aws

管理ガイド

# Amazon WorkSpaces

# Amazon WorkSpaces: 管理ガイド

# Table of Contents

# Amazon WorkSpaces とは

Amazon WorkSpaces を使用すると、WorkSpaces と呼ばれるクラウドベースの仮想デスクトップをユーザーに向けてプロビジョニングできます。これらのデスクトップでは、Microsoft Windows、Amazon Linux 2、Ubuntu Linux、Rocky Linux、または Red Hat Enterprise Linux を実行できます。WorkSpaces 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。

Amazon WorkSpaces では、組織とユーザーのニーズに応じて、WorkSpaces Personal と WorkSpaces Pools のいずれかを選択できます。

- WorkSpaces Personal - 高度にパーソナライズされた専用のデスクトップを必要とするユーザーに向けて、カスタマイズされた永続的な仮想デスクトップをプロビジョニングする必要がある場合は、WorkSpaces Personal を選択します。これは、個人に割り当てられた物理的なデスクトップコンピュータに似ています。詳細については、「WorkSpaces Personal で WorkSpace を作成する」を参照してください。
- WorkSpaces Pools - 一時的なインフラストラクチャでホストされている高度に選別されたデスクトップ環境へのアクセスを必要とするユーザーに向けて、カスタマイズされた非永続的な仮想デスクトップを提供する必要がある場合は、WorkSpaces Pools を選択します。詳細については、「WorkSpaces Pools を管理する」を参照してください。

WorkSpaces のデスクトップは、さまざまな方法で設定できます。

- さまざまなハードウェア設定、ソフトウェア設定、 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「 the section called “カスタムイメージとバンドルを作成する” 」を参照してください。
- WorkSpaces が Windows を実行している場合は、独自のライセンスとアプリケーションを持ち込むか、 AWS Marketplace for Desktop Apps から購入できます。
- WorkSpaces で Windows 10 または 11 を実行する場合は、WorkSpaces を Microsoft Entra ID に参加させることで、ユーザーは既存の Entra ID 認証情報を使用して Microsoft 365 Apps for Enterprise へシームレスにアクセスできます。また、WorkSpaces を Intune に登録し、Intune を使って仮想デスクトップを管理することもできます。詳細については、「WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する」を参照してください。Microsoft Entra ID の詳細については、「What is Microsoft Entra ID?」を参照してください。Microsoft Intune の

詳細については、「Microsoft Intune securely manages identities, manages apps, and manages devices」を参照してください。

- PCoIP または DCV プロトコルを選択します。詳細については、「WorkSpaces Personal のプロトコル」を参照してください。
- ユーザー用にスタンドアロンのマネージド型 Microsoft Active Directory を作成するか、WorkSpaces をオンプレミスの Active Directory に接続します。これにより、ユーザーは既存の認証情報を使用して、自社リソースにシームレスにアクセスできるようになります。詳細については、「the section called “WorkSpaces のディレクトリを管理する”」を参照してください。
- 同じツールを使用して、オンプレミスデスクトップの管理に使用する WorkSpace 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、保管中のデータ、ディスク I/O、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 WorkSpaces にアクセスするときに使用してよい IP アドレスを選択します。
- WorkSpaces を月額料金で使用するか時間単位の料金で使用するかを選択します。詳細については、WorkSpaces の料金を参照してください。

WorkSpaces の詳しい使い方については、以下を参照してください。

- 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 セッションなどが含まれます
- クラウドでのデスクトップのプロビジョニング
- Amazon WorkSpaces をデプロイするためのベストプラクティス
- Amazon WorkSpaces のよくある質問
- WorkSpaces の料金体系と例については、「WorkSpaces の料金」を参照してください。

# 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

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、またはサポートされているオペレーティングシステムのサポートされているウェブブラウザを介して WorkSpaces に接続できます。

> **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。

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

- 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。

# WorkSpaces で自分の 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れば、お客様の Windows 10 または 11 デスクトップを WorkSpaces に持ち込んでデプロイできます。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 クラウド内のお客様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、WorkSpaces の料金を参照してください。

> **Important**
>
> イメージの作成は、あるバージョンの Windows 10 または 11 から新しいバージョンの Windows 10 または 11 にアップグレードされた Windows 10 または 11 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 の累積的な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 のイメージ作成プロセスでサポートされます。

## Amazon EC2 Image Builder の使用 (Windows 11 のみ )

Windows 11 を使用している場合は、Amazon EC2 Image Builder を使用して WorkSpaces の BYOL イメージをインポートおよび作成できます。これを行うには、以下の代わりに Amazon EC2 Image Builder を使用します。

- the section called “ステップ 4: VM が BYOL 要件を満たしていることを確認する”
- the section called “ステップ 5: 仮想化環境から VM をエクスポートする”

詳細については、Amazon EC2 Image Builder ユーザーガイド」を参照してください。

# ステップ 1: Amazon WorkSpaces で Microsoft BYOL を使用するための前提条件

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 非対応のバンドル (Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro 以外のバンドル) を使用する場合は、リージョンごとに 100 以上の WorkSpaces を使用することになります。これらの 100 の WorkSpaces は、AlwaysOn WorkSpace と AutoStop WorkSpace の任意の組み合わせにすることができます。専有ハードウェアで WorkSpaces を実行するには、リージョンごとに少なくとも 100 の WorkSpaces を使用する必要があります。専有ハードウェアでの WorkSpaces の実行は、Microsoft とのライセンス契約の要件を満たすために必要です。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 対応のバンドル (Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro) の使用を予定している場合は、リージョンごとに 1 か月あたり最低 4 つの AlwaysOn または 20 の AutoStop GPU 対応 WorkSpaces を専用ハードウェアで実行することを確認してください。

> **Note**
>
> - イメージのインポートプロセスの一環として、 はシステムログ AWS を自動的に取得して、イメージのインポートエラーを解決し、トラブルシューティングのヘルプを提供し、ユーザーに正確なエラーメッセージを提供します。
> - GraphicsPro バンドルは 2025 年 10 月 31 日にend-of-lifeとなります。GraphicsPro WorkSpaces は、2025 年 10 月 31 日より前にサポートされている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、「WorkSpaces Personal で WorkSpace を移行する」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。それまでに 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、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
> - Graphics 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。
> - Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro バンドルは、アフリカ (ケープタウン) リージョンとイスラエル (テルアビブ) リージョンでは利用できません。

