒] の設定はデフォルトのままにします。

9. [***your_domain_name***に追加するフェイルオーバーレコード] で、[フェイルオーバーレコードの定義] を選択します。

次に、プライマリリージョンとフェイルオーバーリージョンのフェイルオーバーレコードを設定する必要があります。

例: プライマリリージョンのフェイルオーバーレコードを設定するには

1. [フェイルオーバーレコードの定義] ダイアログボックスの [値/トラフィックのルーティング先] で、[レコードのタイプに応じた IP アドレスまたは別の値] を選択します。
2. サンプルテキストエントリを入力するためのボックスが開きます。プライマリリージョンの接続エイリアスの関連付けの接続識別子を入力します。
3. [フェイルオーバーレコードタイプ] で、[プライマリ] を選択します。
4. [ヘルスチェック] で、プライマリリージョン用に作成したヘルスチェックを選択します。
5. [レコード ID] に、このレコードを識別するための説明を入力します。
6. [フェイルオーバーレコードの定義] を選択します。新しいフェイルオーバーレコードは、[***your_domain_name*** に追加するフェイルオーバーレコード] の下に表示されます。

例: フェイルオーバーリージョンのフェイルオーバーレコードを設定するには

1. [***your_domain_name***に追加するフェイルオーバーレコード] で、[フェイルオーバーレコードの定義] を選択します。
2. [フェイルオーバーレコードの定義] ダイアログボックスの [値/トラフィックのルーティング先] で、[レコードのタイプに応じた IP アドレスまたは別の値] を選択します。
3. サンプルテキストエントリを入力するためのボックスが開きます。フェイルオーバーリージョンの接続エイリアスの関連付けの接続識別子を入力します。
4. [フェイルオーバーレコードタイプ] で、[セカンダリ] を選択します。
5. (オプション) [ヘルスチェック] に、フェイルオーバーリージョン用に作成したヘルスチェックを入力します。
6. [レコード ID] に、このレコードを識別するための説明を入力します。
7. [フェイルオーバーレコードの定義] を選択します。新しいフェイルオーバーレコードは、[***your_domain_name*** に追加するフェイルオーバーレコード] の下に表示されます。

プライマリリージョンに設定したヘルスチェックが失敗した場合、DNS フェイルオーバールーティングポリシーは WorkSpaces ユーザーをフェイルオーバーリージョンにリダイレクトします。Route 53 は引き続きプライマリリージョンのヘルスチェックを監視し、プライマリリージョンのヘルスチェックが失敗しなくなった場合、Route 53 は WorkSpaces ユーザーをプライマリリージョン WorkSpaces の に自動的にリダイレクトします。

DNS レコードの作成の詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 コンソールを使用したレコードの作成を参照してください。DNS TXT レコードの設定の詳細については、Amazon Route 53 デベロッパーガイドの TXT レコードタイプを参照してください。

ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する

停止中にユーザーの WorkSpaces 権限が必要に応じてリダイレクトされるようにするには、接続文字列 (FQDN) をユーザーに送信する必要があります。リージョンベースの登録コード (などWSpdx+ABC12D) を WorkSpaces 既にユーザーに発行している場合、それらのコードは引き続き有効です。ただし、クロスリージョンリダイレクトが機能するには、 WorkSpaces ユーザーはクライアントアプリケーション WorkSpaces に WorkSpaces を登録するときに、接続文字列を登録コードとして使用する必要があります。

> **Important**
>
> Active Directory でユーザーを作成するのではなく、 WorkSpaces コンソールでユーザーを作成すると、 WorkSpaces 新しい を起動するたびに、 によってリージョンベースの登録コード (などWSpdx+ABC12D) が記載された招待メールがユーザーに自動的に送信されます WorkSpace。既にクロスリージョンリダイレクトを設定している場合でも、新しい に自動的に送信される招待 E メールには、接続文字列の代わりにこのリージョンベースの登録コード WorkSpaces が含まれます。
>
> WorkSpaces ユーザーがリージョンベースの登録コードではなく接続文字列を使用していることを確認するには、次の手順を使用して、接続文字列を含む別の E メールを送信する必要があります。

接続文字列を WorkSpaces ユーザーに送信するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリAWSリージョンを選択します WorkSpaces。
3. ナビゲーションペインで、 を選択しますWorkSpaces。

4. WorkSpaces ページで、検索ボックスを使用して招待を送信するユーザーを検索し、検索結果 WorkSpace から対応する を選択します。一度に選択できる は 1 WorkSpace つだけです。
5. [アクション]、[Invite User (ユーザーを招待)] の順に選択します。
6. 「ユーザーにユーザーを招待する WorkSpaces」ページに、ユーザーに送信する E メールテンプレートが表示されます。
7. (オプション) WorkSpaces ディレクトリに複数の接続エイリアスが関連付けられている場合は、接続エイリアス文字列リストからユーザーに使用する接続文字列を選択します。E メールテンプレートが更新され、選択した文字列が表示されます。
8. メールアプリケーションを使用して、E メールテンプレートテキストをコピーしユーザー宛のメールに貼り付けます。E メールアプリケーションでは、必要に応じてテキストを変更できます。招待 E メールの準備ができたら、ユーザーに送信します。

クロスリージョンリダイレクトのアーキテクチャ図

次の図は、クロスリージョンリダイレクトのデプロイプロセスを示しています。

> **Note**
>
> クロスリージョンリダイレクトは、クロスリージョンフェイルオーバーとフォールバックのみを容易にします。セカンダリリージョン WorkSpaces での の作成と保守が容易ではなく、クロスリージョンデータレプリケーションも許可されません。 WorkSpaces プライマリリージョンとセカンダリリージョンの両方の は、個別に管理する必要があります。

クロスリージョンリダイレクトを開始する

障害が発生した場合は、DNS レコードを手動で更新するか、ヘルスチェックに基づいて自動ルーティングポリシーを使用して、フェイルオーバーリージョンを決定できます。「Amazon Route 53 を使用したディザスタリカバリメカニズムの作成」で説明されているディザスタリカバリメカニズムに従うことをお勧めします。

クロスリージョンリダイレクト時の動作

リージョンのフェイルオーバー中、 WorkSpaces ユーザーはプライマリリージョン WorkSpaces のから切断されます。再接続しようとすると、次のエラーメッセージが表示されます。

```
We can't connect to your WorkSpace. Check your network connection, and then
try again.
```

その後、ユーザーは再度ログインするように求められます。登録コードとして FQDN を使用している場合、再度ログインすると、DNS フェイルオーバールーティングポリシー WorkSpaces によって、フェイルオーバーリージョンで設定した にリダイレクトされます。

> **Note**
>
> 場合によっては、ユーザーが再度ログインしたときに再接続できないことがあります。この動作が発生した場合は、 WorkSpaces クライアントアプリケーションを閉じて再起動してから、再度ログインする必要があります。

ディレクトリからの接続エイリアスの関連付けを解除する

ディレクトリから接続エイリアスの関連付けを解除できるのは、ディレクトリを所有するアカウントだけです。

接続エイリアスを別のアカウントと共有していて、そのアカウントがそのアカウントが所有するディレクトリに接続エイリアスを関連付けている場合は、そのアカウントを使用して接続エイリアスとディレクトリとの関連付けを解除する必要があります。

ディレクトリから接続エイリアスの関連付けを解除するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、関連付けを解除する接続エイリアスが含まれている AWS リージョンを選択します。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[アクション]、[関連付け/関連付け解除] を選択します。

   接続エイリアスの詳細ページから接続エイリアスの関連付けを解除することもできます。これを行うには、[関連付けられたディレクトリ] で、[関連付け解除] を選択します。
5. [関連付け/関連付け解除] ページで、[関連付けを解除] を選択します。
6. 関連付けの解除を確認するダイアログボックスで、[関連付けを解除] を選択します。

接続エイリアスの共有を解除する

接続エイリアスの所有者だけがエイリアスを共有解除できます。接続エイリアスをアカウントと共有解除すると、そのアカウントは接続エイリアスをディレクトリに関連付けることができなくなります。

接続エイリアスを共有解除するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、共有を解除する接続エイリアスを含む AWS リージョンを選択します。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[アクション]、[接続エイリアスの共有/共有解除] を選択します。

   接続エイリアスの詳細ページから接続エイリアスの共有を解除することもできます。これを行うには、[共有アカウント] で [共有解除] を選択します。
5. [接続の共有/共有解除] ページで、[共有解除] を選択します。
6. 接続エイリアスの共有解除を確認するダイアログボックスで、[共有解除] を選択します。

接続エイリアスを削除する

接続エイリアスは、アカウントによって所有され、ディレクトリに関連付けられていない場合にのみ、削除できます。

接続エイリアスを別のアカウントと共有していて、そのアカウントがそのアカウントが所有するディレクトリに接続エイリアスを関連付けている場合、接続エイリアスを削除する前に、そのアカウントと接続エイリアスをディレクトリから関連付け解除する必要があります。

> **Important**
>
> 接続文字列を作成すると、その文字列は常に AWS アカウントに関連付けられます。元のアカウントからすべてのインスタンスを削除しても、同じ接続文字列を別のアカウントで再作成することはできません。接続文字列は、アカウント用にグローバルに予約されています。

> **Warning**
>
> ユーザーの登録コード WorkSpaces として FQDN を使用しなくなる場合は、潜在的なセキュリティ問題を防ぐために、一定の予防措置を講じる必要があります。詳細については、「クロスリージョンリダイレクトの使用を停止する場合のセキュリティ上の考慮事項」を参照してください。

接続エイリアスを削除するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、削除する接続エイリアスを含む AWS リージョンを選択します。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[削除] を選択します。

   接続エイリアスの詳細ページから接続エイリアスを削除することもできます。これを行うには、ページの右上の [削除] を選択します。

   > **Note**
   >
   > [削除] ボタンが無効になっている場合は、そのエイリアスの所有者であることを確認し、エイリアスがディレクトリに関連付けられていないことを確認します。

5. 削除の確認を求めるダイアログボックスで、[削除] を選択します。

接続エイリアスを関連付けおよび関連付け解除するための IAM 許可

IAM ユーザーを使用して接続エイリアスを関連付け、または関連付けを解除する場合、ユーザーには `workspaces:AssociateConnectionAlias` および `workspaces:DisassociateConnectionAlias` のアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
```

```
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Important

接続エイリアスを所有していないアカウントの接続エイリアスを関連付け、または関連付けを解除するための IAM ポリシーを作成する場合は、ARN でアカウント ID を指定できません。代わりに、次のポリシー例に示すように、アカウント ID には * を使用する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

ARN でアカウント ID を指定できるのは、関連付け、または関連付けを解除する接続エイリアスをそのアカウントが所有している場合だけです。

IAM の操作方法の詳細については、WorkSpaces の Identity and Access Management を参照してください。

クロスリージョンリダイレクトの使用を停止する場合のセキュリティ上の考慮事項

WorkSpaces ユーザーの登録コードとして FQDN を使用しなくなる場合は、潜在的なセキュリティ問題を防ぐために、以下の予防措置を講じる必要があります。

- ディレクトリのリージョン固有の登録コード (などWSpdx+ABC12D) を WorkSpaces ユーザーに発行 WorkSpaces し、登録コードとして FQDN の使用を停止するよう指示してください。
- まだこのドメインを所有している場合は、フィッシング攻撃で悪用されないように、DNS TXT レコードを更新してこのドメインを削除してください。DNS TXT レコードからこのドメインを削除し、 WorkSpaces ユーザーが FQDN を登録コードとして使用しようとすると、接続試行は無害に失敗します。
- このドメイン を所有しなくなった場合、 WorkSpaces ユーザーはリージョン固有の登録コードを使用する必要があります。登録コードとして FQDN を使用し続けると、接続試行が悪意のあるサイトにリダイレクトされる可能性があります。

Amazon のマルチリージョンレジリエンス WorkSpaces

Amazon WorkSpaces Multi-Region Resilience (MRR) を使用すると、中断したイベントが原因でプライマリリージョンに到達できない場合に、ユーザーをセカンダリ WorkSpaces リージョンにリダイレクトできます。スタンバイ へのログ記録時に登録コードを切り替える必要はありません WorkSpaces。スタンバイ WorkSpaces は、スタンバイデプロイの作成と管理を効率化する Amazon WorkSpaces マルチリージョンレジリエンスの機能です。セカンダリリージョンでユーザーディレクトリを設定したら、スタンバイを作成するプライマリリージョン WorkSpace の を選択します WorkSpace 。システムはプライマリ WorkSpace バンドルイメージをセカンダリリージョンに自動的にミラーリングします。その後、セカンダリリージョン WorkSpace に新しいスタンバイを自動的にプロビジョニングします。

Amazon WorkSpaces マルチリージョンレジリエンスは、DNS ヘルスチェックとフェイルオーバー機能を活用するクロスリージョンリダイレクトに基づいて構築されています。これにより、WorkSpaces 登録コードとして完全修飾ドメイン名 (FQDN) を使用できます。ユーザーが にログインすると WorkSpaces、FQDN のドメインネームシステム (DNS) ポリシーに基づいて、サポートされている WorkSpaces リージョン間でリダイレクトできます。Amazon Route 53 を使用する場合は、 のクロスリージョンリダイレクト戦略を策定するときに、Amazon CloudWatch アラームをモニタリングするヘルスチェックを使用することをお勧めします WorkSpaces。詳細について

は、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 ヘルスチェックの作成」および「DNS フェイルオーバーの設定」を参照してください。

データレプリケーションは、プライマリリージョンからセカンダリリージョンにデータを一方向でレプリケート WorkSpaces するスタンバイのアドオン機能です。データレプリケーションを有効にすると、システムボリュームとユーザーボリュームの EBS スナップショットが 12 時間ごとに作成されます。マルチリージョンレジリエンスは、定期的に新しいスナップショットをチェックします。スナップショットが見つかると、セカンダリリージョンへのコピーが開始されます。コピーがセカンダリリージョンに到着すると、セカンダリ の更新に使用されます WorkSpace。

内容

前提条件

- スタンバイ を作成する前に、プライマリリージョンのユーザー WorkSpaces 用に を作成する必要があります WorkSpaces。の作成の詳細については、 WorkSpaces「」を参照してくださいWorkSpaces を使用して仮想デスクトップを起動します。。
- スタンバイ でデータレプリケーションを有効にするには WorkSpaces、セルフマネージド Active Directory または AWS Managed Microsoft AD がスタンバイリージョンにレプリケートするように設定されている必要があります。詳細については、AWS 「 Managed Microsoft AD ディレクトリを作成する」および「レプリケートされたリージョンを追加する」を参照してください。
- ENA、NVMe ドライバー、PV ドライバーなどのネットワーク依存関係ドライバーをプライマリで必ず更新してください WorkSpaces。これは少なくとも 6 か月に 1 回行う必要があります。詳細については、「Elastic Network Adapter (ENA) ドライバー のインストールまたはアップグレードAWS NVMe ドライバー 」、「Windows インスタンス 用」、および「Windows インスタンスで PV ドライバーをアップグレードする」を参照してください。

- EC2Config, EC2Launch、および EC2Launch V2 エージェントを定期的に最新バージョンに更新してください。これは少なくとも 6 か月に 1 回行う必要があります。詳細については、EC2Config と EC2Launch の更新」を参照してください。
- 適切なデータレプリケーションを行うには、プライマリリージョンとセカンダリリージョンの Active Directory が FQDN、OU、およびユーザー SID と同期していることを確認します。
- スタンバイのデフォルトのクォータ (制限) WorkSpaces は 0 です。スタンバイ を作成する前に、サービスクォータの引き上げをリクエストする必要があります WorkSpace。詳細については、「Amazon WorkSpaces クォータ」を参照してください。
- カスタマーマネージドキーを使用して、プライマリ とスタンバイ の両方を暗号化していることを確認します WorkSpaces。単一リージョンキーまたはマルチリージョンキーを使用して、プライマリ とスタンバイ を暗号化できます WorkSpaces。

制限事項

- スタンバイはプライマリ のバンドルイメージ WorkSpaces のみをコピーします WorkSpaces が、プライマリ からシステムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) をコピーしません WorkSpaces。システムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) WorkSpaces をプライマリ からスタンバイ にコピーするには WorkSpaces、データレプリケーションを有効にする必要があります。
- スタンバイ を直接変更、再構築、復元、または移行することはできません WorkSpace。
- クロスリージョンリダイレクトのフェイルオーバーは、DNS 設定で制御します。自動フェイルオーバーシナリオを実装するには、クロスリージョンリダイレクトと組み合わせて別のメカニズムを使用する必要があります。例えば、Amazon Route 53 フェイルオーバー DNS ルーティングポリシーを、プライマリリージョンの CloudWatch アラームをモニタリングする Route 53 ヘルスチェックと組み合わせて使用できます。プライマリリージョンの CloudWatch アラームが呼び出されると、DNS フェイルオーバールーティングポリシーは、フェイルオーバーリージョンで WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。
- データレプリケーションは 1 つの方法のみで、プライマリリージョンからセカンダリリージョンにデータをコピーします。スタンバイ WorkSpaces フェイルオーバー中は、12～24 時間でデータとアプリケーションにアクセスできます。停止後、セカンダリで作成したデータを手動でバックアップ WorkSpace し、ログアウトします。プライマリ からデータにアクセスできるように、作業内容をネットワークドライブなどの外部ドライブに保存することをお勧めします WorkSpace。
- データレプリケーションは Simple AD AWS をサポートしていません。
- スタンバイ でデータレプリケーションを有効にすると WorkSpaces、プライマリ WorkSpaces (ルートボリュームとシステムボリュームの両方) の EBS スナップショットが 12 時間ごとに取

得されます。特定のデータボリュームの初期スナップショットはフルで、それ以降のスナップショットは増分です。その結果、特定の の最初のレプリケーション WorkSpace には、それ以降のレプリケーションよりも時間がかかります。スナップショットは の内部スケジュールで開始 WorkSpaces され、タイミングを制御することはできません。

- プライマリ WorkSpace とスタンバイが同じドメインを使用して WorkSpace 参加する場合は、ドメインコントローラーとの接続が失われないように WorkSpace 、特定の時点でプライマリ WorkSpace またはスタンバイのいずれかにのみ接続することをお勧めします。
- マルチリージョンレプリケーション AWS Managed Microsoft AD 用に を設定する場合、プライマリリージョンのディレクトリのみを で使用するために登録できます WorkSpaces。で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると WorkSpaces、失敗します。を使用したマルチリージョンレプリケーション AWS Managed Microsoft AD は、レプリケートされたリージョン WorkSpaces 内での での使用はサポートされていません。
- クロスリージョンリダイレクトを既に設定していて、スタンバイ を使用せずにプライマリリージョンとセカンダリリージョン WorkSpaces の両方で作成している場合は WorkSpaces、セカンダリリージョン WorkSpace の既存の をスタンバイ WorkSpace に直接変換することはできません。代わりに、セカンダリリージョン WorkSpace で をシャットダウンし、スタンバイを作成するプライマリリージョン WorkSpace で を選択し WorkSpace 、スタンバイを使用してスタンバイ WorkSpaces を作成する必要があります WorkSpace。
- 停止後、セカンダリで作成したデータを手動でバックアップ WorkSpace し、ログアウトします。プライマリ からデータにアクセスできるように、作業内容をネットワークドライブなどの外部ドライブに保存することをお勧めします WorkSpace。
- WorkSpaces マルチリージョンレジリエンスは現在、次のリージョンで利用できます。
  - 米国東部 (バージニア北部) リージョン
  - 米国西部 (オレゴン) リージョン
  - 欧州 (フランクフルト) リージョン
  - 欧州 (アイルランド) リージョン
- WorkSpaces マルチリージョンレジリエンスは、Linux、macOS、および Windows WorkSpaces クライアントアプリケーションのバージョン 3.0.9 以降でのみサポートされています。ウェブアクセスでマルチリージョンレジリエンスを使用することもできます。
- WorkSpaces マルチリージョンレジリエンスは、Windows と Bring Your Own License (BYOL) をサポートしています WorkSpaces。Amazon Linux、Ubuntu WorkSpaces、または GPU 対応 WorkSpaces （ 例： Graphics、 GraphicsProGraphics.g4dn、または GraphicsPro.g4dn)。
- フェイルオーバーまたはフェイルバックが完了したら、15～30 分待ってから に接続します WorkSpace。

マルチリージョンレジリエンススタンバイを設定する WorkSpace

マルチリージョンレジリエンススタンバイを設定するには WorkSpace

1. プライマリリージョンとセカンダリリージョンの両方でユーザーディレクトリを設定します。各リージョンの各 WorkSpaces ディレクトリで同じユーザー名を使用していることを確認してください。

   Active Directory ユーザーデータを同期させるには、AD Connector を使用して、ユーザー WorkSpaces 用に設定した各リージョンで同じ Active Directory を指すことをお勧めします。ディレクトリの作成の詳細については、「 でディレクトリを登録する WorkSpaces」を参照してください。

   > **Important**
   >
   > マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを で使用するために登録できます WorkSpaces。で使用するためにレプリケートされたリージョンにディレクトリを登録しようとすると失敗 WorkSpaces します。を使用したマルチリージョンレプリケーション AWS Managed Microsoft AD は、レプリケートされたリージョン WorkSpaces 内での での使用はサポートされていません。

2. プライマリリージョンのユーザー WorkSpaces 用に を作成します。の作成の詳細については WorkSpaces、「 の起動 WorkSpaces」を参照してください。
3. セカンダリリージョン WorkSpace にスタンバイを作成します。スタンバイ の作成の詳細については WorkSpace、「スタンバイ の作成 WorkSpace」を参照してください。
4. 接続文字列 (FQDN) を作成して、プライマリリージョンとセカンダリリージョンのユーザーディレクトリに関連付けます。

   スタンバイはクロスリージョンリダイレクトに基づいて構築されるため WorkSpaces 、アカウントでクロスリージョンリダイレクトを有効にする必要があります。 Amazon のクロスリージョンリダイレクトの手順のステップ 1～3 に従います WorkSpaces。
5. DNS サービスを設定し、DNS ルーティングポリシーを設定します。

   DNS サービスを設定し、必要な DNS ルーティングポリシー を設定する必要があります。クロスリージョンリダイレクトは、DNS ルーティングポリシーと組み合わせて機能し、必要に応じて WorkSpaces ユーザーをリダイレクトします。

6. クロスリージョンリダイレクトの設定が完了したら、FQDN 接続文字列を記載したメールをユーザーに送信する必要があります。詳細については、「ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する」を参照してください。 WorkSpaces ユーザーが、プライマリリージョンのリージョンベースの登録コード (WSpdx +ABC12D など) の代わりに FQDN ベースの登録コードを使用していることを確認します。

> **Important**
>
> - Active Directory でユーザーを作成するのではなく WorkSpaces 、コンソールでユーザーを作成すると、 は、新しい を起動するたびに、リージョンベースの登録コードが記載された招待メールをユーザー WorkSpaces に自動的に送信します WorkSpace。つまり、セカンダリ リージョンのユーザー WorkSpaces 用に を設定すると、ユーザーはこれらのセカンダリ の E メールも自動的に受信します WorkSpaces。リージョンベースの登録コードを含む E メールを無視するようにユーザーに指示する必要があります。
> - リージョン固有の登録コードは引き続き有効ですが、クロスリージョンリダイレクトが機能するには、ユーザーは登録コードとして FQDN を使用する必要があります。

スタンバイを作成する WorkSpace

スタンバイ を作成する前に WorkSpace、プライマリリージョンとセカンダリリージョンの両方でユーザーディレクトリを作成する、プライマリリージョンでユーザー WorkSpaces をプロビジョニングする、アカウントでクロスリージョンリダイレクトを設定する、サービスクォータによるスタンバイ WorkSpaces 制限の引き上げをリクエストするなど、前提条件を満たしていることを確認してください。

スタンバイを作成するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで、 を選択しますWorkSpaces。
4. スタンバイを作成する WorkSpace を選択します WorkSpace 。
5. アクション を選択し、スタンバイ の作成 WorkSpaceを選択します。
6. スタンバイ を作成するセカンダリリージョンを選択し WorkSpace、次へ を選択します。
7. セカンダリリージョンのユーザーディレクトリを選択し、[Next] (次へ) を選択します。

8. (オプション) 暗号化キーの追加、データ暗号化の有効化、タグの管理を行います。

   - 暗号化キーを追加するには、「入力暗号化キー」に入力します。
   - データレプリケーションを有効にするには、データレプリケーションを有効にする を選択します。次に、チェックボックスをオンにして、月額料金の追加を承認していることを確認します。
   - タグを追加するには、[新しいタグを追加] を選択します。

   [次へ] を選択します。

   > **Note**
   >
   > - 元の WorkSpace が暗号化されている場合、このフィールドは事前に入力されています。ただし、独自の暗号化キーで置き換えることもできます。
   > - データレプリケーションステータスの更新には数分かかります。
   > - スタンバイ WorkSpace がプライマリ のスナップショットで正常に更新されると WorkSpace、スナップショットのタイムスタンプはリカバリスナップショット で確認できます。

9. スタンバイの設定を確認し WorkSpaces 、 の作成を選択します。

   > **Note**
   >
   > - スタンバイ に関する情報を表示するには WorkSpaces、プライマリ WorkSpace 詳細ページに移動します。
   > - スタンバイはプライマリ のバンドルイメージ WorkSpace のみをコピーします WorkSpace が、プライマリ からシステムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) をコピーしません WorkSpaces。デフォルトでは、データレプリケーションはオフになっています。システムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) WorkSpaces をプライマリ からスタンバイ にコピーするには WorkSpaces、データレプリケーションを有効にする必要があります。

スタンバイの管理 WorkSpace

スタンバイ を直接変更、再構築、復元、または移行することはできません WorkSpace。

スタンバイのデータレプリケーションを有効にするには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. プライマリリージョンに移動し、プライマリ WorkSpace ID を選択します。
3. スタンバイ WorkSpace セクションまでスクロールし、スタンバイ の編集 WorkSpaceを選択します。
4. データレプリケーションを有効にする を選択します。次に、チェックボックスをオンにして、月額料金の追加を承認していることを確認します。次に、保存を選択します。

> **Note**
>
> - スタンバイは休止 WorkSpaces できません。スタンバイ を停止しても WorkSpace、保存されていない作業は保持されません。スタンバイ を終了する前に、必ず作業を保存することをお勧めします WorkSpaces。
> - スタンバイ でデータレプリケーションを有効にするには WorkSpaces、セルフマネージド Active Directory または AWS Managed Microsoft AD がスタンバイリージョンにレプリケートするように設定されている必要があります。ディレクトリを設定するには、Amazon WorkSpaces および AWS Directory Services でのビジネス継続性の構築のチュートリアルセクションのステップ 1 ~ 3 に従います。または、「Amazon でのマルチリージョン AWS マネージドアクティブディレクトリ WorkSpacesの使用」を参照してください。マルチリージョンレプリケーションは、 Managed Microsoft AD の AWS Enterprise Edition でのみサポートされています。
> - データレプリケーションステータスの更新には数分かかります。
> - スタンバイ WorkSpace がプライマリ のスナップショットで正常に更新されると WorkSpace、スナップショットのタイムスタンプはリカバリスナップショット で確認できます。

スタンバイを削除する WorkSpace

スタンバイは、通常の を終了する WorkSpace のと同じ方法で終了できます WorkSpace。

スタンバイを削除するには WorkSpace

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。

3. ナビゲーションペインで、 を選択しますWorkSpaces。
4. スタンバイ を選択し WorkSpace 、 の削除 を選択します。スタンバイ の削除には約 5 分かかります WorkSpace。削除中、スタンバイのステータス WorkSpace は の終了に設定されます。削除が完了すると、スタンバイはコンソールから WorkSpace 消えます。

> **Note**
>
> スタンバイの削除 WorkSpace は永続的なアクションであり、元に戻すことはできません。スタンバイ WorkSpace ユーザーのデータは保持されず、破棄されます。ユーザーデータのバックアップについては、 AWS サポートにお問い合わせください。

スタンバイ用の一方向データレプリケーション WorkSpaces

マルチリージョンレジリエンスでデータレプリケーションを有効にすると、プライマリリージョンからセカンダリリージョンにデータをレプリケートできます。定常状態では、マルチリージョンレジリエンスは 12 時間 WorkSpaces ごとにプライマリのシステム (C ドライブ) とデータ (D ドライブ) のスナップショットをキャプチャします。これらのスナップショットはセカンダリリージョンに転送され、スタンバイ の更新に使用されます WorkSpaces。デフォルトでは、スタンバイ のデータレプリケーションは無効になっています WorkSpaces。

スタンバイ でデータレプリケーションを有効にすると WorkSpaces、特定のデータボリュームの初期スナップショットは完了し、それ以降のスナップショットは増分になります。その結果、特定のの最初のレプリケーション WorkSpace は、それ以降のレプリケーションよりも時間がかかります。スナップショットは 内の所定の間隔でトリガー WorkSpaces され、ユーザーがタイミングを制御することはできません。

フェイルオーバー中、ユーザーがセカンダリリージョンにリダイレクトされると、12～24 時間経過したデータやアプリケーション WorkSpaces を使用してスタンバイにアクセスできます。ユーザーがスタンバイ を使用している間 WorkSpaces、マルチリージョンレジリエンスは、スタンバイ WorkSpaces からログアウトしたり、プライマリリージョンのスナップショット WorkSpaces でスタンバイを更新したりすることを強制しません。

停止後、ユーザーはスタンバイ からログアウト WorkSpaces する前に、セカンダリ で作成したデータを手動でバックアップする必要があります WorkSpaces。再度ログインすると、プライマリリージョンとそのプライマリ に誘導されます WorkSpaces。

Amazon EC2 容量を復旧用に予約する計画

Amazon マルチリージョンレジリエンス (MRR) は、デフォルトで Amazon EC2 オンデマンドプールに依存しています。特定の Amazon EC2 インスタンスタイプがリカバリをサポートできない場合、MRR は使用可能なインスタンスタイプが見つかるまでインスタンスのスケールアップを自動的に試行しますが、極端な状況では、インスタンスが常に利用可能であるとは限りません。最も重要なに必要なインスタンスタイプの可用性を向上させるには WorkSpaces、 AWS サポートにお問い合わせください。キャパシティプランニングをサポートします。

Amazon WorkSpaces に関するセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS の顧客は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS と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、AWS クラウドで AWS の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負います。また、AWS は、使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。WorkSpaces に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の AWS サービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS のサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、WorkSpaces 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。ここでは、セキュリティとコンプライアンスの目標を満たすように WorkSpaces を設定する方法を説明します。また、WorkSpaces リソースのモニタリングや保護に役立つ、他の AWS サービスの使用方法についても説明します。

目次

Amazon でのデータ保護 WorkSpaces

責任 AWS 共有モデル、Amazon のデータ保護に適用されます WorkSpaces。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

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

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- を使用して API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、WorkSpaces または SDK を使用して AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

WorkSpaces および FIPS エンドポイントの暗号化の詳細については、「」を参照してくださいFedRAMP 認証または DoD SRG 準拠のために Amazon WorkSpaces をセットアップする。

保管中の暗号化

のストレージボリュームは、 の AWS KMS キー WorkSpaces を使用して暗号化できます AWS Key Management Service。詳細については、「暗号化済み WorkSpaces」を参照してください。

暗号化されたボリューム WorkSpaces で を作成すると、 WorkSpaces は Amazon Elastic Block Store (Amazon EBS) を使用してそれらのボリュームを作成および管理します。EBS は、業界標準の AES-256 アルゴリズムを使用してデータキーでボリュームを暗号化します。詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS 暗号化Amazon EC2」を参照してください。

転送中の暗号化

PCoIP については、転送中のデータは、TLS 1.2 暗号化と SigV4 リクエスト署名を使用して暗号化されます。PCoIPプロトコルは、AES暗号化で暗号化されたUDPトラフィックをストリーミングピクセルに使用します。ポート4172 (TCPおよびUDP) を使用するストリーミング接続は、AES-128暗号とAES-256暗号を使用して暗号化されますが、暗号化のデフォルトは128ビットです。このデフォルトを 256 ビットに変更するには、Windows の PCoIP セキュリティ設定グループポリシーの設定を使用するか WorkSpaces、Amazon Linux の `pcoip-agent.conf` ファイルで PCoIP セキュリティ設定を変更します WorkSpaces。

Amazon のグループポリシー管理の詳細については WorkSpaces、「」のPCoIP セキュリティ設定を構成する「」を参照してくださいWindows の管理 WorkSpaces。変更の詳細については、「」を参照してください。`pcoip-agent.conf`ファイルについては、Amazon Linux で PCoIP エージェントの動作を制御する WorkSpacesおよびPCoIP セキュリティ設定Teradiciのドキュメントを参照してください。

WorkSpaces ストリーミングプロトコル (WSP) の場合、転送中のデータのストリーミングと制御は、UDP トラフィックの DTLS 1.2 暗号化と TCP トラフィックの TLS 1.2 暗号化を使用して、AES-256 暗号で暗号化されます。

WorkSpaces の Identity and Access Management

デフォルトでは、IAM ユーザーには WorkSpaces のリソースおよびオペレーションのための許可がありません。IAM ユーザーに WorkSpaces のリソース管理を許可するには、それらのユーザーに許可を明示的に付与する IAM ポリシーを作成し、このポリシーを許可を必要とする IAM ユーザーまたはグループと結びつける必要があります。

アクセスを提供するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「シークレットの作成と管理」の手順に従ってください。
- ID プロバイダーを通じて IAM で管理されているユーザー:

  ID フェデレーションのロールを作成する。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。
- IAM ユーザー:
  - ユーザーが設定できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
  - (非推奨) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス許可の追加」の指示に従います。

IAM ポリシーの詳細については、IAM ユーザーガイドのポリシーとアクセス許可を参照してください。

WorkSpaces はまた、WorkSpaces サービスが必要なリソースにアクセスするのを許可する IAM ロール `workspaces_DefaultRole` を作成します。

IAM の詳細については、Identity and Access Management (IAM) および IAM ユーザーガイドを参照してください。IAM アクセス許可ポリシーで使用する WorkSpaces 固有のリソース、アクション、および条件コンテキストキーは、IAM ユーザーガイドの Amazon WorkSpaces のアクション、リソース、および条件キーにあります。

IAM ポリシーの作成に役立つツールについては、AWS Policy Generator を参照してください。また、IAM Policy Simulator を使用して、ポリシー がAWS への特定のリクエストを許可するか拒否するかをテストすることもできます。

> **Note**
>
> Amazon WorkSpaces は、WorkSpace への IAM 認証情報のプロビジョニング (インスタンスプロファイルなど) をサポートしていません。

目次

- IAM ポリシーで WorkSpaces リソースを指定する
- workspaces_DefaultRole ロールを作成する
- AmazonWorkSpacesPCAAccess サービスロールを作成する
- WorkSpaces 用の AWS 管理ポリシー

ポリシーの例

以下の例では、Amazon WorkSpaces に対して IAM ユーザーが所有するアクセス許可を制御するために使用できるポリシーステートメントを示しています。

Example 1: すべての WorkSpaces タスクを実行する

次のポリシーステートメントは、ディレクトリの作成や管理などすべての WorkSpaces タスクを実行するための許可を IAM ユーザーに付与します。また、クイックセットアップ手順を実行するアクセス許可も付与されます。

Amazon WorkSpaces は、API およびコマンドラインツールを使用する際に `Action` および `Resource` 要素を完全にサポートしますが、AWS Management Console から Amazon WorkSpaces を使用するには、IAM ユーザーに次のアクションおよびリソースのための許可が必要です。

- アクション: `"workspaces:*"` と `"ds:*"`
- リソース: `"Resource": "*"`

次のポリシー例では、IAM ユーザーが AWS Management Console から Amazon WorkSpaces を使用することを許可する方法を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
```

```
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Example 2: WorkSpace 固有のタスクを実行します

次のポリシーステートメントは、WorkSpaces の起動や削除など、WorkSpace 固有のタスクを実行するためのアクセス許可を IAM ユーザーに付与します。ポリシーステートメントで、ds:* アクションは広範なアクセス許可 (アカウント内のすべての Directory Services オブジェクトの完全なコントロール) を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

WorkSpaces 内のユーザーが Amazon WorkDocs を有効にすることも許可するには、次の例に示すように workdocs オペレーションを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

ユーザーが Launch WorkSpaces ウィザードを使用することも許可するには、次の例に示すように kms オペレーションを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3: BYOL WorkSpaces のすべての WorkSpaces タスクを実行する

次のポリシーステートメントでは、IAM ユーザーに対し、自分のライセンスを使用する (BYOL) WorkSpaces の作成に必要な Amazon EC2 タスクを含む、すべての WorkSpaces タスクを実行するための許可を付与しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
```

```
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

IAM ポリシーで WorkSpaces リソースを指定する

ポリシーステートメントの `Resource` 要素で WorkSpaces リソースを指定するためには、リソースの Amazon リソースネーム (ARN) を使用します。IAM ポリシーステートメントの `Action` 要素に指定された API アクションを使用する許可を許可または拒否することで、WorkSpaces リソースへのアクセスを制御できます。WorkSpaces は、WorkSpaces、バンドル、IP グループ、およびディレクトリの ARN を定義します。