- アフリカ (ケープタウン) リージョンで WorkSpaces を実行するには、アフリカ (ケープタウン) リージョンで最低 400 の WorkSpaces を実行する必要があります。
- Windows 11 バンドルは、DCV の WorkSpaces で作成できます。Windows 11 バンドルは、WorkSpaces Core によるパートナープロトコルでもサポートされています。
- Graphics および GraphicsPro バンドルは Windows 11 ではサポートされていません。
- Value バンドルは Windows 11 および WorkSpaces Pools では使用できません。既存のバリューバンドルの WorkSpaces の移行の詳細については、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
- 最高のビデオ会議エクスペリエンスを得るには、Power (4 vCPU、16 GB 以上のメモリ) バンドルを使用することをお勧めします。
- Windows 11 が機能するには、統合拡張ファームウェアインターフェイス (UEFI) ブートモードが必要です。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 では、IP アドレス範囲 /16 で管理インターフェイスを使用できます。この管理インターフェイスは、インタラクティブなストリーミング用にセキュアな WorkSpaces 管理ネットワークに接続されます。これにより、WorkSpaces がユーザーの WorkSpaces を管理できるようになります。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。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 WorkSpaces 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を開いていることを確認します。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が許可された WorkSpaces_BYOL アカウントを作成することをお勧めします。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 4: Amazon WorkSpaces の Windows VM が Microsoft BYOL の要件を満たしていることを確認する 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。
- `%WINDIR%\panther` および `%WINDIR%\panther\unattend` のパスにある Windows のデフォルトのシステム無人ファイルは変更しないでください。

> **Note**
>
> - BYOL AutoStop WorkSpaces の場合、多数の同時ログインにより、WorkSpaces が使用可能になるまでの時間が大幅に長くなる可能性があります。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。
> - 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 のプロビジョニング後に有効にすることができます。

# 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 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、WorkSpaces 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。Microsoft でサポートされなくなった Windows のバージョンは動作する保証はなく、 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。

# ステップ 2: WorkSpaces アカウントが Microsoft BYOL で使用できるかどうかを判断する

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。このプロセスを完了するまで、Amazon WorkSpaces コンソールで [Enable BYOL] (BYOL の有効化) オプションは使用できません。

> **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 AcceptAccountLinkInvitation などの APIs を使用して AWS 、アカウントを接続できます。詳細については、「WorkSpaces で 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アカウントの BYOL 適格性を確認するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
2. ナビゲーションウィンドウで、[Account Settings] (アカウント設定) を選択し、[Bring your own license (BYOL)] で [View WorkSpaces BYOL settings] (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連絡するか、 AWS サポート 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 WorkSpacesの数
   - ランプアップ計画はどのような内容ですか?
   - WorkSpaces をリセラー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ると、BYOL 適格性を判断するために、これらのアカウントにデプロイされた WorkSpaces の総数が集計されます。これらの質問の両方に対する回答がはいの場合、アカウントをリンクできます。 CreateAccountLinkInvitations や AcceptAccountLinkInvitation などの APIs を使用して AWS 、アカウントを接続できます。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 適格性が確認されたら、次のステップに進むことができます。ここで、Amazon WorkSpaces コンソールで、アカウントのために BYOL を有効にします。

# ステップ 3: Amazon WorkSpaces コンソールを使用して、対象となる WorkSpaces アカウントの BYOL を有効にする Amazon WorkSpaces

「ステップ 2: WorkSpaces アカウントが Microsoft BYOL で使用できるかどうかを判断する」の手順に従って、WorkSpaces アカウントが Microsoft Bring Your Own License (BYOL) の使用に適格であることを確認したら、管理ネットワークインターフェイスを指定してアカウントの BYOL を有効にする必要があります。このインターフェイスは、セキュアな 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や、Amazon WorkSpaces が WorkSpace を管理できるようにするために使用されます。

> **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/v2/home「https://www.com」で WorkSpaces コンソールを開きます。

2. ナビゲーションウィンドウで、[Account Settings] (アカウント設定) を選択し、[Bring your own license (BYOL)] で [View WorkSpaces BYOL settings] (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 2: WorkSpaces アカウントが Microsoft BYOL で使用できるかどうかを判断する」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、指定した範囲内で使用可能な IP アドレス範囲を検索し、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連絡するか、 AWS サポート 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 によって、BYOL のアカウントが有効になっていれば、次のステップに進みます。

# ( オプション) Amazon EC2 Image Builder を使用する (Windows 11 のみ )

Amazon EC2 Image Builder は、raw ISO ファイルから Amazon マシンイメージ (AMI) を作成できます。この機能は Windows 11 システムでのみ使用できます。

Amazon EC2 Image Builder を使用して必要なイメージを作成する場合は、以下をスキップできます。

- the section called “ステップ 4: VM が BYOL 要件を満たしていることを確認する”
- the section called “ステップ 5: 仮想化環境から VM をエクスポートする”

ISO ファイルを AMI に変換する

1. ISO ファイルを S3 にアップロードします。「Amazon Simple Storage Service ユーザーガイド」の「オブジェクトのアップロード」を参照してください。
2. ISO ファイルを AMI に変換します。「EC2 Image Builder ユーザーガイド」の「Image Builder を使用した検証済み Windows ISO ディスクイメージのインポート」を参照してください。 EC2
3. the section called “ステップ 6: VM をイメージとして Amazon EC2 にインポートする” に進む

# ステップ 4: Amazon WorkSpaces の Windows VM が Microsoft BYOL の要件を満たしていることを確認する

> **Note**
>
> Amazon EC2 Image Builder を使用している場合は、「」に進むことができますthe section called “ステップ 6: VM をイメージとして Amazon EC2 にインポートする”。

「ステップ 3: Amazon WorkSpaces コンソールを使用して、対象となる WorkSpaces アカウントの BYOL を有効にする Amazon WorkSpaces 」の手順に従ってアカウントの BYOL を有効にしたら、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。確認するには、以下のステップで、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 PowerShell を開きます。Windows の [Start (スタート)] ボタンを選択して [Windows PowerShell] を右クリックし、[Run as administrator (管理者として実行)] を選択します。[User Account Control] (ユーザーアカウント制御) で、デバイスに変更を加えることを PowerShell に許可するかどうかを選択するメッセージが表示されたら、[Yes] (はい) を選択します。
2. PowerShell コマンドプロンプトで、BYOL Checker スクリプトが配置されているディレクトリに移動します。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、コンピュータ上の PowerShell 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の確認を求められたら、A と入力することで、すべての項目に「はい」を指定します。
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 Image Validation] (WorkSpaces イメージ検証) ダイアログボックスで、[Begin Tests] (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。

    また、Sysprep の実行を促すプロンプトも表示されます。プロンプトを閉じて、Sysprep はまだ実行しないでください。

12. VM をシャットダウンしてエクスポートします。詳細については、「VM Import/Export ユーザーガイド」の「VM の仮想化環境からのエクスポート」を参照してください。

13. (オプション) VM を起動し、BYOL Checker スクリプトをもう一度実行します。すべての検証に合格する必要があります。Sysprep の実行ボタンが付いた画面が再びポップアップ表示されます。[Run Sysprep] を選択します。Sysprep が成功した場合は、手順 12 でエクスポートした VM を Amazon Elastic Compute Cloud (Amazon EC2) にインポートできます。

    Sysprep が失敗した場合は、`%WINDIR%\System32\Sysprep\Panther` パスで Sysprep のログを確認し、手順 12 でエクスポートした VM に戻ってログに記録されている問題を解決し、修正した VM をエクスポートして手順 12 を再度完了します。その後、BYOL Checker スクリプトを再実行して、問題が解決していることを確認します。

    Sysprep が失敗する代表的な原因は、一部のユーザーにおいて Modern Appx Packages がアン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. 手順 12 でエクスポートした VM を Amazon EC2 にインポートします。

# 一般的なエラーメッセージとその解決策

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. [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 のインポートには、Workspaces_BYOL アカウントを有効にする必要があります

Workspaces_BYOL アカウントが有効になっている必要があります。詳細については、「Amazon WorkSpaces コンソールを使用して、アカウントのために 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。

BYOL WorkSpace イメージのインポートに使用されている Amazon マシンイメージには、C 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 のインポートには、自動ログオンが無効になっている必要があります。

自動ログオン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、`0` に設定する必要があり、設定しない場合、値 `DefaultUser` は消去され、自動ログオンは失敗します。

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 ブートモード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。

BYOL インポートでは、Windows リザーブドストレージの状態を無効にする必要があります

リザーブドストレージの状態を無効にするには

1. すべての Windows 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。
2. 新しい更新がないことを確認します。
3. 管理者として Powershell で次のいずれかのコマンドを実行します。
   - `Set-WindowsReservedStorageState -State Disabled`
   - `DISM.exe /Online /Set-ReservedStorageState /State:Disabled`
4. システムを再起動します。

> **Note**
>
> 予約ストレージが使用されている場合、無効になっていない可能性があり、次のエラーメッセージが返されます。`This operation is not supported when reserved`

```
storage is in use. Please wait for any servicing operations to
complete and then try again later.
```

BYOL インポートでは、ドライブ文字の使用が制限されています。

D: ドライブは WorkSpaces の制限付きドライブ文字です。イメージからインスタンスを起動するときにD:、 が使用されていないか、 にマッピングされないことを確認してください。

BYOL インポートには、選択したストリーミングプロトコルと互換性のない OS イメージがあります。

インポートされるイメージは、選択したストリーミングプロトコルではサポートされていません。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。

BYOL インポートはメモリの整合性と互換性がありません。

WorkSpace の Windows オペレーティングシステムで Credential Guard が有効になっている場合、メモリ整合性はサポートされていません。イメージのインポート中に無効にできない UEFILock でメモリ整合性が検出されました。UEFILock が無効になっているイメージをインポートしてください。「認証情報ガードを無効にする」を参照してください。

## SysPrep エラーメッセージとエラー修正のリスト

インポート対象の AMI に AppX パッケージがインストールされています。それらを削除し、イメージを再インポートしてください。

Modern AppX Packages が、ユーザーにインストールされている可能性があります。Powershell cmdlet、Remove-AppxPackage を実行して AppX パッケージを削除します。

> **Note**
>
> BYOL インポートプロセス中に、問題のある AppX パッケージがクリーンアップされ、Sysprep が再試行されます。イメージのインポートプロセスが引き続き失敗する場合は、AppX パッケージを手動でクリーンアップする必要があることを意味します。

インポート対象の AMI でストレージの予約が有効になっています。Windows Update の後で予約を無効にし、イメージを再インポートしてください。

ストレージの予約を無効にするには

1. `regedit.exe` と入力してレジストリエディタを開きます。
2. レジストリキー `HKLM\Software\Microsoft\Windows\CurrentVersion\ReserveManager` に移動します。
3. パラメータ `ShippedWithReserves` の値を `1` から `0` に変更します。
4. `ActiveScenario` の値を `0` に変更します。
5. 次のコマンドを使用して、Windows でストレージの予約を無効にします。

```
DISM.exe /Online /Set-ReservedStorageState /State:Disabled
```

インポート対象の AMI にウイルス対策ソフトウェアまたはスパイウェア対策ソフトウェアがインストールされています。ソフトウェアを削除してイメージを再インポートしてください。

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。詳細については、「ステップ 4: Amazon WorkSpaces の Windows VM が Microsoft BYOL の要件を満たしていることを確認する」を参照してください。

AMI SysPrep の実行中、インポート対象の AMI に不明なエラーが発生しました。

SysPrep が失敗した理由を特定できませんでした。 https://aws.amazon.com/support AWS のサポートにお問い合わせください。

# ステップ 5: Amazon WorkSpaces の仮想化環境から VM をエクスポートする

> **Note**
>
> Amazon EC2 Image Builder を使用している場合は、「」に進むことができますthe section called “ステップ 6: VM をイメージとして Amazon EC2 にインポートする”。

ステップ 4: Amazon WorkSpaces の Windows VM が Microsoft BYOL の要件を満たしていることを確認するの手順に従って VM が Microsoft BYOL の要件を満たしていることを確認したら、仮想化環境から VM をエクスポートする必要があります。これは、WorkSpaces で使用する BYOL 用のイメージを作成するために必要です。

エクスポートする 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 の仮想化環境からのエクスポート」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 AWS を使用した Windows 11 イメージの への持ち込み」を参照してください。