WorkSpace ARN

WorkSpace ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

リージョン

WorkSpace があるリージョン (例: `us-east-1`)。

account_id

ハイフンなしの AWS アカウントの ID (例: `123456789012`)。

workspace_identifier

WorkSpace の ID (例: `ws-a1bcd2efg`) 。

次に示すのは、特定の WorkSpace を識別するポリシーステートメントの `Resource` 要素の形式です。

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

「`*`」ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべての WorkSpace を指定できます。

イメージ ARN

WorkSpace イメージ ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

リージョン

WorkSpace イメージがあるリージョン (例: us-east-1)。

account_id

ハイフンなしの AWS アカウントの ID (例: 123456789012)。

bundle_identifier

WorkSpace イメージの ID (例: wsi-a1bcd2efg)。

次に示すのは、特定のイメージを識別するポリシーステートメントの Resource 要素の形式です。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

「*」ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべてのイメージを指定できます。

バンドル ARN

バンドル ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

リージョン

WorkSpace があるリージョン (例: us-east-1)。

account_id

ハイフンなしの AWS アカウントの ID (例: 123456789012)。

bundle_identifier

WorkSpace バンドルの ID (例: wsb-a1bcd2efg) 。

次に示すのは、特定のバンドルを識別するポリシーステートメントの Resource 要素の形式です。

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

「*」ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべてのバンドルを指定できます。

IP グループ ARN

IP グループ ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

リージョン

WorkSpace があるリージョン (例: us-east-1)。

account_id

ハイフンなしの AWS アカウントの ID (例: 123456789012)。

ipgroup_identifier

IP グループの ID (例: wsipg-a1bcd2efg)。

次に示すのは、特定の IP グループを識別するポリシーステートメントの Resource 要素の形式です。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

「*」ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべての IP グループを指定できます。

ディレクトリ ARN

ディレクトリ ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

リージョン

WorkSpace があるリージョン (例: us-east-1)。

account_id

ハイフンなしの AWS アカウントの ID (例: 123456789012)。

directory_identifier

ディレクトリの ID (例: d-12345a67b8)。

次に示すのは、特定のディレクトリを識別するポリシーステートメントの Resource 要素の形式です。

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

「*」ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべてのディレクトリを指定できます。

接続エイリアス ARN

接続エイリアス ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

リージョン

接続エイリアスがあるリージョン (例: us-east-1)。

account_id

ハイフンなしの AWS アカウントの ID (例: 123456789012)。

connectionalias_identifier

接続エイリアスの ID (例: wsca-12345a67b8)。

次に示すのは、特定の接続エイリアスを識別するポリシーステートメントの Resource 要素の形式です。

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

* ワイルドカードを使用して、特定リージョンの特定のアカウントに属するすべての接続エイリアスを指定できます。

リソースレベルのアクセス許可をサポートしない API アクション

リソース ARN は、次の API アクションで指定することはできません。

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

リソースレベルの権限をサポートしていない API アクションの場合は、次の例に示すように、Resource ステートメントを指定する必要があります。

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

共有リソースに対するアカウントレベルの制限をサポートしない API アクション

次の API アクションでは、リソースがアカウントによって所有されていない場合、リソース ARN でアカウント ID を指定することはできません。

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

これらの API アクションでは、アクション対象のリソースをそのアカウントが所有している場合にのみ、リソース ARN でアカウント ID を指定できます。アカウントがリソースを所有していない場合は、次の例に示すように、アカウント ID に * を指定する必要があります。

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

workspaces_DefaultRole ロールを作成する

API を使用してディレクトリを登録する前に、workspaces_DefaultRole という名前のロールが存在していることを確認します。このロールは、高速セットアップによって作成されます。または、AWS Management Console を使用して WorkSpace を起動した場合、特定の AWS リソースにアクセスする許可が Amazon WorkSpaces 自動的に付与されます。このロールが存在しない場合は、以下の手順で作成できます。

workspaces_DefaultRole ロールを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[Roles] を選択します。
3. [ロールの作成] を選択します。
4. [Select type of trusted entity] (信頼できるエンティティのタイプを選択) で、[Another AWS account] (別の アカウント) を選択します。
5. [Account ID] には、ハイフンやスペースを入れずにアカウント ID を入力します。
6. [Options] では、多要素認証 (MFA) を指定しないでください。
7. [Next: Permissions (次へ: アクセス許可)] を選択します。
8. [Attach permissions policies] (許可ポリシーをアタッチ) ページで、AWS 管理ポリシーとして AmazonWorkSpacesServiceAccess と AmazonWorkSpacesSelfServiceAccess を選択します。
9. [許可の境界を設定] では、このロールにアタッチされているポリシーと競合する可能性があるため、アクセス許可の境界を使用しないことをお勧めします。このような競合が発生すると、ロールに必要な特定の許可がブロックされる可能性があります。
10. [次へ: タグ] を選択します。
11. [Add tags (optional)] ページで、必要に応じてタグを追加します。
12. [Next: Review] を選択します。
13. [Review] ページの [Role name] に、**workspaces_DefaultRole** を入力します。

14. (オプション) [ロールの説明] に、説明を入力します。
15. [ロールの作成] を選択します。
16. workspaces_DefaultRole ロールの [Summary] ページで [Trust relationships] タブを選択します。
17. [信頼関係] タブで、[信頼関係の編集] を選択します。
18. [Edit Trust Relationship] ページで、既存のポリシーステートメントを次のステートメントに置き換えます。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. [Update Trust Policy] を選択します。

AmazonWorkSpacesPCAAccess サービスロールを作成する

ユーザーが証明書ベースの認証を使用してログインする前に、AmazonWorkSpacesPCAAccess という名前のロールが存在することを確認する必要があります。このロールは、AWS Management Consoleを使用してディレクトリで証明書ベースの認証を有効にしたときに作成されます。このロールは、ユーザーに代わって AWS Private CA リソースにアクセスすることを Amazon WorkSpaces に許可します。コンソールを使用して証明書ベースの認証を管理していないために、このロールが存在しない場合は、次の手順で作成できます。

AWS CLI を使用して AmazonWorkSpacesPCAAccess サービスロールを作成するには

1. AmazonWorkSpacesPCAAccess.json という名前の JSON ファイルを次の内容で作成します。

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

```
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 必要に応じて AmazonWorkSpacesPCAAccess.json パスを調整し、次の AWS CLI コマンドを実行してサービスロールを作成します。次に、AmazonWorkspacesPCAAccess 管理ポリシーをアタッチします。

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

WorkSpaces 用の AWS 管理ポリシー

AWS 管理ポリシーを使用すると、ユーザー、グループ、ロールへのアクセス許可の追加が、自分でポリシーを作成するよりも簡単になります。チームに必要な許可のみを提供する IAM カスタマー管理ポリシーを作成するには、時間と専門知識が必要です。AWS マネージドポリシーを使用することで、すぐに使用を開始できます。これらのポリシーは、一般的なユースケースを対象範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については、「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 のサービスは、AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの許可を変更することはできません。サービスでは、新しい機能を利用できるようにするために、AWS マネージドポリシーに許可が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは、AWS マネージドポリシーからの許可を削除しないため、ポリシーの更新によって既存の許可が破棄されることはありません。

加えて AWS では、複数のサービスにまたがるジョブ機能のための管理ポリシーもサポートしています。例えば、ReadOnlyAccess AWS 管理ポリシーでは、すべての AWS のサービスおよびリソー

スへの読み取り専用アクセスを許可します。あるサービスで新しい機能を立ち上げる場合は、AWS は、追加された演算とリソースに対し、読み込み専用の許可を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドの「AWSジョブ関数のマネージドポリシー」を参照してください。

AWS 管理ポリシー: AmazonWorkSpacesAdmin

このポリシーは、Amazon WorkSpaces の管理アクションへのアクセスを提供します。以下のアクセス許可が提供されます。

- workspaces – WorkSpaces リソースに対する管理アクションを実行するためのアクセスを許可します。
- kms – KMS キーの一覧へのアクセスと説明、および エイリアスの一覧表示を許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
```

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

AWS マネージドポリシー: AmazonWorkspacesPCAAccess

このマネージドポリシーは、証明書ベースの認証のために AWS アカウントの AWS Certificate Manager Private Certificate Authority (Private CA) リソースへのアクセスを提供します。これは AmazonWorkSpacesPCAAccess ロールに含まれており、次のアクセス許可を提供します。

- `acm-pca` - 証明書ベースの認証を管理するために AWS Private CA へのアクセスを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

AWS 管理ポリシー: AmazonWorkSpacesSelfServiceAccess

このポリシーでは、Amazon WorkSpaces サービスにアクセスして、ユーザーが開始した WorkSpaces セルフサービスアクションを実行できるようにします。これは `workspaces_DefaultRole` ロールに含まれており、次のアクセス許可が付与されます。

- workspaces – ユーザーを対象とした WorkSpace の自己管理機能を利用できるようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS管理ポリシー: AmazonWorkSpacesServiceAccess

このポリシーは、WorkSpaces を起動するための Amazon WorkSpaces サービスへのカスタマーアカウントアクセスを提供します。これは workspaces_DefaultRole ロールに含まれており、次のアクセス許可が付与されます。

- ec2 – ネットワークインターフェイスなど、WorkSpace に関連付けられた Amazon EC2 リソースを管理するためのアクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces による AWS マネージドポリシーの更新

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

変更	説明	日付
the section called “AmazonWorkSpacesAdmin” – Updated policy	WorkSpaces が `workspaces:RestoreWorkspace` アクションを Amazon WorkspacesAdmin マネージドポリシーに追加し、管理者に WorkSpaces を復元するためのアクセス権を付与します。	2023 年 6 月 25 日
the section called “AmazonWorkspacesPCAAccess” - 新しいポリシーを追加しました	WorkSpaces は、証明書ベースの認証を管理するために、AWS Private CA を管理する `acm-pca` アクセス許可をグラントする新しいマネージドポリシーを追加しました。	2022 年 11 月 18 日
WorkSpaces で変更の追跡が開始されました	WorkSpaces が、WorkSpaces マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

Amazon WorkSpaces のコンプライアンスの検証

サードパーティーの監査者は、さまざまな AWS コンプライアンスプログラムの一環として Amazon WorkSpaces のセキュリティとコンプライアンスを評価します。このプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」「」「」を参照してください。

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

WorkSpaces および FedRAMP の詳細については、「 FedRAMP 認証または DoD SRG 準拠のために Amazon WorkSpaces をセットアップする 」を参照してください。

WorkSpaces を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- 「セキュリティとコンプライアンスのクイックスタートガイド」「」 – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、AWS でセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするためのステップが記載されています。
- 「Architecting for HIPAA Security and Compliance on Amazon Web Services」(Amazon Web Services での HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ) – このホワイトペーパーは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法を説明しています。
- AWSコンプライアンスのリソース– このワークブックおよびガイドのコレクションは、お客様の業界と拠点に適用されるものである場合があります。
- AWS Configデベロッパーガイドのルールでのリソースの評価 – AWS Configは、リソース設定が、社内のプラクティス、業界のガイドラインそして規制にどの程度適合しているのかを評価します。
- AWS Security Hub– AWSのこのサービスは、 AWS内でのユーザーのセキュリティ状態に関する包括的な見解を提供し、業界のセキュリティ標準、およびベストプラクティスに対するコンプライアンスを確認するために役立ちます。

Amazon WorkSpaces の耐障害性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく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、および拡張性が優れています。

AWS リージョンと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。

Amazon WorkSpaces は、クロスリージョンリダイレクトも提供します。これは、ドメインネームシステム (DNS) フェイルオーバールーティングポリシーと連携して、プライマリ WorkSpaces が利用

できない場合に WorkSpaces ユーザーを別の AWS リージョン内の別の WorkSpaces にリダイレクトする機能です。詳細については、「Amazon のクロスリージョンリダイレクト WorkSpaces」を参照してください。

Amazon WorkSpaces のインフラストラクチャセキュリティ

マネージドサービスである Amazon WorkSpaces は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWS クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 - AWS Well-Architected Framework」の「インフラストラクチャ保護」を参照してください。

AWS が発行している APIコールを使用して、ネットワーク経由で WorkSpaces にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時セキュリティ認証情報を生成し、リクエストに署名することもできます。

ネットワークの隔離

仮想プライベートクラウド (VPC) は、AWS クラウド内の論理的に隔離された領域にある仮想ネットワークです。VPC のプライベートサブネットに WorkSpaces をデプロイできます。詳細については、「の VPC を設定する WorkSpaces」を参照してください。

特定のアドレス範囲 (企業ネットワークなど) からのトラフィックのみを許可するには、VPC のセキュリティグループを更新するか、IP アクセスコントロールグループを使用します。

有効な証明書を使用して、信頼できるデバイスへの WorkSpace アクセスを制限できます。詳細については、「信頼できるデバイス WorkSpaces へのアクセスを制限する」を参照してください。

物理ホストでの分離

同じ物理ホスト上の異なる WorkSpaces は、ハイパーバイザーを介して互いに分離されます。これは、別々の物理ホスト上にあるかのようになります。WorkSpace が削除されると、割り当てられたメモリがハイパーバイザーによってスクラブ (ゼロに設定) されてから、新しい WorkSpace に割り当てられます。

企業ユーザーの承認

WorkSpaces では、ディレクトリは AWS Directory Service を介して管理されます。ユーザー用のスタンドアロンのマネージド型ディレクトリを作成できます。または、既存の Active Directory 環境と統合することもできます。統合した場合、ユーザーは現在の認証情報を使用して社内リソースにシームレスにアクセスできます。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。

WorkSpaces へのアクセスをさらに制御するには、多要素認証を使用します。詳細については、「 AWS サービスの多要素認証を有効にする方法」を参照してください。

VPC インターフェイスエンドポイント経由で Amazon WorkSpaces API リクエストを行う

インターネット経由で接続するのではなく、Virtual Private Cloud (VPC) のインターフェイスエンドポイントを通じて Amazon WorkSpaces API エンドポイントに直接接続できます。VPC インターフェイスエンドポイントを使用すると、AWS ネットワーク内で VPC と Amazon WorkSpaces API エンドポイント間の通信が完全かつ安全に実施されます。

> **Note**
>
> この機能は、WorkSpaces API エンドポイントへの接続にのみ使用できます。WorkSpaces クライアントを使用して WorkSpaces に接続するには、「の IP アドレスとポートの要件 WorkSpaces」で説明されているように、インターネット接続が必要です。

Amazon WorkSpaces API エンドポイントでは、Amazon Virtual Private Cloud (Amazon VPC) インターフェイスエンドポイントがサポートされています。このエンドポイントは、AWS PrivateLink を使用します。各 VPC エンドポイントは VPC サブネットの 1 つ以上のネットワークインスタンス (別名: Elastic Network Interface (ENI)) とプライベート IP アドレスで表されます。

VPC インターフェイスエンドポイントは VPC を Amazon WorkSpaces API エンドポイントに直接接続します。その際、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用しません。VPC のインスタンスは、パブリック IP アドレスがなくても Amazon WorkSpaces API エンドポイントと通信できます。

インターフェイスエンドポイントを作成し、AWS Management Console または AWS Command Line Interface (AWS CLI) コマンドのいずれかを使用して、Amazon WorkSpaces と接続できます。手順については、「インターフェイスエンドポイントの作成」を参照してください。

VPC エンドポイントを作成すると、endpoint-url パラメータを使用して、Amazon WorkSpaces API エンドポイントへのインターフェイスエンドポイントを指定する次のサンプル CLI コマンドを使用できます。

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

VPC エンドポイントのプライベート DNS ホスト名を有効にした場合は、エンドポイント URL を指定する必要はありません。CLI および Amazon WorkSpaces SDK がデフォルトで使用する Amazon WorkSpaces API DNS ホスト名 (https://api.workspaces.*Region*.amazonaws.com) は、ご自身の VPC エンドポイントに解決されます。

Amazon WorkSpaces API エンドポイントは、すべてのAWS両方Amazon VPCおよびAmazon WorkSpacesが利用不可。Amazon WorkSpaces では、すべてのパブリック APIを VPC 内に配置します。

AWS PrivateLink の詳細については、AWS PrivateLink ドキュメントを参照してください。VPC エンドポイントの料金については、「VPC の料金」を参照してください。VPC およびエンドポイントの詳細については、「Amazon VPC」を参照してください。

リージョンごとの Amazon WorkSpaces API エンドポイントのリストについては、「WorkSpaces API エンドポイント」を参照してください。

> **Note**
>
> AWS PrivateLink がある Amazon WorkSpaces API エンドポイントは、連邦情報処理規格 (Federal Information Processing Standards/FIPS)Amazon WorkSpaces API エンドポイントではサポートされません。

Amazon WorkSpaces の VPC エンドポイントポリシーの作成

Amazon WorkSpaces の Amazon VPC エンドポイントに対するポリシーを作成して、以下を指定することができます。

- アクションを実行できるプリンシパル。
- 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、『Amazon VPC ユーザーガイド』の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

> **Note**
>
> VPC エンドポイントポリシーは、連邦情報処理規格 (Federal Information Processing Standards/FIPS)Amazon WorkSpaces エンドポイントではサポートされません。

次の例の VPC エンドポイントポリシーでは、VPC インターフェイスエンドポイントにアクセスできるすべてのユーザーが、Amazon WorkSpaces でホストされた、`ws-f9abcdefg` という名前のエンドポイントを呼び出すことが許可されます。