## ステップ 6: WorkSpaces の BYOL イメージを作成する準備として、VM をイメージとして Amazon EC2 にインポートする

Amazon EC2 Image Builder を使用して Windows 11 ISO をインポートしたら、以下の AMI のインポートに進みます。

「ステップ 5: Amazon WorkSpaces の仮想化環境から VM をエクスポートする」の手順に従って 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 リファレンスの ImportImage 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 7: Amazon WorkSpaces の 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、 を通じて 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 イメージにプレインストールされ、このイメージから起動するあらゆる WorkSpaces に含まれます。

> **Note**
>
> - PCoIP 使用の Graphics.g4dn および GraphicsPro.g4dn BYOL イメージは、Office 2019 のみをサポートしています。Office 2016 はサポートしていません。
> - DCV 使用の Graphics.g4dn および GraphicsPro.g4dn BYOL イメージは、[アプリケーションの管理] を使用して Office バンドルをサポートします (「WorkSpaces Personal でアプリケーションを管理する」を参照)。

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、WorkSpaces の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 がすでにインストールされている場合は、経由で 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 Visual Studio 2022、Microsoft Visio 2021、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 WorkSpaces の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で独自の Microsoft 365 ライセンスを使用するには、BYOL イメージ取り込みプロセスが完了した後に Microsoft 365 アプリケーションを BYOL イメージに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 のみをサポートしており、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 8: 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

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、Office サブスクリプションに使用される言語を選択します。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。

既定では、頻繁に使用する Office 言語パックが WorkSpaces にインストールされます。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、WorkSpaces で Office の言語設定を調整できます。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 管理用テンプレート (.admx/.adml) を使用して、すべての WorkSpaces ユーザーに対して既定の Office 言語設定を強制する

グループポリシーオブジェクト (GPO) 設定を使用して、WorkSpaces ユーザーに対して既定の Office 言語設定を適用できます。

> **Note**
>
> WorkSpaces ユーザーは、GPO によっ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 Personal で 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。管理用テンプレートファイルをダウンロードしたら、`office16.admx` および `office16.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。(`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。ディレクトリ管理用の 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、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 WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、Windows エクスプローラーを開き、アドレスバーに \\example.com のような組織の完全修飾ドメイン名 (FQDN) を入力します。
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 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) を開きます。
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、WorkSpace の次回のグループポリシーの更新後、および 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、次のいずれかを実行します。

    - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpace を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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: WorkSpaces で Office 言語のレジストリ設定を更新する

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\LanguageResources\UILanguage
- 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。Office LCID の一覧については、Microsoft のドキュメントの「Office 2016 の言語識別子および OptionState ID の値」を参照してください。

GPO 設定またはログオンスクリプトを使用して、これらのレジストリ設定を WorkSpaces 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 WorkSpaces に Office を追加する

次の操作を行って、Office のサブスクリプションを既存の BYOL WorkSpaces 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) – Microsoft Office、Microsoft Visual Studio 2022、Microsoft Visio、または Microsoft Project 2021 を既存の WorkSpaces にインストールして設定できます。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。
- WorkSpace の移行 – Office がインストールされた BYOL バンドルを準備したら、WorkSpace の移行機能を使用して、既存の BYOL WorkSpace を Office にサブスクライブしているこの BYOL バンドルに移行できます。詳細については、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。

> **Note**
>
> [アプリケーションの管理] オプションは、Microsoft Office 2021 や他のアプリケーション (Microsoft Visual Studio 2022、Microsoft Visio 2021、Microsoft Project 2021 など) を WorkSpaces にインストールする場合に使用できます。Microsoft Office 2016 または 2019 を WorkSpaces にインストールする場合は、「WorkSpaces Personal で WorkSpace を移行する」を使用してください。

## 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 やその他のアプリケーション (Microsoft Visual Studio 2022、Microsoft Visio 2021、Microsoft Project 2021 など) を既存の WorkSpaces にインストールできます。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。
- WorkSpace の移行 – 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している BYOL バンドルを作成する必要があります。次に、WorkSpaces の移行機能を使用して、Office にサブスクライブされている既存の BYOL WorkSpaces を、移行する 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 にサブスクライブしている 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 にサブスクライブされている既存の BYOL WorkSpaces 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、「WorkSpaces の移行」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 にサブスクライブされている WorkSpaces 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、WorkSpace からの Microsoft Office のアンインストールに限定されます。WorkSpaces 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用意する必要があります。

> **Note**
>
> アプリケーションの管理を使用して、Microsoft Office、Microsoft Visio、または Microsoft Project 2021 を WorkSpaces にインストールまたはアンインストールできます。Microsoft Office 2016 または 2019 バージョンは、WorkSpaces からのみ削除できます。Microsoft Office 2016 または 2019 を WorkSpaces にインストールするには、WorkSpaces を移行してください。

移行プロセスの詳細については、WorkSpaces Personal で WorkSpace を移行する 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 およびその他のアプリケーション (Microsoft Visio や Microsoft Project など) を、WorkSpaces からアンインストールできます。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。
- WorkSpace Spaces の移行 – 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 の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、「WorkSpaces Personal で WorkSpace を移行する」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 8: WorkSpaces コンソールを使用して BYOL イメージを作成する

「ステップ 6: WorkSpaces の BYOL イメージを作成する準備として、VM をイメージとして Amazon EC2 にインポートする」の手順に従って VM を Amazon EC2 にインポートしたら、以下の手順を実行して WorkSpaces の BYOL イメージを作成します。

> **Note**
>
> この手順を実行するには、 AWS Identity and Access Management 次の (IAM) アクセス許可があることを確認します。
>
> - WorkSpaces **`ImportWorkspaceImage`** 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 **`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 WorkSpaces に固有の IAM ポリシーの例については、WorkSpaces の Identity and Access Management を参照してください。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、GraphicsPro バンドルを作成するには、AWS サポート 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 イメージ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/v2/home「https://www.com」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 6: WorkSpaces の BYOL イメージを作成する準備として、VM をイメージとして 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、イメージに使用する プロトコル (PCoIP と DCV のいずれか) に応じて適切なバンドルタイプ (Regular、Graphics.g4dn、Graphics、GraphicsPro) 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 非対応のバンドル (Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro 以外のバンドル) の場合は、[Regular] を選択します。