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
```

```
    ]
}
```

この例では、以下のアクションが拒否されます。

- 以外の Amazon WorkSpaces でホストされたエンドポイントの呼び出し`ws-f9abcdefg`。
- 指定された 1 つのリソース (WorkSpace ID: `ws-f9abcdefg`) 以外のリソースに対するアクションの実行。

> **Note**
>
> この例では、ユーザーは VPC の外部からその他の Amazon WorkSpaces API アクションをまだ実行できます。API コールを VPC 内部からに制限するには、ID ベースポリシーを使用して API エンドポイントへのアクセスを制御する方法について「 WorkSpaces の Identity and Access Management 」を参照してください。

プライベートネットワークを VPC に接続する

VPC 経由で Amazon WorkSpaces API を呼び出すには、VPC 内にあるインスタンスから接続するか、Amazon Virtual Private Network (VPN) AWS Virtual Private Network (AWS VPN) または AWS Direct Connect を使用してプライベートネットワークを VPC に接続する必要があります。Amazon VPN については、Amazon Virtual Private Cloud ユーザーガイドの「VPN 接続」を参照してください。AWS Direct Connect の詳細については、AWS Direct Connect ユーザーガイドの「コネクションの作成」を参照してください。

での更新管理 WorkSpaces

のオペレーティングシステムとアプリケーションに定期的にパッチを適用、更新、保護することをお勧めします WorkSpaces。は、通常のメンテナンスウィンドウ中に によって WorkSpaces 更新 WorkSpaces されるように設定することも、自分で更新することもできます。詳細については、「WorkSpace のメンテナンス」を参照してください。

上のアプリケーションの場合 WorkSpaces、提供されている任意の自動更新サービスを使用するか、アプリケーションベンダーが提供する更新のインストールに関する推奨事項に従うことができます。

WorkSpaces 問題のトラブルシューティング

以下の情報は、 に関する問題のトラブルシューティングに役立ちます WorkSpaces。

高度なログ記録の有効化

ユーザーが経験する可能性のある問題のトラブルシューティングに役立つように、任意の Amazon WorkSpaces クライアントで高度なログ記録を有効にできます。

高度なログ記録では、診断情報とデバッグレベルの詳細 (詳細なパフォーマンスデータなど) を含むログファイルが生成されます。1.0 以降および 2.0 以降のクライアントの場合、これらの高度なログファイルは のデータベースに自動的にアップロードされます AWS。

> **Note**
>
> 高度なログファイル AWS の確認や、 WorkSpaces クライアントに関する問題のテクニカルサポートを受けるには、 にお問い合わせください AWS Support。詳細については、AWS Support センターを参照してください。

Web Access で高度なログ記録を有効にするには

Web Access で高度なログ記録を有効にするには

1. Amazon WorkSpaces Web Access クライアントを開きます。
2. WorkSpaces サインインページの上部で、診断ログ を選択します。
3. ポップアップダイアログボックスで、[診断ログ] が有効になっていることを確認します。
4. [ログレベル] で [高度なログ記録] を選択します。

Google Chrome、Microsoft Edge、および Firefox でログファイルにアクセスするには

1. ブラウザでコンテキスト (右クリック) メニューを開くか、キーボードの Ctrl + Shift + I (Mac の場合は command + option + I) を押して、開発者ツールパネルを開きます。
2. 開発者ツールパネルで、[コンソール] タブを選択してログファイルを見つけます。

Safari でログファイルにアクセスするには

1. [Safari]、[設定] の順に選択します。
2. [設定] セクションで、[詳細] を選択します。
3. [メニューバーに "開発" メニューを表示] を選択します。
4. メニューバーの [開発] タブから、[開発] > [Web インスペクターを表示] を選択します。
5. Safari の [Web インスペクター] パネルで、[コンソール] タブを選択してログファイルを見つけます。

4.0 以上のクライアントで高度なログ記録を有効にするには

Windows クライアントのログは、次の場所に保存されています。

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. コマンドプロンプトアプリを開きます。
3. `-l3` フラグを使用して WorkSpaces クライアントを起動します。

   ```
   c:

   cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > WorkSpaces がすべてのユーザーではなく 1 人のユーザーにインストールされている場合は、次のコマンドを使用します。
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

macOS クライアントのログは次の場所に保存されます。

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

macOS クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   open -a workspaces --args -l3
   ```

Android くらいで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. Android クライアントメニューを開きます。
3. [Support] (サポート) を選択します。
4. [Logging settings] (ログ記録設定) を選択します。
5. [Enable advanced logging] (高度なログ記録の有効化) を選択します。

高度なログを有効にした後に Android クライアントのログを取得するには

- [Extract log] (ログの抽出) をクリックして、圧縮したログをローカルに保存します。

Linux クライアントのログは、次の場所に保存されます。

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Linux クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

3.0 以上のクライアントで高度なログ記録を有効にするには

Windows クライアントのログは、次の場所に保存されています。

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. コマンドプロンプトアプリを開きます。
3. `-l3` フラグを使用して WorkSpaces クライアントを起動します。

   ```
   c:

   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > WorkSpaces がすべてのユーザーではなく 1 人のユーザーにインストールされている場合は、次のコマンドを使用します。
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

macOS クライアントのログは次の場所に保存されます。

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

macOS クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   open -a workspaces --args -l3
   ```

Android くらいで高度な口グ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. Android クライアントメニューを開きます。
3. [Support] (サポート) を選択します。
4. [Logging settings] (口グ記録設定) を選択します。
5. [Enable advanced logging] (高度な口グ記録の有効化) を選択します。

高度な口グを有効にした後に Android クライアントの口グを取得するには

- [Extract log] (口グの抽出) をクリックして、圧縮した口グをローカルに保存します。

Linux クライアントの口グは、次の場所に保存されます。

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Linux クライアントで高度な口グ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 次のコマンドを実行します。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

1.0 以上および 2.0 以上のクライアントで高度な口グ記録を有効にするには

1. WorkSpaces クライアントを開きます。
2. クライアントアプリケーションの右上隅にある歯車アイコンを選択します。
3. [Advanced Settings (詳細設定)] を選択します。
4. [Enable Advanced Logging (高度な口グ記録を有効にする)] チェックボックスをオンにします。
5. [Save] (保存) を選択します。

Windows クライアントの口グは、次の場所に保存されています。

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

macOS クライアントのログは次の場所に保存されます。

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

固有の問題のトラブルシューティング

以下の情報は、 に関する特定の問題のトラブルシューティングに役立ちます WorkSpaces。

問題

- ユーザー名に無効な文字 WorkSpace があるため、Amazon Linux を作成できません
- Amazon Linux のシェルを変更しました WorkSpace が、PCoIP セッションをプロビジョニングできません
- Amazon Linux WorkSpaces が起動しない
- 接続されたディレクトリ WorkSpaces での の起動が失敗することが多い
- 内部エラーで起動が WorkSpaces 失敗する
- ディレクトリを登録しようとすると、登録が失敗し、ディレクトリが ERROR 状態のままになります
- ユーザーがインタラクティブなログオンバナー WorkSpace で Windows に接続できない
- ユーザーが Windows に接続できない WorkSpace
- ユーザーが WorkSpaces Web Access WorkSpaces から にログオンしようとすると問題が発生する
- Amazon WorkSpaces クライアントは、ログイン画面に戻る前にしばらくの間、灰色の「ロード中」画面を表示します。他のエラーメッセージは表示されない。
- ユーザーにWorkSpace 「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。
- ユーザーに「このデバイスは へのアクセスを許可されていません WorkSpace。Please contact your administrator for assistance.」というメッセージが表示される。
- ユーザーが WSP WorkSpace に接続しようとすると、「ネットワークがありません。ネットワーク接続が失われました ネットワーク接続を確認するか、管理者に問い合わせてください。」 WSP に接続しようとする場合 WorkSpace
- WorkSpaces クライアントはユーザーにネットワークエラーを与えますが、デバイスで他のネットワーク対応アプリケーションを使用できます
- WorkSpace ユーザーに「デバイスは登録サービスに接続できません。ネットワーク設定を確認してください」というエラーが表示されます。

- PCoIP ゼロクライアントユーザーに、「指定された証明書はタイムスタンプのために無効です」というエラーが表示される
- PCoIP ゼロクライアントで USB プリンタと他の USB 周辺機器が動作しない
- ユーザーが Windows または macOS クライアントアプリケーションの更新をスキップしても、最新バージョンをインストールするように求められない
- ユーザーが Chromebook に Android クライアントアプリケーションをインストールできない
- ユーザーに招待 E メールまたはパスワードリセット E メールが届かない
- クライアントのログイン画面でユーザーに [パスワードを忘れた場合] が表示されません。
- Windows にアプリケーションをインストールしようとすると、「システム管理者は、このインストールを防ぐためのポリシーを設定しています」というメッセージが表示されます。 WorkSpace
- ディレクトリ WorkSpaces にインターネットに接続できない
- WorkSpace インターネットアクセスを失った
- オンプレミスディレクトリに接続しようとすると、「DNS unavailable」というエラーが表示される
- オンプレミスディレクトリに接続しようとすると、「Connectivity issues detected」というエラーが表示される
- オンプレミスディレクトリに接続しようとすると、「SRV record」というエラーが表示される
- Windows WorkSpace がアイドル状態のままになるとスリープ状態になる
- の 1 つの状態 WorkSpaces が UNHEALTHY
- WorkSpace が予期せずクラッシュまたは再起動している
- 同じユーザー名に複数の がありますが WorkSpace、ユーザーは の 1 つのみにログインできます。 WorkSpaces
- Amazon での Docker の使用に問題がある WorkSpaces
- 一部の API コールに ThrottlingException エラーが表示される
- バックグラウンドで実行させると切断 WorkSpace し続けます
- SAML 2.0 フェデレーションが動作していません。ユーザーに WorkSpaces デスクトップをストリーミングする権限がありません。
- ユーザーは 60 分ごとに WorkSpaces セッションから切断されます。
- ユーザーが SAML 2.0 ID プロバイダー (IdP) 開始フローを使用してフェデレーションすると、リダイレクト URI エラーが発生します。または、IdP にフェデレーションした後にユーザーがクライ

アントからサインインしようとするたびに、 WorkSpaces クライアントアプリケーションの追加のインスタンスが開始されます。

- ユーザーが「Something went wrong: An error occurred while launching your " WorkSpacewhen they attempt to sign in to the WorkSpaces client application after federating to the IdP」というメッセージを受信しました。
- ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインインしようとすると、「タグを検証できません」というメッセージが表示されます。
- 「The client and the server cannot communicate, because they do not possess a common algorithm」(クライアントとサーバーは共通のアルゴリズムを所有していないため、通信できません) というメッセージがユーザーに表示されます。
- マイクまたはウェブカメラが Windows で動作していません WorkSpaces。
- ユーザーは証明書ベースの認証を使用してログインできず、デスクトップセッションに接続すると、 WorkSpaces クライアントまたは Windows サインオン画面でパスワードの入力を求められます。
- Windows インストールメディアを必要とするが、提供 WorkSpaces していないことをしようとしている。
- サポートされていない WorkSpaces リージョンで作成された既存の AWS Managed Directory WorkSpaces で を起動したい。
- Amazon Linux 2 で Firefox をアップデートしたいと考えています。
- ユーザーは、 で設定されたきめ細かなパスワードポリシー (FFGP) 設定を無視して、WorkSpaces クライアントを使用してパスワードをリセットできます AWS Managed Microsoft AD。
- ユーザーに「この OS/プラットフォームは、ウェブアクセス WorkSpace を使用して Windows/Linux にアクセスしようとする WorkSpaceと、 にアクセスする権限がありません」というエラーメッセージが表示される

ユーザー名に無効な文字 WorkSpace があるため、Amazon Linux を作成できません

Amazon Linux の場合 WorkSpaces、ユーザー名：

- 最大 20 文字を含めることができます。
- UTF-8 で表現可能な文字、スペース、および数字を含めることができます。

- 次の特殊文字を含めることができます: _.-#
- ダッシュ記号 (-) をユーザー名の 1 文字目として使用することはできません。

> **Note**
>
> これらの制限は Windows には適用されません WorkSpaces。Windows では、ユーザー名のすべての文字に対して @ および - 記号 WorkSpaces がサポートされています。

Amazon Linux のシェルを変更しました WorkSpace が、PCoIP セッションをプロビジョニングできません

Linux のデフォルトシェルを上書きするには WorkSpaces、「」を参照してくださいAmazon Linux のデフォルトシェルを上書きする WorkSpaces。

Amazon Linux WorkSpaces が起動しない

2020 年 7 月 20 日以降、Amazon Linux WorkSpaces は新しいライセンス証明書を使用します。これらの新しい証明書は、PCoIP エージェントの 2.14.1.1、2.14.7、2.14.9、および 20.10.6以降のバージョンでのみ互換性があります。

サポートされていないバージョンの PCoIP エージェントを使用している場合は、最新のバージョン (20.10.6) にアップグレードする必要があります。このバージョンでは、新しい証明書と互換性のある最新の修正とパフォーマンスが向上できます。7 月 20 日までにこれらのアップグレードを行わないと、Linux のセッションプロビジョニング WorkSpaces は失敗し、エンドユーザーは に接続できなくなります WorkSpaces。

PCoIP エージェントを最新バージョンにアップグレードするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、 を選択しますWorkSpaces。
3. Linux を選択し WorkSpace、アクション 、再起動 を選択して再起動 WorkSpacesします。WorkSpace ステータスが の場合はSTOPPED、アクション 、最初に開始 WorkSpaces を選択し、ステータスが になるまで待ってからAVAILABLE再起動する必要があります。
4. WorkSpace が再起動し、ステータスが になったらAVAILABLE、このアップグレードの実行ADMIN_MAINTENANCE中に のステータス WorkSpace を に変更することをお勧めします。完

了したら、 のステータスを WorkSpace に変更しますAVAILABLE。ADMIN_MAINTENANCE モードの詳細については、「手動メンテナンス」を参照してください。

のステータスを WorkSpace に変更するにはADMIN_MAINTENANCE、次の手順を実行します。

a. WorkSpace を選択し、アクション 、 の変更 WorkSpaceを選択します。
b. [Modify State (状態の変更)] を選択します。
c. [想定される状態] で、[ADMIN_MAINTENANCE] を選択します。
d. [Modify] を選択します。

5. SSH WorkSpace を使用して Linux に接続します。詳細については、「Linux の SSH 接続を有効にする WorkSpaces」を参照してください。
6. PCoIP エージェントを更新するには、次のコマンドを実行します。

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. エージェントのバージョンを確認し、更新が成功したことを確認するには、次のコマンドを実行します。

```
rpm -q pcoip-agent-standard
```

検証コマンドは、次の結果を生成する必要があります。

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. から切断し WorkSpace 、再度再起動します。
9. で のステータス WorkSpace を ADMIN_MAINTENANCE に設定する場合はStep 4、 を繰り返しStep 4て、目的の状態を に設定しますAVAILABLE。

PCoIP エージェントのアップグレード後も Linux の起動に WorkSpace 失敗する場合は、 AWS サポートにお問い合わせください。

接続されたディレクトリ WorkSpaces での の起動が失敗することが多い

オンプレミスのディレクトリの 2 つの DNS サーバーまたはドメインコントローラーが、ディレクトリに接続したときに指定した各サブネットからアクセス可能であることを確認します。各サブネットでAmazon EC2 インスタンスを起動し、2 つの DNS サーバーの IP アドレスを使用してディレクトリにインスタンスを結合することで、この接続を確認できます。

内部エラーで起動が WorkSpaces 失敗する

サブネットが、サブネット内で起動されたインスタンスに IPv6 アドレスを自動的に割り当てるように設定されているかどうかを確認します。この設定を確認するには、Amazon VPC コンソールを開き、サブネットを選択し、[Subnet Actions] を選択して、次に [Modify auto-assign IP settings] を選択します。この設定が有効になっている場合、パフォーマンスバンドルまたはグラフィックスバンドル WorkSpaces を使用して を起動することはできません。代わりに、この設定を無効にし、インスタンスを起動するときに IPv6 アドレスを手動で指定します。

ディレクトリを登録しようとすると、登録が失敗し、ディレクトリが ERROR 状態のままになります

この問題は、マルチリージョンレプリケーション用に設定された AWS Managed Microsoft AD ディレクトリを登録しようとしている場合に発生する可能性があります。プライマリリージョンのディレクトリは Amazon で使用するために正常に登録できますが WorkSpaces、レプリケートされたリージョンにディレクトリを登録しようとすると失敗します。 AWS Managed Microsoft AD によるマルチリージョンレプリケーションは、レプリケートされたリージョン WorkSpaces 内の Amazon での使用はサポートされていません。

ユーザーがインタラクティブなログオンバナー WorkSpace で Windows に接続できない

インタラクティブログオンメッセージを実装してログオンバナーを表示している場合、ユーザーは Windows にアクセスできなくなります WorkSpaces。インタラクティブログオンメッセージグループポリシー設定は、現在 PCoIP WorkSpacesではサポートされていません。 WorkSpaces グループポリシーが適用されていない組織単位 (OU) に Interactive logon: Message text for users attempting to log on を移動します。ログオンメッセージは WSP でサポートされており WorkSpaces、ユーザーはログオンバナーを受け入れた後に再度ログインする必要があります。

ユーザーが Windows に接続できない WorkSpace

ユーザーが Windows に接続しようとすると、次のエラーが表示されます WorkSpaces。

```
"An error occurred while launching your WorkSpace. Please try again."
```

このエラー WorkSpace は、 が PCoIP を使用して Windows デスクトップをロードできない場合によく発生します。以下をチェックしてください:

- このメッセージは、Windows 向けの PCoIP Standard Agent サービスが実行されていない場合に表示されます。RDP を使用して接続し、サービスが実行されていること、サービスが自動的に開始されるように設定されていること、および管理インターフェイス (eth0) 経由で通信できることを確認します。

- PCoIP エージェントをアンインストールした場合は、Amazon WorkSpaces コンソール WorkSpace から を再起動して自動的に再インストールします。

- また、WorkSpacesセキュリティグループがアウトバウンドトラフィックを制限するように変更された場合、長時間の遅延後に Amazon WorkSpaces クライアントでこのエラーが表示されることがあります。送信トラフィックを制限すると、Windows はディレクトリコントローラーと通信してログインできなくなります。セキュリティグループが、プライマリネットワークインターフェイスを介して、必要なすべてのポートでディレクトリコントローラーとの通信 WorkSpaces を に許可していることを確認します。

このエラーの別の原因として、ユーザー権利の割り当てグループポリシーに関連がある場合があります。次のグループポリシーが正しく設定されていない場合、ユーザーは Windows にアクセスできなくなります WorkSpaces。

コンピュータ構成\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- 正しくないポリシー:

  ポリシー: ネットワークからこのコンピュータにアクセスする

  設定: #####\ドメインコンピュータ

  優先される GPO: ファイルアクセスを許可する
- 正しいポリシー:

  ポリシー: ネットワークからこのコンピュータにアクセスする

  設定: #####\ドメインユーザー

  優先される GPO: ファイルアクセスを許可する

> **Note**
>
> このポリシー設定は、ドメインコンピュータの代わりにドメインユーザーに適用する必要があります。

詳細については、Microsoft Windows のドキュメントの「ネットワークセキュリティポリシーの設定からこのコンピュータにアクセスする」および「セキュリティポリシー設定を構成する」を参照してください。

ユーザーが WorkSpaces Web Access WorkSpaces から にログオンしようとすると問題が発生する

Amazon WorkSpaces は、ユーザーが Web Access クライアントから正常にログオンできるように、特定のログオン画面設定に依存しています。

Web Access ユーザーが にログオンできるようにするには WorkSpaces、グループポリシー設定と 3 つのセキュリティポリシー設定を設定する必要があります。これらの設定が正しく設定されていない場合、ユーザーが にログオンしようとすると、ログオン時間が長くなり、画面が黒くなることがあります WorkSpaces。これらの設定を構成するには、「Amazon WorkSpaces Web Access の有効化と設定」を参照してください。

> **Important**
>
> 2020 年 10 月 1 日以降、お客様は Amazon WorkSpaces Web Access クライアントを使用して Windows 7 カスタム WorkSpaces または Windows 7 Bring Your Own License (BYOL) に接続できなくなります WorkSpaces。

Amazon WorkSpaces クライアントは、ログイン画面に戻る前にしばらくの間、灰色の「ロード中」画面を表示します。他のエラーメッセージは表示されない。

この動作は通常、 WorkSpaces クライアントがポート 443 経由で認証できるが、ポート 4172 (PCoIP) またはポート 4195 (WSP) 経由でストリーミング接続を確立できないことを示します。この状況は、ネットワークの前提条件が満たされていない場合に発生する可能性があります。クライアント側の問題により、クライアントでのネットワークチェック

が失敗することがよくあります。どのヘルスチェックが失敗しているかを確認するには、ネットワークチェックアイコン (通常、2.0+ クライアントのログイン画面の右下隅に感嘆符が付いた赤い三角形、または 3.0+ クライアントの右上隅にあるネットワークアイコン

)

を選択します。

> **Note**
>
> この問題の最も一般的な原因は、クライアント側のファイアウォールまたはプロキシがポート 4172 または 4195 (TCP および UDP) 経由のアクセスを防止していることです。このヘルスチェックが失敗した場合は、ローカルのファイアウォール設定を確認してください。

ネットワークチェックに合格すると、 のネットワーク設定に問題がある可能性があります WorkSpace。たとえば、Windows ファイアウォールの規則により、管理インターフェイス上のポート UDP 4172 または 4195 がブロックされる場合があります。リモートデスクトッププロトコル (RDP) クライアント WorkSpace を使用して に接続し、 WorkSpace が必要なポート要件を満たしていることを確認します。

ユーザーにWorkSpace 「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。

このエラーは通常、 SkyLightWorkSpacesConfigService サービスがヘルスチェックに応答していないことを示します。

を再起動または開始したばかりの場合は WorkSpace、数分待ってからもう一度試してください。

WorkSpace がしばらく実行されていてもこのエラーが表示される場合は、RDP を使用して接続し、SkyLightWorkSpacesConfigService サービスが次のことを確認します。

- 実行中である。
- 自動的に開始するように設定されている。
- 管理インターフェイス (eth0) を介して通信できる。

- サードパーティー製のウイルス対策ソフトウェアによってブロックされていない。

ユーザーに「このデバイスは へのアクセスを許可されていません WorkSpace。Please contact your administrator for assistance.」というメッセージが表示される。

このエラーは、IP アクセスコントロールグループが WorkSpace ディレクトリに設定されているが、クライアントの IP アドレスが許可リストに登録されていないことを示します。

ディレクトリの設定を確認します。ユーザーが接続しているパブリック IP アドレスが へのアクセスを許可していることを確認します WorkSpace。

ユーザーが WSP WorkSpace に接続しようとすると、「ネットワークがありません。ネットワーク接続が失われました ネットワーク接続を確認するか、管理者に問い合わせてください。」 WSP に接続しようとする場合 WorkSpace

このエラーが発生したが、ユーザーに接続の問題が発生していない場合は、ネットワークのファイアウォールでポート 4195 が開いていることを確認してください。 WorkSpaces ストリーミングプロトコル (WSP) WorkSpaces を使用する場合、クライアントセッションのストリーミングに使用されるポートが 4172 から 4195 に変更されました。

WorkSpaces クライアントはユーザーにネットワークエラーを与えますが、デバイスで他のネットワーク対応アプリケーションを使用できます

WorkSpaces クライアントアプリケーションは AWSクラウド内のリソースへのアクセスに依存しており、少なくとも 1 Mbps のダウンロード帯域幅を提供する接続が必要です。デバイスにネットワークへの断続的な接続がある場合、 WorkSpaces クライアントアプリケーションはネットワークの問題を報告する可能性があります。

WorkSpaces は、2018 年 5 月の時点で Amazon Trust Services によって発行されたデジタル証明書の使用を強制します。Amazon Trust Services は、 でサポートされているオペレーティングシステムで既に信頼されたルート CA です WorkSpaces。オペレーティングシステムのルート CA リストが最新でない場合、デバイスは に接続できず WorkSpaces 、クライアントはネットワークエラーを表示します。

証明書の失敗による接続の問題を認識するには

- PCoIP ゼロクライアント - 次のエラーメッセージが表示されます。

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- その他のクライアント – ヘルスチェックは、インターネットの赤い三角形の警告が表示されて失敗します。

証明書の失敗を解決するには

- Windows クライアントアプリケーション
- PCoIP ゼロクライアント
- その他のクライアントアプリケーション

Windows クライアントアプリケーション

証明書が失敗した場合は、次のいずれかの解決策を使用します。

解決策 1: クライアントアプリケーションを更新する

https://clients.amazonworkspaces.com/. から最新の Windows 。クライアントアプリケーションは、インストール中に、Amazon Trust Services によって発行された証明書をオペレーティングシステムが信頼するようにします。

解決策 2: Amazon Trust Services をローカルのルート CA リストに追加する

1. https://www.amazontrust.com/repository/ を開きます。
2. DER 形式の Starfield 証明書 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) をダウンロードします。
3. Microsoft マネジメントコンソールを開きます。 (コマンドプロンプトから、mmc を実行します。)
4. [ファイル]、[スナップインの追加と削除]、[証明書]、[追加] の順に選択します。

5. [証明書スナップイン] ページで、[コンピュータ アカウント] を選択し、[次へ] を選択します。デフォルトの [ローカル コンピュータ] のままにします。[Finish] を選択します。[OK] をクリックします。
6. [証明書 (ローカル コンピュータ)] を展開し、[信頼されたルート証明機関] を選択します。[アクション]、[すべてのタスク]、[インポート] の順に選択します。
7. ウィザードに従って、ダウンロードした証明書をインポートします。
8. WorkSpaces クライアントアプリケーションを終了して再起動します。

解決策 3: グループポリシーを使用して Amazon Trust Services を信頼された CA としてデプロイする

グループポリシーを使用して、ドメインの信頼されたルート CA に Starfield 証明書を追加します。詳細については、「Use Policy to Distribute Certificates」を参照してください。

PCoIP ゼロクライアント

ファームウェアバージョン 6.0 以降 WorkSpace を使用して に直接接続するには、Amazon Trust Services によって発行された証明書をダウンロードしてインストールします。

Amazon Trust Services を信頼されたルート CA として追加するには

1. https://certs.secureserver.net/repository/ を開きます。
2. [Starfield Certificate Chain] で、サムプリント 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 の証明書をダウンロードします。
3. 証明書をゼロクライアントにアップロードします。詳細については、Teradici ドキュメントの「Uploading Certificates」を参照してください。

その他のクライアントアプリケーション

Amazon Trust Services から、Starfield 証明書 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) を追加します。ルート CA の追加方法の詳細については、以下のドキュメントを参照してください。

- Android: 証明書の追加と削除
- Chrome OS: Chrome 端末でのクライアント証明書の管理
- macOS および iOS: Installing a CA's Root Certificate on Your Test Device

WorkSpace ユーザーに「デバイスは登録サービスに接続できません。ネットワーク設定を確認してください」というエラーが表示されます。

登録サービスの障害が発生すると、 WorkSpace 接続ヘルスチェックページに「デバイスが WorkSpaces 登録サービスに接続できない」というエラーメッセージが表示されることがあります。デバイスを に登録することはできません WorkSpaces。ネットワーク設定を確認してください」というエラーメッセージが表示されることがあります。

このエラーは、 WorkSpaces クライアントアプリケーションが登録サービスに到達できない場合に発生します。通常、これは WorkSpaces ディレクトリが削除されたときに発生します。このエラーを解決するには、登録コードが有効で、 AWS クラウドで実行中のディレクトリに対応していることを確認してください。

PCoIP ゼロクライアントユーザーに、「指定された証明書はタイムスタンプのために無効です」というエラーが表示される

Teradici でネットワークタイムプロトコル (NTP) が有効になっていない場合、PCoIP ゼロクライアントユーザーに証明書の失敗エラーが表示されることがあります。NTP を設定するには、「WorkSpaces の PCoIP ゼロクライアントをセットアップする」を参照してください。

PCoIP ゼロクライアントで USB プリンタと他の USB 周辺機器が動作しない

PCoIP エージェントのバージョン 20.10.4 以降、Amazon は Windows レジストリを介した USB リダイレクトをデフォルトで WorkSpaces 無効にします。このレジストリ設定は、ユーザーが PCoIP ゼロクライアントデバイスを使用して に接続している場合の USB 周辺機器の動作に影響します WorkSpaces。

WorkSpaces でバージョン 20.10.4 以降の PCoIP エージェントを使用している場合、USB リダイレクトを有効にするまで、USB 周辺機器は PCoIP ゼロクライアントデバイスでは動作しません。

> **Note**
>
> 32 ビット仮想プリンタードライバーを使用している場合は、それらのドライバーを 64 ビット版に更新する必要があります。

PCoIP ゼロクライアントデバイスの USB リダイレクトを有効にするには

これらのレジストリの変更は、グループポリシー WorkSpaces を通じて にプッシュアウトすることをお勧めします。詳細については、「Teradiciのマニュアル」からエージェントの設定および環境の設定を参照してください。

1. 次のレジストリキーの値を 1 (有効) に設定します。

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP \pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
2. 次のレジストリキーの値を 1 (有効) に設定します。

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP \pcoip_admin_defaults

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
3. まだログアウトしていない場合は、 からログアウト WorkSpaceしてから再度ログインします。これで USB デバイスが動作するはずです。

ユーザーが Windows または macOS クライアントアプリケーションの更新をスキップしても、最新バージョンをインストールするように求められない

ユーザーが Amazon WorkSpaces Windows クライアントアプリケーションの更新をスキップすると、SkipThisバージョンレジストリキーが設定され、クライアントの新しいバージョンがリリースされたときにクライアントを更新するように求められなくなります。最新バージョンに更新するには、「Amazon ユーザーガイド」の WorkSpaces 「Windows クライアントアプリケーションを新しいバージョンに更新する」の説明に従ってレジストリを編集できます。 WorkSpaces 次の PowerShell コマンドを実行することもできます。

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

ユーザーが Amazon WorkSpaces macOS クライアントアプリケーションの更新をスキップすると、SUSkippedVersion設定が設定され、クライアントの新しいバージョンがリリースされたときにクライアントを更新するように求められなくなります。最新バージョンに更新するには、「Amazon WorkSpaces ユーザーガイド」の WorkSpaces macOS クライアントアプリケーションを新しいバージョンに更新する」で説明されているように、この設定をリセットできます。

ユーザーが Chromebook に Android クライアントアプリケーションをインストールできない

バージョン 2.4.13 は、Amazon WorkSpaces Chromebook クライアントアプリケーションの最終リリースです。 Google は Chrome Apps のサポートを段階的に廃止しているため、 WorkSpaces Chromebook クライアントアプリケーションへの更新は行われず、その使用はサポートされていません。

Android アプリケーションのインストールをサポートする Chromebook の場合は、代わりに WorkSpaces Android クライアントアプリケーションを使用することをお勧めします。

場合によっては、ユーザーの Chromebook で Android アプリケーションのインストールを有効にする必要があります。詳細については、「Chromebook 用の Android のセットアップ」を参照してください。

ユーザーに招待 E メールまたはパスワードリセット E メールが届かない

AD Connector または信頼 WorkSpaces されたドメインを使用して作成された のウェルカムまたはパスワードリセット E メールは、ユーザーに自動的に送信されません。また、ユーザーが既に Active Directory に存在する場合も、招待メールは自動的に送信されません。

これらのユーザーに招待 E メールを手動で送信するには、「招待 E メールの送信」を参照してください 。

ユーザーパスワードをリセットするには、「WorkSpaces の Active Directory 管理ツールを設定する」を参照してください。

クライアントのログイン画面でユーザーに [パスワードを忘れた場合] が表示されません。

AD Connector または信頼できるドメインを使用している場合、ユーザーは自分のパスワードをリセットできません。（ WorkSpaces クライアントアプリケーションのログイン画面のパスワードを忘れた場合？ オプションは使用できません。）ユーザーパスワードをリセットする方法については、WorkSpaces の Active Directory 管理ツールを設定する を参照してください。

Windows にアプリケーションをインストールしようとすると、「システム管理者は、このインストールを防ぐためのポリシーを設定しています」というメッセージが表示されます。 WorkSpace

この問題に対処するには、Windows インストーラのグループポリシー設定を変更します。このポリシーをディレクトリ WorkSpaces 内の複数の にデプロイするには、ドメインに参加している EC2 インスタンスから WorkSpaces 組織単位 (OU) にリンクされたグループポリシーオブジェクトにこの設定を適用します。AD Connector を使用している場合は、ドメインコントローラーからこれらの変更を行うことができます。Active Directory 管理ツールを使用してグループポリシーオブジェクトを操作する方法の詳細については、AWS Directory Service 管理ガイドの「Active Directory 管理ツールのインストール」を参照してください。

次の手順は、 WorkSpaces グループポリシーオブジェクトの Windows インストーラ設定を構成する方法を示しています。

1. 最新のWorkSpaces グループポリシー管理テンプレートがドメインにインストールされていることを確認します。
2. Windows WorkSpace クライアントでグループポリシー管理ツールを開き、 WorkSpaces マシンアカウントの WorkSpaces グループポリシーオブジェクトに移動して選択します。メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration (コンピュータの構成)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Classic Administrative Templates (従来の管理用テンプレート)]、[Windows Components (Windows コンポーネント)]、[Windows Installer (Windows インストーラ)] の順に選択します。
4. [Turn Off Windows Installer (Windows インストーラをオフ)] 設定を開きます。
5. [Turn Off Windows Installer (Windows インストーラをオフ)] ダイアログボックスで、[Not Configured (未構成)] を [Enabled (有効)] に変更し、[Disable Windows Installer (Windows インストーラを無効にする] を [Never (しない)] に設定します。

6. [OK] をクリックします。
7. グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace（ WorkSpaces コンソールで を選択し、アクション WorkSpace、再起動 WorkSpaces を選択します ）。
   - 管理コマンドプロンプトから、gpupdate /force と入力します。

ディレクトリ WorkSpaces にインターネットに接続できない

WorkSpaces デフォルトでは、 はインターネットと通信できません。明示的にインターネットアクセスを許可する必要があります。詳細については、「からのインターネットアクセスを提供する WorkSpace」を参照してください。

WorkSpace インターネットアクセスを失った

WorkSpace がインターネットにアクセスできなくなり、RDP WorkSpace を使用して に接続できない場合、この問題はおそらく のパブリック IP アドレスが失われたことが原因と考えられます WorkSpace。ディレクトリレベルで Elastic IP アドレスの自動割り当てを有効にしている場合、起動 WorkSpace 時に (Amazon が提供するプールからの) Elastic IP アドレスが に割り当てられます。ただし、所有している Elastic IP アドレスを に関連付けた後 WorkSpace、その Elastic IP アドレスとの関連付けを解除すると WorkSpace、 はパブリック IP アドレスを WorkSpace 失い、Amazon が提供するプールから新しい IP アドレスを自動的に取得しません。

Amazon が提供するプールの新しいパブリック IP アドレスを に関連付けるには WorkSpace、 を再構築 WorkSpaceする必要があります。を再構築しない場合は WorkSpace、所有している別の Elastic IP アドレスを に関連付ける必要があります WorkSpace。

の WorkSpace 起動後に の Elastic Network Interface WorkSpaceを変更しないことをお勧めします。Elastic IP アドレスが に割り当てられると WorkSpace、 は同じパブリック IP アドレス WorkSpace を保持します (WorkSpace が再構築されない限り、新しいパブリック IP アドレスを取得します ）。

オンプレミスディレクトリに接続しようとすると、「DNS unavailable」というエラーが表示される

オンプレミスディレクトリに接続するときに、次のようなエラーメッセージが表示されます。

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connectorは、ポート 53 上で TCP および UDP によってオンプレミス DNS サーバーと通信できる必要があります。セキュリティグループおよびオンプレミスのファイアウォールが、このポート上の TCP および UDP 通信を許可していることを確認します。

オンプレミスディレクトリに接続しようとすると、「Connectivity issues detected」というエラーが表示される

オンプレミスディレクトリに接続するときに、次のようなエラーメッセージが表示されます。

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connectorは、以下のポート上で TCP および UDP によってオンプレミスドメインコントローラーと通信できる必要があります。セキュリティグループおよびオンプレミスのファイアウォールが、これらのポート上の TCP および UDP 通信を許可していることを確認します。

- 88 (Kerberos)
- 389 (LDAP)

オンプレミスディレクトリに接続しようとすると、「SRV record」というエラーが表示される

オンプレミスディレクトリに接続するときに、次のいずれかまたは複数のエラーメッセージが表示されます。

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

AD Connector は、ディレクトリに接続するときに、_ldap._tcp.*dns-domain-name* および _kerberos._tcp.*dns-domain-name* SRV レコードを取得する必要があります。ディレクトリに接続するときに、サービスが指定された DNS サーバーからこれらのレコードを取得できない場合、このエラーが表示されます。DNS サーバーにこれらの SRV レコードが含まれていることを確認します。詳細については、「Microsoft の SRV リソースレコード」を参照してください TechNet。

Windows WorkSpace がアイドル状態のままになるとスリープ状態になる

この問題を解決するには、 に接続 WorkSpace し、次の手順を使用して電源プランを高パフォーマンスに変更します。

1. から WorkSpaceコントロールパネル を開き、ハードウェア を選択するか、ハードウェアとサウンド を選択します (Windows のバージョンによって名前が異なる場合があります)。
2. [Power Options (電源オプション)] で [Choose a power plan (電源プランを選択)] を選択します。
3. [Choose or customize a power plan] (電力プランの選択あるいはカスタマイズ) ペインで [High performance] (高パフォーマンス) 電力プランを選択し、[Change plan settings] (プラン設定の変更)を選択します。
   - オプションで、[High performance](高パフォーマンス) 電力プランの選択が無効になっている場合は、[現在利用できない設定を変更する] を選択してから、[高パフォーマンス] 電力プランを選択します。
   - そのファイルに[高パフォーマンス]プランが非表示になっている場合は、[追加プランを表示]の右側にある矢印を選択して表示するか、もしくは左のナビゲーションで[電源プランを作成する]から[高パフォーマンス]を選択し、電源プランに名前を付けたうえで、[次へ] を選択します。
4. [プランの設定を変更する:高パフォーマンス]ページでは、[ディスプレイをオフにする]および (利用可能な場合) [コンピュータをスリープ状態にする]などについて[Never](決してしない) を選択してあることを確認してください。
5. 高パフォーマンスプランに変更した場合は、[変更の保存] を選択します。(または新しいプランを作成するのであれば[作成]を選択します)。

上記の手順で問題を解決できない場合は、次の操作を行います。

1. から WorkSpaceコントロールパネル を開き、ハードウェア を選択するか、ハードウェアとサウンド を選択します (Windows のバージョンによって名前が異なる場合があります)。
2. [Power Options (電源オプション)] で [Choose a power plan (電源プランを選択)] を選択します。
3. [Choose or customize a power plan] (電力プランの選択あるいはカスタマイズ) ペインで、[High performance] (高パフォーマンス) 電源プランの右側にある [Change plan settings] (プラン設定の変更) リンクを選択して、[Change advanced power settings] (高度な電源設定の変更) リンクを選択します。