   > **Note**
   >
   > - 現時点では、GraphicsPro イメージは、PCoIP プロトコルでのみ作成できます。

- Windows 11 イメージは DCV プロトコルでのみ作成できます。
- Graphics イメージと GraphicsPro イメージは Windows 11 で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、「ステップ 7: Amazon WorkSpaces の 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 Personal で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。

   > **Note**
   >
   > BYOL インポートプロセス中に、問題のある AppX パッケージがクリーンアップされ、Sysprep が再試行されます。イメージのインポートプロセスが引き続き失敗する場合は、AppX パッケージを手動でクリーンアップする必要があることを意味します。

# ステップ 9: WorkSpaces で BYOL イメージからカスタムバンドルを作成する

「ステップ 8: WorkSpaces コンソールを使用して BYOL イメージを作成する」の手順に従って BYOL イメージを作成したら、その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、WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する を参照してください。

# ステップ 10: WorkSpaces に BYOL イメージを使用するための専用ディレクトリを作成する

WorkSpaces の BYOL イメージを使用するには、この目的専用のディレクトリを作成する必要があります。

WorkSpaces のディレクトリを作成するには、「WorkSpaces Personal のディレクトリを作成する」を参照してください。ディレクトリを作成するときは、[専用 WorkSpaces を有効化] を必ず選択してください。

専用ハードウェアで実行されていない WorkSpaces 用の 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。また、ディレクトリを登録解除してから、専用 WorkSpaces のディレクトリとして再度登録することもできます。既存の AWS Directory Service ディレクトリの登録と登録解除の詳細については、「」を参照してくださいWorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する。

# ステップ 11: BYOL WorkSpaces を起動する

「」の手順に従って専用 WorkSpaces のディレクトリを登録したらステップ 8: WorkSpaces コンソールを使用して BYOL イメージを作成する、このディレクトリで BYOL WorkSpaces Personal と WorkSpaces Pools を起動できます。

## BYOL WorkSpaces Personal を起動する

個人用 WorkSpace を起動するには、「」を参照してくださいWorkSpaces Personal で WorkSpace を作成する。

## BYOL WorkSpaces Pools を起動する

WorkSpaces Pools を起動するには、個人用 WorkSpace を起動してその個人用 WorkSpace のイメージを作成し、そのイメージを使用してプールを起動する必要があります。

BYOL WorkSpaces Pools のイメージを作成するには

1. WorkSpaces Pools に使用する BYOL イメージの個人用 WorkSpace を起動します。WorkSpaces Personal の起動方法については、「WorkSpaces Personal で WorkSpace を作成する」を参照してください。

2. 個人用 WorkSpace にログインし、すべての Windows Update がインストールされていることを確認します。
3. Amazon EC2 の設定を更新します。Windows 10 を使用して EC2 設定を更新するには、「EC2Config の最新バージョンのインストール」を参照してください。Windows 11 を使用して EC2 設定を更新するには、「EC2Launch の最新バージョンのインストール」を参照してください。
4. Windows Defender の除外リストに追加します。詳細については、「Windows セキュリティに除外を追加する」を参照してください。

   Windows Defender の除外リストに次のフォルダを追加します。

   - `C:\Program Files\Amazon\*`
   - `C:\ProgramData\Amazon\*`
   - `C:\Program Files\NICE\*`
   - `C:\ProgramData\NICE\*`
   - `C:\Program Files (x86)\AWS Tools\*`
   - `C:\Program Files (x86)\AWS SDK for .NET\*`
   - `C:\AWS EUC\*` (これはセッションスクリプト用です)
5. 次のコマンドを入力して、起動時の Windows Update を無効にします。

```
Open powershell as admin-
    Run following command -

    New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Force
    New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -
Force
    Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
\AU" -Name "NoAutoUpdate" -Value 1 -Force
```

6. WorkSpace を再起動します。詳細については、「WorkSpaces Personal の WorkSpace を再起動する」を参照してください。

> **Note**
>
> BYOL WorkSpaces Pools のイメージを作成する前に、以下を実行することをお勧めします。
>
> - 不要なスタートアップアプリケーションを削除します。

- スケジュールされた不要なタスクを削除または無効にします。スタートメニューを開き、[スケジュールされたタスク] を選択し、無効にするタスクを選択してから、[無効化] を選択します。

7. 次のコマンドを入力して、再起動後に Image Checker を実行します。

```
C:\Program Files\Amazon\ImageChecker.exe
```

カスタム WorkSpaces イメージの作成の詳細については、「WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する」を参照してください。

8. Image Checker で見つかったエラーをすべて解決します。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。
9. Image Checker のすべてのテストに合格したら、WorkSpaces コンソールに戻ります。
10. ナビゲーションペインの [WorkSpaces] で、[個人] を選択します。BYOL 個人用 WorkSpaces を選択し、[アクション]、[イメージの作成] を選択します。
11. ナビゲーションペインで [ Images] を選択します。[イメージ] で、イメージが作成されているかどうかを確認します。

これで、作成したイメージで WorkSpaces Pools を起動できるようになりました。WorkSpaces Pools の起動方法については、「WorkSpaces プールを作成する」を参照してください。

# BYOL イメージのアップロードと作成に関する動画

BYOL イメージをアップロードする方法のデモについては、次の動画をご覧ください。

Microsoft Hyper-V で BYOL イメージを作成する方法のデモについては、次の動画をご覧ください。

VMware Workstation で BYOL イメージを作成する方法のデモについては、次の動画をご覧ください。

# WorkSpaces で 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 ライセンス付属の WorkSpaces を作成するために使用するイメージが含まれます。リンクされるすべてのアカウントは、同一の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 アカウントリンク用の API は、 AWS GovCloud (US) Regionでは使用できません。

**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. ターゲットアカウントが AcceptAccountLinkInvitation API を使用して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。

# WorkSpaces Personal の使用と管理

WorkSpaces Personal では、個人に割り当てられた物理デスクトップコンピュータと同様に、高度にパーソナライズされた専用のデスクトップを必要とするユーザーに向けてカスタマイズされた永続的な仮想デスクトップをプロビジョニングします。

各 WorkSpace は、仮想プライベートクラウド (VPC) とディレクトリに関連付けられ、WorkSpace とユーザーの情報を保存して管理します。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 WorkSpaces サービスによって、または AWS Managed Microsoft AD とも呼ばれ AWS Directory Serviceる Simple AD、AD Connector、または AWS Directory Service for Microsoft Active Directory のオプションを提供する によって管理されます。詳細については、AWS Directory Service 管理ガイドを参照してください。