4. 設定リストの [Power Options (電源オプション)] ダイアログボックスで、[Hard disk (ハードディスク)] の左側にあるプラス記号を選択して関連する設定を表示します。

5. [Plugged in (プラグイン)] の [Turn off hard disk after (経過後にハードディスクを切断する)] 値が、[On battery (バッテリー使用時)] よりも大きいことを確認します (デフォルト値は 20 分)。
6. [PCI Express] の左側にあるプラス記号を選択し、[Link State Power Management (ステート電力管理リンク)] でも同様の選択を行います。
7. [Link State Power Management (ステート電力管理リンク)] 設定が [オフ] であることを確認します。
8. [OK] (あるいは、設定を変更した場合には [適用]) を選択して、ダイアログボックスを閉じます。
9. 設定を変更した場合には、[Change settings for the plan (プランの設定変更)] ペインで [変更の保存] を選択します。

の 1 つの状態 WorkSpaces が UNHEALTHY

WorkSpaces サービスは定期的にステータスリクエストを に送信します WorkSpace。 WorkSpace は、これらのリクエストに応答UNHEALTHYできない場合にマークされます。この問題に対する一般的な原因は次のとおりです。

- 上のアプリケーション WorkSpace がネットワークポートをブロックしているため、 WorkSpace はステータスリクエストに応答できません。
- CPU 使用率が高い WorkSpace と、 がステータスリクエストにタイムリーに応答できなくなります。
- のコンピュータ名が変更され WorkSpace ました。これにより、 WorkSpaces と の間で安全なチャネルが確立されなくなります WorkSpace。

次の方法を使用して、この状況を修正するよう試みることができます。

- WorkSpaces コンソール WorkSpace から を再起動します。
- 次の手順 WorkSpace を使用して、異常のある に接続します。これはトラブルシューティングの目的にのみ使用してください。

  1. 異常のある WorkSpace と同じディレクトリ内の オペレーションに接続します WorkSpace。
  2. 運用上の から WorkSpace、リモートデスクトッププロトコル (RDP) を使用して、異常のある の IP アドレス WorkSpace を使用して異常のある に接続します WorkSpace。問題の範囲によっては、異常な に接続できない場合があります WorkSpace。
  3. 異常のある で WorkSpace、最小ポート要件が満たされていることを確認します。

- SkyLightWorkSpacesConfigService サービスがヘルスチェックに応答できることを確認します。この問題のトラブルシューティングについては、「ユーザーにWorkSpace「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。」を参照してください。
- WorkSpaces コンソール WorkSpace から を再構築します。を再構築 WorkSpace するとデータが失われる可能性があるため、このオプションは、問題を修正する他のすべての試行が失敗した場合にのみ使用してください。

WorkSpace が予期せずクラッシュまたは再起動している

PCoIP 用に WorkSpace 設定された が繰り返しクラッシュまたは再起動し、エラーログまたはクラッシュダンプが `spacedeskHookKmode.sys`または の問題を参照している場合`spacedeskHookUmode.dll`、または次のエラーメッセージが表示されている場合は、 へのウェブアクセスを無効にする必要がある場合があります WorkSpace。

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - これらのトラブルシューティング手順は、 WorkSpaces ストリーミングプロトコル (WSP) 用に WorkSpaces 設定された には適用されません。これらは、PCoIP WorkSpaces に設定されている にのみ適用されます。 PCoIP
> - Web Access を無効にするのは、ユーザーに Web Access の使用を許可しない場合だけです。

へのウェブアクセスを無効にするには WorkSpace、 WorkSpaces ディレクトリでウェブアクセスを無効にし、 を再起動する必要があります WorkSpace。

同じユーザー名に複数の がありますが WorkSpace、ユーザーは の 1 つのみにログインできます。 WorkSpaces

最初にユーザーを削除せずに Active Directory (AD) でユーザーを削除し、そのユーザーを Active Directory に再度追加して WorkSpace そのユーザーの新しい を作成する WorkSpace と、同じユーザー名が同じディレクトリ WorkSpaces に 2 つの を持つようになります。ただし、ユーザーが元のに接続しようとすると WorkSpace、次のエラーが表示されます。

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

さらに、Amazon WorkSpaces コンソールでユーザー名を検索すると、両方 WorkSpaces がまだ存在する場合でも WorkSpace、新しい のみが返されます。(ユーザー名の代わりに WorkSpace ID を検索 WorkSpace することで、元の を見つけることができます)。

この動作は、最初に を削除せずに Active Directory でユーザーの名前を変更した場合にも発生する可能性があります WorkSpace。その後、ユーザー名を元のユーザー名に戻し、その WorkSpace ユーザーの新しいユーザー名を作成すると、同じユーザー名が ディレクトリ WorkSpaces に 2 つ含まれます。

この問題は、Active Directory がユーザー名ではなくユーザーのセキュリティ識別子 (SID) を使用してユーザーを一意に識別するために発生します。ユーザーを削除して Active Directory で再作成すると、ユーザー名が同じであっても、そのユーザーに新しい SID が割り当てられます。ユーザー名の検索中、Amazon WorkSpaces コンソールは SID を使用して Active Directory で一致を検索します。また、Amazon WorkSpaces クライアントは SID を使用して、ユーザーが に接続するときにユーザーを識別します WorkSpaces。

この問題を解決するには、以下のいずれかの操作を行います。

- ユーザーが削除されて Active Directory で再作成されたためにこの問題が発生した場合は、Active Directory のごみ箱機能を有効にすると、削除された元のユーザーオブジェクトを復元できる可能性があります。元のユーザーオブジェクトを復元できる場合は、ユーザーが元の に接続できることを確認してください WorkSpace。可能な場合は、手動でバックアップし、ユーザーデータを新しい から元の に転送した後 WorkSpace (必要に応じて)、新しい WorkSpace を削除 WorkSpaceできます。
- 元のユーザーオブジェクトを復元できない場合は、ユーザーの元の を削除します WorkSpace。ユーザーは、 WorkSpace 代わりに新しい に接続して使用できる必要があります。元の から新しい WorkSpace にユーザーデータを手動でバックアップして転送してください WorkSpace。

> **Warning**
>
> の削除 WorkSpace は永続的なアクションであり、元に戻すことはできません。WorkSpace ユーザーのデータは保持されず、破棄されます。ユーザーデータのバックアップに関するヘルプについては、 AWS サポートにお問い合わせください。

Amazon での Docker の使用に問題がある WorkSpaces

Windows WorkSpaces

ネストされた仮想化 (Docker の使用を含む) は Windows ではサポートされていません WorkSpaces。詳細については、「Docker ドキュメント」を参照してください。

Linux WorkSpaces

Linux で Docker を使用するには WorkSpaces、Docker で使用される CIDR ブロックが、 に関連付けられた 2 つの Elastic Network Interface (ENIsで使用される CIDR ブロックと重複しないようにしてください WorkSpace。Linux での Docker の使用で問題が発生した場合は WorkSpaces、Docker にお問い合わせください。

一部の API コールに ThrottlingException エラーが表示される

WorkSpaces API コールのデフォルトの許容レートは 1 秒あたり 2 回の API コールの一定のレートであり、最大許容「バースト」レートは 1 秒あたり 5 回の API コールです。次の表は、API リクエストのバーストレート制限がどのように機能するかを示しています。

秒	送信されたリクエストの数	許可されたネットリクエスト	詳細
1	0	5	最初の 1 秒 (1 秒目) の間は、1 秒あたり最大 5 回の呼び出しのバーストレートまで、5 つのリクエストが許可されます。
2	2	5	1 秒目で発行されたコール数が 2 つ以下であるため、5 つのコールのフルバーストキャパシティーを引き続き利用できます。

秒	送信されたリクエストの数	許可されたネットリクエスト	詳細
3	5	5	2 秒目で発行された呼び出しは 2 つだけであるため、5 つの呼び出しのフルバーストキャパシティーを引き続き利用できます。
4	2	2	バーストキャパシティーが 3 秒目にいっぱいまで使用されたため、1 秒あたり 2 回の呼び出しの一定のレートのみが使用できます。
5	3	2	バースト容量が残っていないため、現時点では許可される呼び出しは 2 つだけです。これは、3 つの API コールの 1 つが調整されることを意味します。1 つの調整された呼び出しは、短い遅延後に応答します。
6	0	1	5 秒目からの呼び出しの 1 つが 6 秒目で再試行されるため、6 秒目の追加の呼び出しは 1 つだけです。これは、1 秒あたり 2 回の呼び出しが一定のレート制限であるためです。
7	0	3	キューに調整された API コールがないため、レート制限はバーストレート制限が 5 回まで引き上げられます。
8	0	5	7 秒目には呼び出しが発行されなかったため、リクエストの最大数が許可されます。
9	0	5	8 秒目には呼び出しが発行されませんが、レート制限は 5 つを超えることはありません。

バックグラウンドで実行させると切断 WorkSpace し続けます

Mac ユーザーの場合は、Power Nap 機能がオンになっていないかどうかをチェックしてください。オンになっている場合は、オフにします。Power Nap をオフにするには、ターミナルを開いて、以下のコマンドを実行します。

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 フェデレーションが動作していません。ユーザーに WorkSpaces デスクトップをストリーミングする権限がありません。

このエラーは、SAML 2.0 フェデレーションの IAM ロール用に埋め込まれているインラインポリシーに、ディレクトリの Amazon リソースネーム (ARN) からストリーミングするためのアクセス許可が含まれていないことが原因で発生する可能性があります。IAM ロールは、 WorkSpaces ディレクトリにアクセスするフェデレーティッドユーザーによって引き受けられます。ロールのアクセス許可を編集してディレクトリ ARN を含め、ユーザーが ディレクトリ WorkSpace に を持っていることを確認します。詳細については、「SAML 2.0 認証」および「 を使用した SAML 2.0 フェデレーションのトラブルシューティング AWS」を参照してください。

ユーザーは 60 分ごとに WorkSpaces セッションから切断されます。

SAML 2.0 認証を に設定している場合 WorkSpaces、ID プロバイダー (IdP) によっては、認証レスポンス AWS の一部として IdP が SAML 属性として渡す情報を設定する必要がある場合があります。これには、[Attribute] 要素の設定として、`SessionDuration` 属性を `https://aws.amazon.com/SAML/Attributes/SessionDuration` に設定することが含まれます。

`SessionDuration` は、再認証が必要となるまでに、ユーザーのフェデレーティッドストリーミングセッションをアクティブにしておくことができる最大時間を指定します。`SessionDuration` はオプションの属性ですが、これを SAML 認証レスポンスに含めることをお勧めします。この属性を指定しない場合、セッション時間はデフォルトで 60 分に設定されます。

この問題を解決するには、SAML 認証レスポンスに `SessionDuration` 値を含めるように IdP を設定し、必要に応じた値を設定します。詳細については、「ステップ 5: SAML 認証レスポンスのアサーションを作成する」を参照してください。

ユーザーが SAML 2.0 ID プロバイダー (IdP) 開始フローを使用してフェデレーションすると、リダイレクト URI エラーが発生します。または、IdP にフェデレーションした後にユーザーがクライアントからサインインしようとするたびに、 WorkSpaces クライアントアプリケーションの追加のインスタンスが開始されます。

このエラーが発生するのは、リレーステートの URL が正しい形式でないためです。IdP フェデレーション設定のリレーステートが正しいこと、および WorkSpaces ディレクトリプロパティの IdP

フェデレーションに対してユーザーアクセス URL とリレーステートパラメータ名が正しく設定されていることを確認します。それらが有効で、問題が解決しない場合は、 AWS サポートにお問い合わせください。詳細については、「SAML のセットアップ」を参照してください。

ユーザーが「Something went wrong: An error occurred while launching your " WorkSpacewhen they attempt to sign in to the WorkSpaces client application after federating to the IdP」というメッセージを受信しました。

フェデレーションの SAML 2.0 アサーションを確認します。SAML サブジェクト NameID 値は WorkSpaces ユーザー名と一致する必要があり、通常は Active Directory ユーザーの sAMAccountName 属性と同じです。さらに、 属性が に設定されている `PrincipalTag:Email` Attribute 要素は、 WorkSpaces ディレクトリで定義されている WorkSpaces ユーザーの E メールアドレスと一致する`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`必要があります。詳細については、「SAML のセットアップ」を参照してください。

ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインインしようとすると、「タグを検証できません」というメッセージが表示されます。

`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email` など、フェデレーションの SAML 2.0 アサーションの `PrincipalTag` 属性値を確認します。タグ値には、`_ . : / = + - @` の各文字、英数字、およびスペースの組み合わせを含めることができます。詳細については、「IAM でのタグ付けのルール」および AWS STS「」を参照してください。

「The client and the server cannot communicate, because they do not possess a common algorithm」(クライアントとサーバーは共通のアルゴリズムを所有していないため、通信できません) というメッセージがユーザーに表示されます。

この問題は、TLS 1.2 を有効にしていない場合に発生する可能性があります。

マイクまたはウェブカメラが Windows で動作していません WorkSpaces。

[Start] (スタート) メニューを開いてプライバシー設定を確認してください

- [Start] (スタート) > [Settings] (設定) > [Privacy] (プライバシー) > [Camera] (カメラ)
- [Start] (スタート) > [Settings] (設定)> [Privacy] (プライバシー) > [Microphone] (マイク)

オフになっている場合は、オンにします。

または、 WorkSpaces 管理者はグループポリシーオブジェクト (GPO) を作成して、必要に応じてマイクやウェブカメラを有効にすることもできます。

ユーザーは証明書ベースの認証を使用してログインできず、デスクトップセッションに接続すると、 WorkSpaces クライアントまたは Windows サインオン画面でパスワードの入力を求められます。

このセッションでは、証明書ベースの認証が失敗しました。問題が続く場合、証明書ベースの認証が失敗するのは、次のいずれかの問題が原因である可能性があります。

- WorkSpaces または クライアントはサポートされていません。証明書ベースの認証は、最新の Windows クライアントアプリケーションを使用する Windows WorkSpaces on WorkSpaces Streaming Protocol (WSP) WorkSpaces バンドルでサポートされています。
- WorkSpaces ディレクトリで証明書ベースの認証を有効にした後、 を再起動 WorkSpaces する必要があります。
- WorkSpaces が と通信できなかったか AWS Private CA、証明書を発行 AWS Private CA しませんでした。AWS CloudTrail で証明書が発行されたかどうかを確認してください。詳細については、「証明書ベースの認証の管理」を参照してください。
- ドメインコントローラーには、スマートカードログオン用のドメインコントローラー証明書がないか、有効期限が切れています。詳細については、「前提条件」のステップ 7「Configure domain controllers with a domain controller certificate to authenticate smart card users」(ドメインコントローラー証明書を使用して、スマートカードユーザーを認証するようにドメインコントローラーを設定する) を参照してください。
- 証明書が信頼されていません。詳細については、「前提条件」のステップ 7「Publish the CA to Active Directory」(CA を Active Directory に公開する) を参照してください。ドメインコントローラー`certutil -viewstore -enterprise NTAuth`で を実行して、CA が公開されていることを確認します。
- キャッシュに証明書はありますが、証明書を無効にしたユーザーの属性が変更されています。証明書の有効期限が切れる (24 時間) 前にキャッシュをクリア AWS Support するには、 にお問い合わせください。詳細については、AWS Support センターを参照してください。
- SAML 属性`UserPrincipalName`の userPrincipalName 形式が正しくフォーマットされていないか、ユーザーの実際のドメインに解決されません。詳細については、「前提条件」のステップ 1 を参照してください。

- SAML アサーションの `ObjectSid` 属性 (オプション) が、SAML_Subject `NameID` で指定したユーザーの Active Directory セキュリティ識別子 (SID) と一致しません。SAML フェデレーションの属性マッピングが正しいこと、および SAML ID プロバイダーが Active Directory ユーザーの SID 属性を同期していることを確認してください。
- スマートカードログオンのデフォルトの Active Directory 設定を変更したり、スマートカードがスマートカードリーダーから取り外された場合にアクションを実行したりするグループポリシー設定があります。これらの設定により、上記のエラー以外にも予期しない動作が発生する可能性があります。証明書ベースの認証では、仮想スマートカードがインスタンスのオペレーティングシステムに提示され、ログオンの完了後にそれが削除されます。「Primary Group Policy settings for smart cards」(スマートカードのプライマリグループポリシー設定) と「Additional smart card Group Policy settings and registry keys」(その他のスマートカードのグループポリシー設定とレジストリキー) (スマートカード取り出し時の動作を含む) を参照してください。
- プライベート CA の CRL ディストリビューションポイントは、オンラインでも、 WorkSpaces またはドメインコントローラーからもアクセスできません。詳細については、「前提条件」のステップ 5 を参照してください。
- ドメインまたはフォレストに古い CAs があるかどうかを確認するには、CA `PKIVIEW.msc` で を実行して確認します。古い CAsを使用して手動で削除します。 `PKIVIEW.msc`
- Active Directory レプリケーションが機能しているかどうか、およびドメインに古いドメインコントローラーがないかどうかを確認するには、 を実行します`repadmin /replsum`。

その他のトラブルシューティング手順には、 WorkSpaces インスタンスの Windows イベントログの確認が含まれます。ログオンの失敗を確認する一般的なイベントは、Windows セキュリティログの「イベント 4625: アカウントがログオンに失敗しました」です。

問題が解決しない場合は、 にお問い合わせください AWS Support。詳細については、AWS Support センターを参照してください。

Windows インストールメディアを必要とするが、提供 WorkSpaces していないことをしようとしている。

AWSが提供するパブリックバンドルを使用している場合は、必要に応じて Amazon EC2 が提供する Windows Server OS インストールメディア EBS スナップショットを使用できます。

これらのスナップショットから EBS ボリュームを作成し、Amazon EC2 にアタッチして、必要に応じてファイルを WorkSpace に転送します。で BYOL で Windows 10 を使用して WorkSpaces いて、インストールメディアが必要な場合は、独自のインストールメディアを準備する必要があります。詳細については、「インストールメディアを使用した Windows コンポーネントの追加」を参照

してください。EBS ボリュームを に直接アタッチすることはできないため WorkSpace、Amazon EC2 インスタンスにアタッチしてファイルをコピーする必要があります。

サポートされていない WorkSpaces リージョンで作成された既存の AWS Managed Directory WorkSpaces で を起動したい。

で現在サポートされていないリージョンでディレクトリ WorkSpaces を使用して Amazon を起動するには WorkSpaces、以下の手順に従います。

> **Note**
>
> AWS Command Line Interface コマンドの実行時にエラーが発生した場合は、最新バージョンを使用していることを確認してください AWS CLI 。詳細については、「最新バージョンの AWS CLIを実行していることを確認する」を参照してください。

ステップ 1: アカウント内の別の仮想プライベートクラウド (VPC) との VPC ピアリングを作成します。

1. 異なるリージョンの VPC との VPC ピアリング接続を作成するには 詳細については、「同じアカウントの異なるリージョンにある VPC を使用して作成する」を参照してください。
2. VPC ピアリング接続を承認します。詳細については、「VPC ピアリング接続を承認する」を参照してください。
3. VPC ピアリング接続をアクティブ化すると、Amazon VPC コンソール、、 AWS CLIまたは API を使用して VPC ピアリング接続を表示できます。

ステップ 2: 両方のリージョンで VPC ピアリングのルートテーブルを更新する

ルートテーブルを更新して、IPv4 または IPv6 を介したピア VPC との通信を有効にします。詳細については、「VPC ピアリング接続のルートテーブルを更新する」を参照してください

ステップ 3: AD Connector を作成して Amazon を登録する WorkSpaces

1. AD Connector の前提条件を確認するには、「AD Connector の前提条件」を参照してください。
2. 既存のディレクトリを AD Connector と接続します。詳細については、「AD Connector を作成する」を参照してください。

3. AD Connectorのステータスが [アクティブ] に変わったら、AWS Directory Service コンソールを開き、ディレクトリ ID のハイパーリンクを選択します。
4. AWS アプリケーションとサービスの場合は、Amazon WorkSpaces を選択して、このディレクトリ WorkSpaces で のアクセスを有効にします。
5. ディレクトリを に登録します WorkSpaces。詳細については、「 でディレクトリを登録する WorkSpaces」を参照してください。

Amazon Linux 2 で Firefox をアップデートしたいと考えています。

ステップ 1: 自動更新が有効になっていることを確認する

自動更新が有効になっていることを確認するには、 `systemctl status *os-update-mgmt.timer | grep enabled`で コマンドを実行します WorkSpace。出力に、`enabled` という単語を含む行が 2 行あるはずです。

ステップ 2: 更新を開始する

Firefox は通常、メンテナンスウィンドウ中に、システム内の他のすべてのソフトウェアパッケージ WorkSpaces とともに Amazon Linux 2 で自動的に更新されます。ただし、これは WorkSpaces 使用している のタイプによって異なります。

- の場合 AlwaysOn WorkSpaces、毎週のメンテナンスウィンドウは、 のタイムゾーンの日曜日の 00:00 から 4:00 です WorkSpace。
- AutoStop WorkSpaces。 の場合、その月の第 3 月曜日から最大 2 週間、メンテナンスウィンドウは毎日 の AWS リージョンのタイムゾーンの午前 0 時から午前 5 時まで開かれます WorkSpace。

メンテナンスウィンドウの詳細については、「メンテナンス WorkSpace 」を参照してください。

を再起動 WorkSpaceし、15 分後に再接続することで、即時の更新サイクルを開始することもできます。「`sudo yum update`」と入力して更新を開始することもできます。Firefox 専用の更新を開始するには、「`sudo yum install firefox`」と入力します。

Amazon Linux 2 リポジトリへのアクセスを設定できず、Mozilla によって構築されたバイナリを使用して Firefox をインストールする場合は、Mozilla のサポートで「Mozilla ビルドの Firefox をインストールする」を参照してください。誤って古いバージョンを実行しないように、RPM パッケージ版の Firefox を完全にアンインストールすることをお勧めします。`sudo yum remove firefox` コマンドを実行して Firefox をアンインストールできます。

別のマシンで yumdownloader firefox コマンドを実行して、Amazon Linux 2 リポジトリから必要な RPM パッケージをダウンロードすることもできます。次に、リポジトリを にサイドロードし WorkSpaces、 のような標準YUMコマンドでインストールできますsudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm。

> **Note**
>
> 正確なファイル名は、パッケージのバージョンによって変わります。

ステップ 3: Firefox リポジトリが使用されていることを確認する

Amazon Linux Extras は、Amazon Linux 2 の Firefox 更新を自動的に提供します WorkSpaces。2023 年 7 月 31 日以降に WorkSpaces 作成された Amazon Linux 2 では、Firefox Extra リポジトリが既に有効になっています。 WorkSpace が Firefox Extra リポジトリを使用していることを確認するには、次のコマンドを実行します。

```
yum repolist | grep amzn2extra-firefox
```

コマンド出力は、Firefox Extra リポジトリが使用されている場合、amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10 と類似したものになります。Firefox Extra リポジトリが使用されていない場合は、空になります。Firefox Extra リポジトリが使用されていない場合は、次のコマンドを使用して手動でアクティブ化を試みることができます。

```
sudo amazon-linux-extras install firefox
```

それでも Firefox Extra リポジトリのアクティブ化に失敗する場合は、インターネット接続を確認し、VPC エンドポイントが設定されていないことを確認してください。YUM リポジトリ WorkSpaces 経由で Amazon Linux 2 の Firefox 更新を引き続き受信するには、 WorkSpaces が Amazon Linux 2 リポジトリに到達できることを確認します。インターネットに接続することなく Amazon Linux 2 リポジトリにアクセスする方法の詳細については、こちらのナレッジセンター記事を参照してください。

ユーザーは、 で設定されたきめ細かなパスワードポリシー (FFGP) 設定を無視して、 WorkSpaces クライアントを使用してパスワードをリセットできます AWS Managed Microsoft AD。

ユーザーの WorkSpaces クライアントが に関連付けられている場合 AWS Managed Microsoft AD、デフォルトの複雑さ設定を使用してパスワードをリセットする必要があります。

デフォルトの複雑さパスワードでは大文字と小文字が区別され、8～64 文字の長さにする必要があります。次の各カテゴリから少なくとも 1 文字を含める必要があります。

- 英小文字 (a～z)
- 英大文字 (A～Z)
- 番号 (0～9)
- 英数字以外の文字(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

パスワードに、空白、キャリッジリチャータブ、改行、null 文字など、印刷不可能なユニコード文字が含まれていないことを確認します。

組織に FFGP を に強制する必要がある場合は WorkSpaces、Active Directory 管理者に連絡して、WorkSpaces クライアントではなく Active Directory から直接ユーザーのパスワードをリセットしてください。

ユーザーに「この OS/プラットフォームは、ウェブアクセス WorkSpace を使用して Windows/Linux にアクセスしようとする WorkSpaceと、 にアクセスする権限がありません」というエラーメッセージが表示される

ユーザーが使用しようとしているオペレーティングシステムのバージョンは、 WorkSpaces Web Access と互換性がありません。 WorkSpace ディレクトリのその他のプラットフォーム設定でウェブアクセスを有効にしてください。のウェブアクセスを有効にする方法の詳細については、WorkSpace「」を参照してくださいAmazon WorkSpaces Web Access の有効化と設定。

Amazon WorkSpaces クライアントアプリケーションのサポート終了ポリシー

Amazon WorkSpaces のサポート終了 (EOL) ポリシーは、サポート対象外となって、新しいバージョンとの互換性がテストされなくなる特定のメジャーバージョン (およびそのすべてのマイナーバージョン) に適用されます。

WorkSpaces クライアントバージョンのライフサイクルには、一般的なサポート、テクニカルガイダンス、サポート終了 (EOL) の 3 つのフェーズがあります。一般的なサポートフェーズは、WorkSpaces クライアントの最初のパブリックリリース日に始まり、一定期間続きます。一般的なサポートフェーズでは、WorkSpaces サポートチームが設定の問題に対する全面的なサポートを提供します。不具合の解決と機能のリクエストは、WorkSpaces クライアントの該当するメジャーバージョンおよび関連するマイナーバージョンに実装されます。

テクニカルガイダンスは、一般的なサポートフェーズの終了日からサポート終了日まで提供されます。テクニカルガイダンスフェーズでは、サポートされている設定に関するサポートとガイダンスのみを受けられます。不具合の解決と機能のリクエストは、WorkSpaces クライアントの最新バージョンにのみ実装されます。旧バージョンには実装されません。テクニカルガイダンスフェーズでは、修正が必要な場合、AWS は近く公開されるバージョンリリースでの修正をスケジュールします。お客様は、最新の WorkSpaces バージョンにアップグレードして修正に関連するサポートを受けられます。

メジャーバージョンの EOL は、一般的なサポートとテクニカルガイダンスの両方が終了したときに発生します。EOL の日付を過ぎると、サポートもガイダンスも提供されなくなります。AWS は、互換性の問題のテストを終了します。引き続きサポートを受けるには、最新の WorkSpaces バージョンにアップグレードする必要があります。

特定のバージョンのサポートの詳細については、次の表を参照してください。

Windows クライアント	一般的なサポート	テクニカルガイダンス	EOL
2.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Linux クライアント	一般的なサポート	テクニカルガイダンス	EOL
Ubuntu 18.04 用の 4.x	2021 年 8 月 12 日	2023 年 3 月 31 日	2023 年 8 月 31 日
Ubuntu 18.04 用の 3.x	2019 年 11 月 25 日	2023 年 3 月 31 日	2023 年 8 月 31 日

macOS クライアント	一般的なサポート	テクニカルガイダンス	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

iPad クライアント	一般的なサポート	テクニカルガイダンス	EOL
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Android クライアント	一般的なサポート	テクニカルガイダンス	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Web Access	一般的なサポート		
Google Chrome	現行バージョンと、直近の 2 つのメジャーバージョン		

Web Access	一般的なサポート		
Firefox	現行バージョンと、直近の 2 つのメジャーバージョン		
Microsoft Edge	現行バージョンと、直近の 2 つのメジャーバージョン		

サポートされていないクライアント

以下の WorkSpaces クライアントはサポートされていません。

オペレーティングシステム	クライアントバージョン	一般的なサポート	テクニカルガイダンス	EOL	メモ
Windows	5.11	2023 年 7 月 3 日	2023 年 10 月 1 日	2023 年 10 月 1 日	品質上の問題によりサポートされません
Windows	5.10	2023 年 6 月 19 日	2023 年 10 月 1 日	2023 年 10 月 1 日	品質上の問題によりサポートされません
Windows	5.9	2023 年 5 月 9 日	2023 年 10 月 1 日	2023 年 10 月 1 日	品質上の問題によりサポートされません

EOL に関するよくある質問

EOL に達したバージョンの WorkSpaces クライアントを使用しています。サポートされているバージョンにアップグレードするにはどうしたらいいですか?

WorkSpaces クライアントのダウンロードページに移動して、完全にサポートされているバージョンの WorkSpaces をダウンロードしてインストールしてください。

サポートされている WorkSpaces で、EOL に達したバージョンの WorkSpaces クライアントを使用できますか?

EOL に達したクライアントバージョンには以前の解決策と機能が適用されなくなるため、クライアントを最新バージョンにアップグレードすることを強くお勧めします。EOL に達したクライアントバージョンを使用している場合は、AWS サポートチームに詳細をお問い合わせください。

EOL に達したバージョンの WorkSpaces クライアントを使用しています。これに関する問題を引き続き報告できますか?

まず、サポート対象のバージョンにアップグレードしてから、問題を再現してみる必要があります。サポート対象のバージョンでも問題が解決しない場合は、AWS サポートチームとサポートケースを開いてください。

サポートされている WorkSpaces クライアントバージョンを、EOL に達したオペレーティングシステムで使用しています。これに関する問題を引き続き報告できますか?

EOL に達したオペレーティングシステムでは、技術サポートやソフトウェアアップデートを利用できなくなります。また、AWS は、EOL に達したオペレーティングシステムを使用している WorkSpaces クライアントに対してサポートを提供していません。WorkSpaces クライアントのサポートを利用するには、サポート対象のオペレーティングシステムを使用してください。

Amazon WorkSpaces クォータ

Amazon WorkSpaces は、、イメージ、バンドル、ディレクトリ WorkSpaces、接続エイリアス、IP コントロールグループなど、特定のリージョンのアカウントで使用できるさまざまなリソースを提供します。Amazon Web Services アカウントを作成すると、作成できるリソースの数が、デフォルトのクォータ (制限とも言う) として設定されます。

AWS アカウントの WorkSpaces のデフォルトのクォータを次に示します。Service Quotas コンソールを使用して、デフォルトのクォータや適用されているクォータを表示したり、調整可能なクォータのクォータの引き上げをリクエストすることができます。

Service Quotas が利用できないリージョンの一部では、サポートケースを送信して、制限の引き上げをリクエストする必要があります。詳細については、Service Quotas ユーザーガイドの「Service Quotas の表示」および「クォータの引き上げのリクエスト」を参照してください。

リソース	デフォルト	説明	調整可能
WorkSpaces	1	このアカウントの現在のリージョン WorkSpaces における の最大数。	はい
グラフィックス WorkSpaces	0	このアカウントの現在のリージョン WorkSpaces における Graphics の最大数。 **Note** 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。を WorkSpaces Graphics.	はい

リソース	デフォルト	説明	調整可能
		g4dn バンドルに移行することをお勧めします。詳細については、「の移行 WorkSpace」を参照してください。	
Graphics.g4dn WorkSpaces	0	この WorkSpaces アカウントの現在のリージョンにおける Graphics.g4dn の最大数。	はい
GraphicsPro WorkSpaces	0	このアカウントの現在のリージョン GraphicsPro WorkSpaces における の最大数。	はい
GraphicsPro.g4dn WorkSpaces	0	このアカウントの現在のリージョン WorkSpaces における GraphicsPro.g4dn の最大数。	はい
スタンバイ WorkSpaces	0	このアカウントの現在のリージョン WorkSpaces における の最大数。	はい

リソース	デフォルト	説明	調整可能
バンドル	50	現在のリージョン内のこのアカウントのバンドルの最大数。このクォータはカスタムバンドルにのみ適用され、パブリックバンドルには適用されません。	いいえ
接続エイリアス	20	現在のリージョン内のこのアカウントの接続エイリアスの最大数。	いいえ
ディレクトリ	50	現在のリージョンで、このアカウント WorkSpaces で Amazon で使用するために登録できるディレクトリの最大数。	いいえ
イメージ	40	現在のリージョン内のこのアカウントのイメージの最大数。	はい
IP アクセスコントロールグループ	100	現在のリージョン内のこのアカウントの IP アクセスコントロールグループの最大数。	いいえ

リソース	デフォルト	説明	調整可能
ディレクトリあたりの IP アクセスコントロールグループ数	25	現在のリージョン内のこのアカウントのディレクトリあたりの IP アクセスコントロールグループの最大数。	いいえ
IP アクセスコントロールグループあたりのルール数	10	現在のリージョン内のこのアカウントの IP アクセスコントロールグループあたりのルールの最大数。	いいえ

API スロットリング

許容されるレートは 1 秒あたり 2 回の呼び出しです。詳細については、「スロットリングの例外」を参照してください。

WorkSpaces ストリーミングプロトコル (WSP) ホストエージェントのバージョン

WorkSpaces Streaming Protocol (WSP) ホストエージェントは、 内で実行されるホストエージェントです WorkSpace。のピクセルをクライアントアプリケーション WorkSpace にストリーミングし、双方向のオーディオとビデオ、印刷などのセッション内機能が含まれています。 WorkSpaces ストリーミングプロトコル (WSP) の詳細については、「Amazon のプロトコル WorkSpaces」を参照してください。

ホストエージェントソフトウェアは常に最新バージョンに更新しておくことをお勧めします。を手動で再起動 WorkSpaces して WSP ホストエージェントを更新できます。WSP ホストエージェントは、通常の WorkSpaces デフォルトのメンテナンスウィンドウ中にも自動的に更新されます。メンテナンスウィンドウの詳細については、「 メンテナンスWorkSpace 」を参照してください。これらの機能の一部には、最新の WorkSpaces クライアントバージョンが必要です。最新のクライアントバージョンの詳細については、WorkSpaces 「クライアント」を参照してください。

次の表に、WSP ホストエージェントの各バージョンの変更をまとめています。

リリース	日付	変更
• Windows WorkSpaces - 2.1.0.1554	2024 年 5 月 15 日	• アイドル切断タイムアウトのサポートが追加されました。 • アイドル切断タイムアウトを設定する新しいグループポリシー設定を追加しました。 • ユーザーが表示設定を変更したときに が切断され、白い画面が表示される問題を修正 WorkSpaces しました。 • パフォーマンス向上とバグ修正が行われています。
• Ubuntu WorkSpaces - 2.1.0.1342	2024 年 2 月 29 日	• ウェブカメラの推奨解像度を 480 x 360 から 640 x 480 に変更しました。

リリース	日付	変更
		• パフォーマンス向上とバグ修正が行われています。
• Windows WorkSpaces - 2.0.0.1425	2024 年 2 月 22 日	• リモート Google Chrome または Microsoft Edge ブラウザで実行されているウェブアプリケーションからのセッション内 WebAuthn リダイレクトリクエストのサポートが追加されました。この機能は、DCV リダイレクト拡張機能を有効にするようユーザーに求める 1 WebAuthn 回限りのブラウザプロンプトを追加します。Windows WorkSpaces および WorkSpaces ネイティブクライアントでのみサポートされています。 • ログイン時に白またはフリーズ画面が表示されることがある問題を修正しました。 • パフォーマンス向上とバグ修正が行われています。
• Windows WorkSpaces - 2.0.0.1304	2024 年 1 月 11 日	• ログイン中のストリーミングのフリーズの可能性に関連するバグを修正しました。 • ログ記録関連のバグを修正しました。

リリース	日付	変更
• Windows WorkSpaces - 2.0.0.1288	2023 年 11 月 16 日	• Windows 10 以降の間接ディスプレイドライバー (IDD) のサポートが追加されました。これにより、CPU の消費量が減少し、ストリーミングパフォーマンスが向上します。 • IDD ドライバーを有効または無効にする新しいグループポリシー設定を追加しました。 • クリップボードイメージの透明度に関連するバグを修正しました。 • Windows のスケール係数を保持するバグを修正しました。 • パフォーマンス向上とバグ修正が行われています。
• Windows WorkSpaces - 2.0.0.1164	2023 年 10 月 13 日	• 仮想ディスプレイドライバーに VSync のサポートを追加しました。 • VSync を有効または無効にする新しいグループポリシー設定を追加しました。 • 再接続と信頼性の問題を改善しました。 • パフォーマンス向上とバグ修正が行われています。

リリース	日付	変更
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	2023 年 8 月 18 日	• タイムゾーンのリダイレクトを有効または無効にするための新しい設定を追加しました。 • ログオンタイムアウトを延長し、設定オプションを追加しました。 • 中断後の再接続を迅速に行うことができるようにゲートウェイが改善されました。 • パフォーマンス向上とバグ修正が行われています。
• Amazon Linux WorkSpaces - 2.0.0.907	2023 年 6 月 30 日	• ISV 固有の統合を可能にする DCV 拡張機能 SDK のサポートを追加しました。 • ログアウトするとユーザーのセッションが終了するように切断動作を変更しました。 • タイムゾーンのリダイレクトのサポートを追加しました。 • ログオンタイムアウトを延長し、設定オプションを追加しました。 • アップグレードの問題を修正しました。 • パフォーマンス向上とバグ修正が行われています。
• Windows WorkSpaces - 2.0.0.829	2023 年 6 月 8 日	• ログアウトするとユーザーのセッションが終了するように切断動作を変更しました。 • A/V 同期と日本語キーボードに関するバグを修正しました。 • WSP インストーラの信頼性が向上しました。

リリース	日付	変更
• Ubuntu WorkSpaces - 2.1.0.829	2023 年 5 月 16 日	• ログアウトするとユーザーのセッションが終了するように切断動作を変更しました。 • ISV 固有の統合を可能にする DCV 拡張機能 SDK のサポートを追加しました。 • タイムゾーンのリダイレクトのサポートを追加しました。 • アップグレードの問題を修正しました。
• Windows WorkSpaces - 2.0.0.799	2023 年 5 月 8 日	• いくつかの画質とパフォーマンスの最適化により、UDP ベースの QUIC 転送を強化しました。 • ISV 固有の統合を可能にする DCV 拡張機能 SDK のサポートを追加しました。 • 拡張機能 SDK を有効または無効にする新しいグループポリシー設定を追加しました。 • 韓国語、日本語、およびドイツ語のキーボードレイアウトを改善しました。 • セッションフリーズの問題、ハードウェアアクセラレーション、プリンタのリダイレクト、ログの冗長性、および target-fps グループポリシー設定に関連するバグを修正しました。