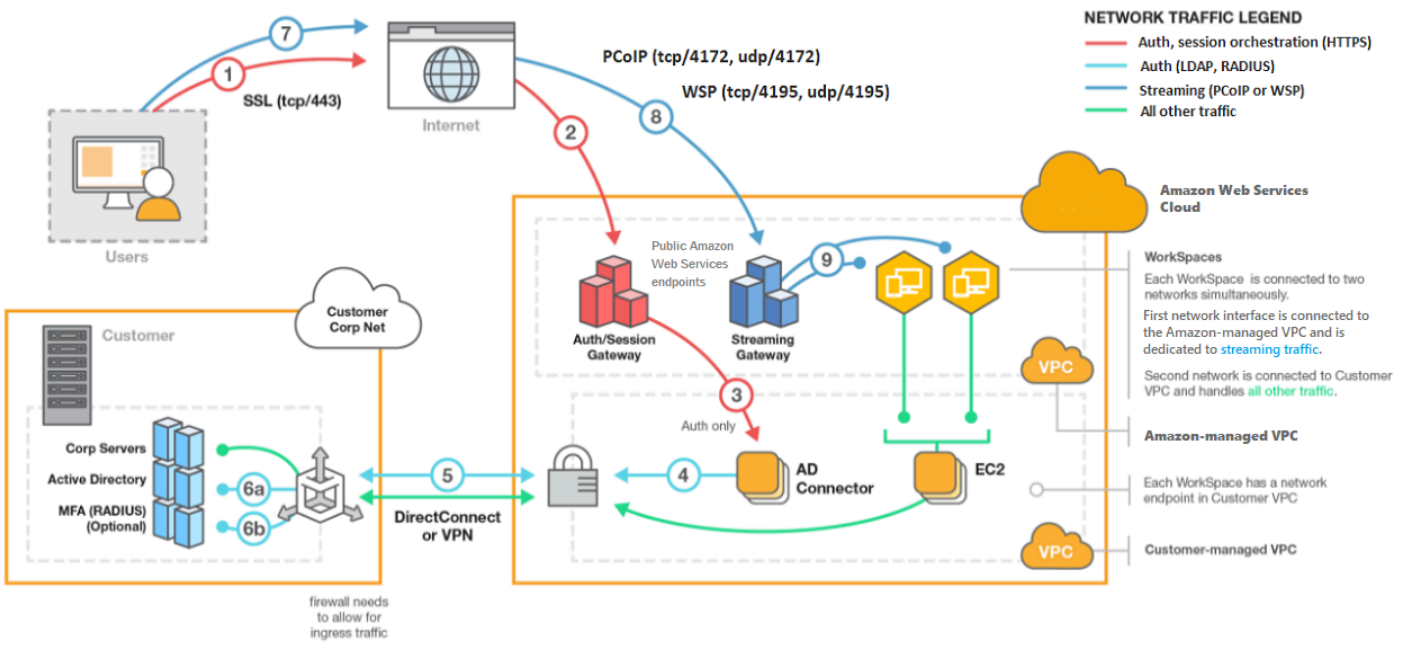
WorkSpaces は、IAM Identity Center (Amazon WorkSpaces によって管理されるディレクトリ用 ) 、Simple AD、AD Connector、または AWS Managed Microsoft AD ディレクトリを使用してユーザーを認証します。ユーザーは、サポートされているデバイスからクライアントアプリケーションを使用するか、Windows WorkSpaces の場合はウェブブラウザから、WorkSpaces にアクセスし、ディレクトリの認証情報を使用してログインします。ログイン情報は認証ゲートウェイに送信され、認証ゲートウェイはトラフィックを WorkSpace のディレクトリに転送します。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、WorkSpace へのピクセルストリーミングにポート 4172 (PCoIP) または 4195 (DCV) 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 (eth0) とプライマリネットワークインターフェイス (eth1) という 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、WorkSpace からのトラフィックが簡単にディレクトリに到達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。

AD Connector を使用する WorkSpaces のアーキテクチャを次の図に示します。

Amazon WorkSpaces Architectural Diagram




# WorkSpaces Personal で WorkSpace を作成するときのオプション

WorkSpace を作成するには、いくつかの方法があります。Quick Setup の手順や詳細設定の手順を使用できるほか、次のオプションから選択することもできます。

- WorkSpaces Personal 用の AWS Managed Microsoft AD ディレクトリを作成する
- WorkSpaces Personal で Simple AD ディレクトリを作成する
- WorkSpaces Personal の AD Connector を作成する
- WorkSpaces Personal の AWS Managed Microsoft AD ディレクトリとオンプレミスドメインの間に信頼関係を作成する
- WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する
- WorkSpaces Personal で専用のカスタムディレクトリを作成する

# WorkSpaces Personal の使用を開始する

WorkSpaces を初めて使用するユーザーは、Quick Setup または詳細設定で WorkSpaces Personal を設定できます。以下のチュートリアルでは、WorkSpaces と AWS Directory Serviceを使用して WorkSpace と呼ばれるクラウドベースのデスクトップをプロビジョニングする方法について説明します。

> **Note**
>
> WorkSpaces Pools の使用を開始する場合は、「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」を参照してください。

## WorkSpaces Personal の Quick Setup

このチュートリアルでは、WorkSpace WorkSpacesおよび を使用して、WorkSpace と呼ばれる仮想クラウドベースの Microsoft Windows、Amazon Linux 2、Ubuntu Linux、Rocky Linux、または Red Hat Enterprise Linux デスクトップをプロビジョニングする方法について説明します AWS Directory Service。

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 Personal のディレクトリを作成する」を参照してください。

> **Note**
>
> この Quick Setup オプションとチュートリアルは、WorkSpaces Pools には適用されません。

> **Note**
>
> クイックセットアップは、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 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に AWS アカウントを必要としません。
- 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。サポートされているリージョンの詳細については、「WorkSpaces AWS のリージョン別の料金」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 DCV) を選択する必要があります。詳細については、「WorkSpaces Personal のプロトコル」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、「the section called “WorkSpaces のディレクトリを管理する”」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、WorkSpaces Personal 用に VPC を設定する に記載されている要件を満たしていることを確認し、WorkSpaces Personal のディレクトリを作成する 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 に Simple AD ディレクトリを設定し、WorkDocs で有効にします。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。クイックセットアップによって最初に AWS アカウント 作成されるのは管理者です AWS アカウント。† 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、 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、「WorkSpaces Personal 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。

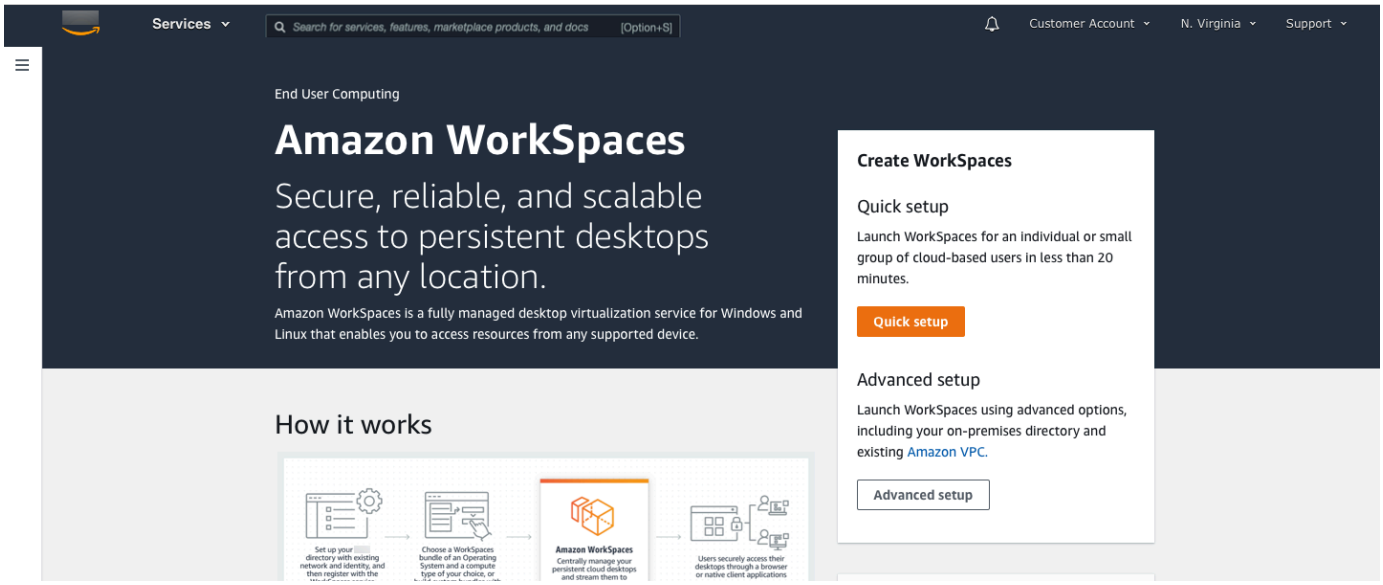
† クイックセットアップによって最初に AWS アカウント 作成されるのは管理者 です AWS アカウント。WorkSpaces コンソール AWS アカウント からこれを更新することはできません。このアカウントの情報は、他の誰とも共有しないでください。WorkSpaces を使用するように他のユーザーを招待するには、新しいユーザー AWS アカウント を作成します。

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。

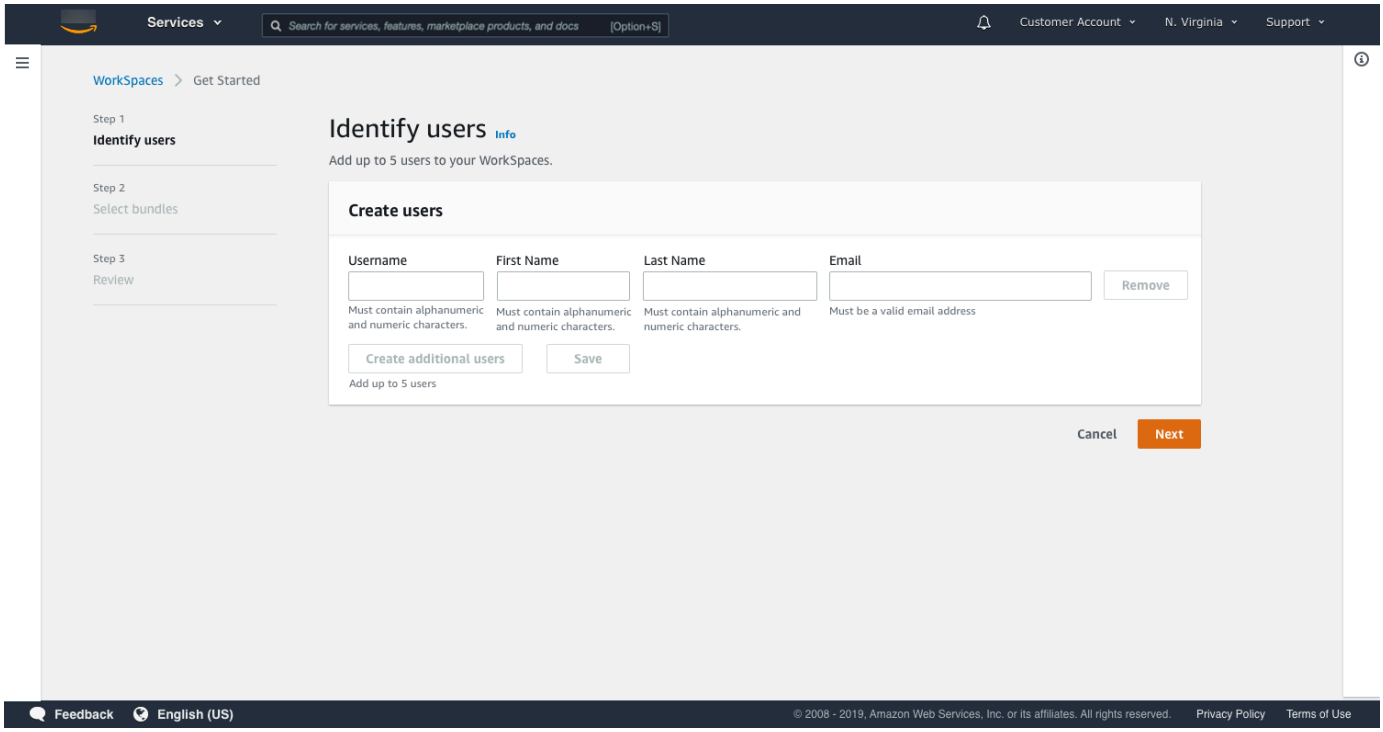
WorkSpace を起動するには

1. https://console.aws.amazon.com/workspaces/v2/home 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 Personal のディレクトリを作成する を参照してください。