Note

- ホストエージェントのバージョンを確認する方法については、「WSP の最新バージョンでサポートされているクライアントとホストのオペレーティングシステムは何ですか?」を参照してください。
- ホストエージェントのバージョンを更新する方法については、「WSP が既にある場合は WorkSpace、どのように更新すればよいですか？」を参照してください。
- WSP macOS クライアントバージョンのリリースノートについては、「 ユーザーガイド」の WorkSpaces macOS クライアントアプリケーション」セクションの「リリースノート WorkSpaces 」を参照してください。
- WSP Windows クライアントバージョンのリリースノートについては、「 ユーザーガイド」の WorkSpaces 「Windows クライアントアプリケーション」セクションの「リリースノート WorkSpaces 」を参照してください。

WSP でサポートされている SDK 拡張機能

Amazon WorkSpaces Streaming Protocol (WSP) は NICE DCV テクノロジーを使用して構築されており、幅広いワークロードやユースケースで WorkSpaces インスタンスへの高性能なリモートアクセスを可能にします。NICE DCV 拡張機能 SDK を使用すると、デベロッパーはエンドユーザー向けに、WSP WorkSpaces エクスペリエンスをカスタマイズできます。これには以下が含まれます。

- カスタムハードウェアのサポートを促進する。
- リモートセッションでのサードパーティーアプリケーションの使いやすさを高める。例えば、VoIP アプリケーションにローカルオーディオの削除を追加したり、会議アプリケーションにローカルビデオ再生を追加したりできます。
- スクリーンリーダーなどのアクセシビリティソフトウェアに、リモートセッションやリモートで実行されているアプリケーションに関する情報を提供する。
- セキュリティソフトウェアに対して、ローカルエンドポイントのセキュリティ体制を分析して条件付きアクセスポリシーを許可できるようにする。
- 確立されたリモートセッションで任意のデータ転送を実行する。

NICE DCV 拡張 SDK の使用を開始するには、NICE DCV 拡張機能 SDK のドキュメントを参照してください。SDK 自体は NICE DCV 拡張機能 SDK の GitHub リポジトリにあります。また、NICE DCV 拡張機能 SDK サンプル GitHub リポジトリに SDK の統合例も記載されています。

WorkSpaces によって以下がサポートされています。

- ストリーミングプロトコル – WorkSpaces Streaming Protocol (WSP)
- WorkSpaces Windows クライアント – Windows: 5.9.0.4110 以降。

> **Note**
>
> WorkSpaces Android、iOS クライアント、ウェブアクセスは NICE DCV 拡張機能 SDK をサポートしていません。

- サポートされている WorkSpaces – Windows、Linux、Ubuntu サーバー

WorkSpaces のドキュメント履歴

次の表では、2018 年 1 月 1 日以降、WorkSpaces サービスと Amazon WorkSpaces 管理ガイドへの重要な変更点が示されています。また、お客様からいただいたフィードバックに対応するために、ドキュメントを頻繁に更新しています。

これらの更新に関する通知については、WorkSpaces RSS フィードにサブスクライブできます。

変更	説明	日付
AmazonWorkSpacesAdmin マネージドポリシーの更新	WorkSpaces は AmazonWorkSpacesAdmin の管理ポリシーに workspaces:RestoreWorkspace アクションを追加し、管理者に WorkSpaces を復元するためのアクセス権を付与します。	2023 年 7 月 17 日
WSP でサポートされている SDK 拡張機能	NICE DCV 拡張機能 SDK を使用すると、デベロッパーはエンドユーザー向けに WSP WorkSpaces エクスペリエンスをカスタマイズできます。	2023 年 5 月 25 日
WorkSpaces Streaming Protocol (WSP) ホストエージェントバージョン	WorkSpaces Streaming Protocol (WSP) のバージョン情報。	2023 年 5 月 8 日
AWS GovCloud (米国東部) での Amazon WorkSpaces の提供開始	Amazon WorkSpaces は、AWS GovCloud (米国東部) で利用可能です。	2023 年 5 月 3 日
Amazon WorkSpaces ウェブカメラのサポート	Amazon WorkSpaces は、ローカルウェブカメラビデオ入力を Windows WorkSpaces デスクトップに WorkSpaces Streaming Protocol (WSP) を使用してシームレスにリダ	2021 年 4 月 5 日

	イレクトすることにより、リアルタイムオーディオビデオ (AV) のサポートを開始しました。	
WorkSpaces MacOS クライアントアプリケーションでの Amazon WorkSpaces スマートカードのサポート	Common Access Card (CAC) および Personal Identity Verification (PIV) スマートカードを使用して、Amazon WorkSpaces MacOS クライアントアプリケーションをご利用いただけるようになりました。スマートカードのサポートは、WorkSpaces Streaming Protocol (WSP) を使用する WorkSpaces で利用可能です。	2021 年 4 月 5 日
Amazon WorkSpaces バンドル管理 API	Amazon WorkSpaces バンドル管理 API が利用可能になりました。これらの API アクションにより、WorkSpaces バンドルの作成や削除、およびイメージの関連付けに関するオペレーションが実行できます。	2021 年 3 月 15 日
Amazon WorkSpaces がアジアパシフィック (ムンバイ) で利用可能に	Amazon WorkSpaces は、アジアパシフィック (ムンバイ) リージョンで利用できます。	2021 年 3 月 8 日

WorkSpaces Streaming Protocol (WSP)	WorkSpaces Streaming Protocol (WSP) は、Graphics と GraphicsPro を除くすべてのバンドルタイプで、ライセンス付属 (Windows Server 2016) と BYOL Windows 10 ベースの WorkSpaces の両方で利用可能となりました。WSP は、AWS GovCloud (米国西部) リージョンの Linux WorkSpaces でも利用できます。	2020 年 12 月 1 日
スマートカード	Amazon WorkSpaces では、AWS GovCloud (米国西部) リージョンにおいて、Windows および Linux WorkSpaces でのセッション前 (ログイン) およびセッション内のスマートカード認証がサポートされるようになりました。	2020 年 12 月 1 日
カスタムイメージの共有	AWS アカウント間でカスタム WorkSpaces イメージを共有できるようになりました。イメージの共有後、受信者アカウントはイメージをコピーし、それを使用して新しい WorkSpaces を起動するためのバンドルを作成できます。	2020 年 10 月 1 日

クロスリージョンリダイレクト	クロスリージョンリダイレクトを使用できるようになりました。クロスリージョンリダイレクトは、ドメインネームシステム (DNS) ルーティングポリシーと連携して、プライマリ WorkSpaces を使用できない場合にユーザーを別の WorkSpaces にリダイレクトする機能です。	2020 年 9 月 10 日
BYOL WorkSpaces のマイクロソフト Office 2016 または 2019 を購読する	Windows ライセンス持ち込み (BYOL) WorkSpaces において、AWS から Microsoft Office Professional 2016 または 2019 にサブスクライブすることが可能になりました。	2020 年 9 月 3 日
中国 (寧夏) における BYOL オートメーション	自分のライセンス使用 (BYOL) オートメーションを使用すると、中国 (寧夏) で Windows 10 のデスクトップライセンスを WorkSpaces に使用するプロセスをシンプルにできます。	2020 年 4 月 2 日
Image Checker	Image Checker ツールは、Windows WorkSpace がイメージ作成の要件を満たしているかどうかを判断するのに役立ちます。Image Checker は、イメージの作成に使用する WorkSpace で一連のテストを実行し、検出された問題を解決する方法に関するガイダンスを提供します。	2020 年 3 月 30 日

WorkSpace の移行	Amazon WorkSpaces の移行機能を使用すると、ユーザーボリューム上のデータを保持しながら、あるバンドルから別のバンドルに WorkSpace を移行できます。この機能を使用して、Windows 7 デスクトップエクスペリエンスから Windows 10 デスクトップエクスペリエンスに WorkSpace を移行できます。また、あるパブリックバンドルまたはカスタムバンドルから別のバンドルに WorkSpace を移行することもできます。	2020 年 1 月 9 日
Amazon WorkSpaces API の PrivateLink の統合	インターネット経由で接続するのではなく、Virtual Private Cloud (VPC) のインターフェイスエンドポイントを通じて Amazon WorkSpaces API エンドポイントに直接接続できます。VPC インターフェイスエンドポイントを使用すると、AWS ネットワーク内で VPC と Amazon WorkSpaces API エンドポイント間の通信が完全かつ安全に実施されます。	2019 年 11 月 25 日
Amazon WorkSpaces 用の Linux クライアント	これで、ユーザーは Linux クライアントを使用して WorkSpaces にアクセスできるようになります。	2019 年 11 月 25 日

Amazon WorkSpaces が中国 (寧夏) で利用可能に	Amazon WorkSpaces は、中国 (寧夏) リージョンで利用できます。	2019 年 11 月 13 日
既知の正常な状態への WorkSpace の復元	復元機能を使用して、WorkSpace を既知の正常な状態にロールバックできます。	2019 年 9 月 18 日
FIPS エンドポイントの暗号化	Federal Risk and Authorization Management Program (FedRAMP) または Department of Defense(DoD)Cloud Computing Security Requirements Guide (SRG) に準拠するには、ディレクトリレベルで連邦情報処理標準 (FIPS) エンドポイント暗号化を使用するように Amazon WorkSpaces を設定できます。	2019 年 9 月 12 日
WorkSpace イメージのコピー	同じリージョン内、またはリージョン間でイメージをコピーできます。	2019 年 6 月 27 日
ユーザーを対象とした WorkSpace の自己管理機能	ユーザーが自分のエクスペリエンスをより詳細に制御するには、WorkSpace 自己管理機能を使用します。	2018 年 11 月 19 日

BYOL オートメーション	自分のライセンス使用 (BYOL) オートメーションを使用すると、Windows 7 および Windows 10 のデスクトップライセンスを WorkSpaces に使用するプロセスをシンプルにできます。	2018 年 11 月 16 日
PowerPro および GraphicsPro バンドル	WorkSpaces では、PowerPro および GraphicsPro のバンドルを使用できます。	2018 年 10 月 18 日
WorkSpace ログインの結果をモニタリングする	Amazon CloudWatch Events のイベントを使用して、WorkSpace ログインの結果をモニタリングし、応答することができます。	2018 年 9 月 17 日
Web Access を使用して Windows 10 WorkSpaces にアクセスする	ユーザーはこのウェブアクセスクライアントを使用して、Windows 10 のデスクトップ環境で実行されている WorkSpace にアクセスできるようになりました。	2018 年 8 月 24 日
URI ログイン	Uniform Resource Identifier (URI) を使用して、ユーザーに自分の WorkSpaces へのアクセスを提供します。	2018 年 7 月 31 日
Amazon Linux WorkSpaces	ユーザー向けに Amazon Linux WorkSpaces をプロビジョニングすることができます。	2018 年 26 月 6 日
IP アクセスコントロールグループ	ユーザーが WorkSpaces にアクセスできる IP アドレスを制御できます。	2018 年 4 月 30 日

インプレースアップグレード	Windows 10 BYOL WorkSpaces を新しいバージョンの Windows 10 にアップグレードできます。	2018 年 3 月 9 日

以前の更新

次の表は、2018 年 1 月 1 日より前の Amazon WorkSpaces サービスおよびそのドキュメントセットへの重要な追加項目を示しています。

変更	説明	日付
フレキシブルなコンピューティングオプション	WorkSpaces を Value、Standard、Performance、および Power バンドル間で切り替えることができます。	2017 年 12 月 22 日
設定可能なストレージ	起動時に WorkSpace のルートボリュームとユーザーボリュームのサイズを設定できます。また、後でこれらのボリュームのサイズを増やすこともできます。	2017 年 12 月 22 日
デバイスのアクセスコントロール	WorkSpaces にアクセスできるデバイスのタイプを指定できます。さらに、WorkSpace へのアクセスを、信頼できるデバイス (管理対象デバイスとも呼ばれます) に限定することもできます。	2017 年 6 月 19 日
相互フォレストの信頼性	AWS Managed Microsoft AD とオンプレミスの Microsoft Active Directory ドメイン間で信頼関係を確立すると、オンプレミスドメインのユーザーに対して WorkSpaces をプロビジョニングできます。	2017 年 2 月 9 日
Windows Server 2016 バンドル	WorkSpaces は、Windows Server 2016 で稼働する Windows 10 デスクトップ環境に含まれるバンドルを提供しています。	2016 年 11 月 29 日

変更	説明	日付
Web Access	WorkSpaces Web Access を使用して、ウェブブラウザから Windows WorkSpaces にアクセスできます。	2016 年 11 月 18 日
時間単位の WorkSpaces	ユーザーへの課金が時間単位になるように WorkSpace を設定できます。	2016 年 8 月 18 日
Windows 10 BYOL	Windows 10 デスクトップのライセンスを WorkSpaces に導入できます (BYOL)。	2016 年 7 月 21 日
タグ指定のサポート	WorkSpaces の管理と追跡にタグを使用できます。	2016 年 5 月 17 日
登録の保存	新しい登録コードを入力するたびに、WorkSpaces クライアントに保存されます。これにより、ディレクトリまたはリージョンが異なる WorkSpace 間での切り替えが簡単になります。	2016 年 1 月 28 日
Windows 7 BYOL、Chromebook クライアント、WorkSpace 暗号化	Chromebook クライアントおよび WorkSpace 暗号化を使用して、Windows 7 デスクトップライセンスを WorkSpaces (BYOL) で使用することができます。	2015 年 10 月 1 日
CloudWatch のモニタリング	CloudWatch モニタリングに関する情報を追加しました。	2015 年 4 月 28 日
自動セッション再接続	WorkSpace のデスクトップクライアントアプリケーションの自動セッション再接続機能についての情報を追加しました。	2015 年 3 月 31 日
パブリック IP アドレス	パブリック IP アドレスを自動的に WorkSpaces に割り当てることができます。	2015 年 1 月 23 日
WorkSpaces がアジアパシフィック (シンガポール) で利用可能に	WorkSpaces は、アジアパシフィック (シンガポール) リージョンでご利用いただけます。	2015 年 1 月 15 日

変更	説明	日付
Value バンドルの追加、Standard バンドルの更新、Office 2013 の追加	Value バンドルが利用可能になり、Standard バンドルのハードウェアがアップグレードされ、Microsoft Office 2013 が Plus パッケージで利用可能になりました。	2014 年 11 月 6 日
イメージとバンドルのサポート	カスタマイズした WorkSpace からイメージを作成し、そのイメージからカスタム WorkSpace バンドルを作成することができます。	2014 年 10 月 28 日
PCoIP ゼロクライアントのサポート	WorkSpaces PCoIP ゼロクライアントデバイスにアクセスできます。	2014 年 10 月 15 日
WorkSpaces がアジアパシフィック (東京) で利用可能に	WorkSpaces は、アジアパシフィック (東京) リージョンでご利用いただけます。	2014 年 8 月 26 日
ローカルプリンターのサポート	WorkSpaces にローカルプリンターのサポートを有効化できます。	2014 年 8 月 26 日
多要素認証	接続したディレクトリで多要素認証を使用できます。	2014 年 8 月 11 日
デフォルト OU のサポートとターゲットドメインのサポート	WorkSpace マシンアカウントが配置されている場所にデフォルトの組織単位 (OU) を選択し、WorkSpace マシンアカウントが作成された場所に別のドメインを選択できます。	2014 年 7 月 7 日
セキュリティグループの追加	WorkSpaces にセキュリティグループを追加できます。	2014 年 7 月 7 日
WorkSpaces がアジアパシフィック (シドニー) で利用可能に	WorkSpaces は、アジアパシフィック (シドニー) リージョンでご利用いただけます。	2014 年 5 月 15 日
WorkSpaces が欧州 (アイルランド) で利用可能に	WorkSpaces は、欧州 (アイルランド) リージョンでご利用いただけます。	2014 年 5 月 5 日

変更	説明	日付
パブリックベータ	WorkSpaces はパブリックベータとして利用できます。	2014 年 3 月 25 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。