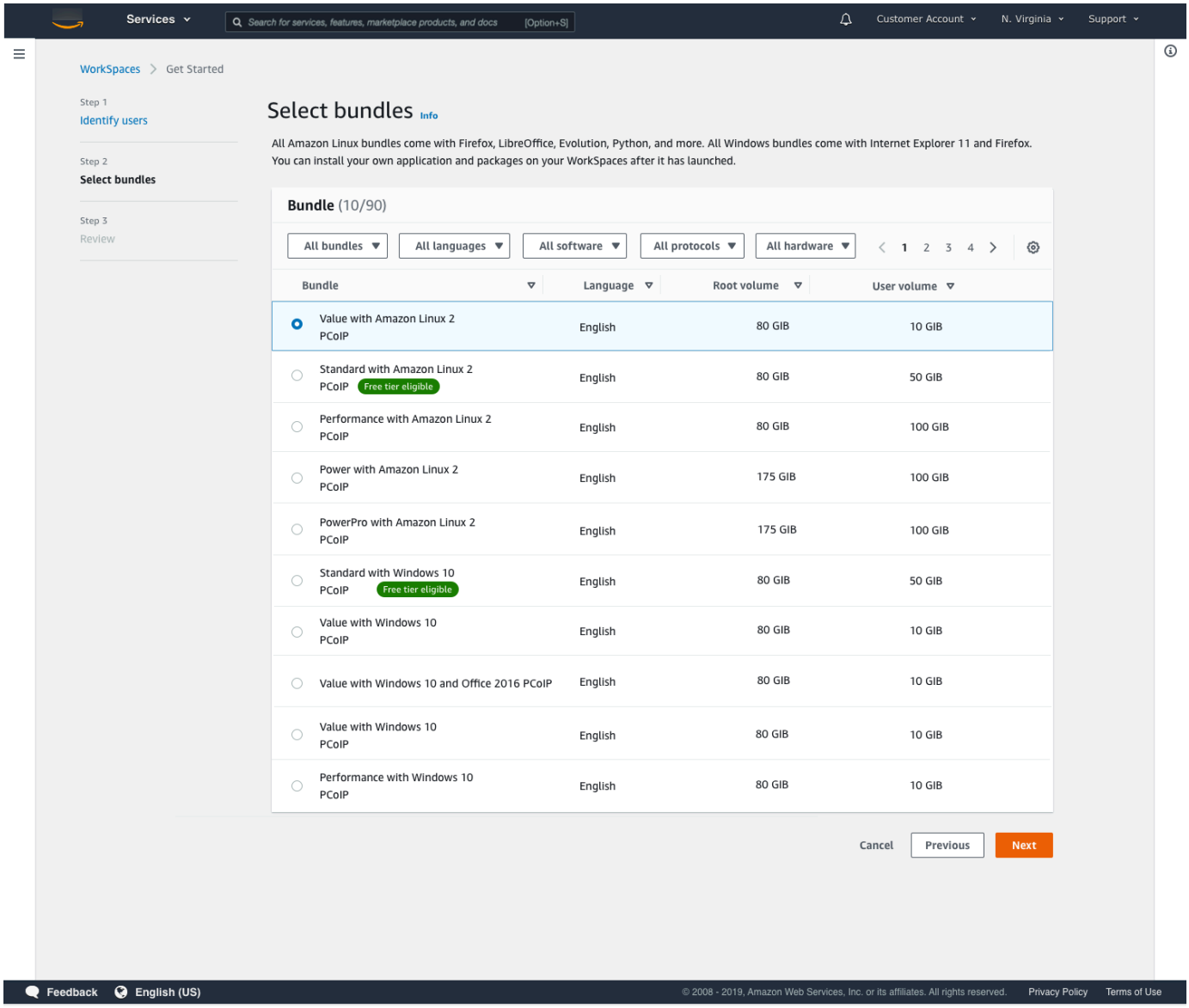



3. [Identify users] (ユーザーの識別) に [Username] (ユーザー名) と [First Name] (名前) を入力します。[Last Name] (姓) および [Emai] (E メール)。次いで、[次へ] を選択します。

> **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. [バンドル] で、該当するプロトコル (PCoIP または DCV) 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 Personal でディレクトリを削除する 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。

- WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する
- WorkSpaces Personal の管理
- WorkSpaces Personal 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 WorkSpaces Personal で WorkSpace を作成する 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 Personal のディレクトリを作成する 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 Personal 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、クラウドベースの Microsoft Windows、Amazon Linux、Ubuntu Linux、または Red Hat Enterprise Linux 仮想デスクトップ (WorkSpace とも呼ばれます) をプロビジョニングする方法を説明します。

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 の作成または管理に使用できる 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に AWS アカウントを必要としません。

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 WorkSpaces 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 DCV) を選択する必要があります。詳細については、「WorkSpaces Personal のプロトコル」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、「the section called “WorkSpaces のディレクトリを管理する”」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/v2/home で WorkSpaces コンソールを開きます。
2. 次のいずれかのディレクトリタイプを選択してから、[Next] (次へ) をクリックします。
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. ディレクトリ情報の入力
4. 2 つの異なるアベイラビリティーゾーンのいずれかから VPC 内の 2 つのサブネットを選択します。詳細については、「パブリックサブネットを持つ VPC の設定」を参照してください。
5. ディレクトリの情報を確認し、[Create directory] (ディレクトリの作成) を選択します。

# WorkSpaces Personal で WorkSpace を作成する

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。

個人用 WorkSpace を作成する前に、次のいずれかを実行してディレクトリを作成します。

- Simple AD ディレクトリを作成します。
- Microsoft Active Directory 用の AWS Directory Service を作成します。これは AWS Managed Microsoft AD とも呼ばれます。
- 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。

- Microsoft Entra ID を (IAM アイデンティティセンター経由で) ID ソースとして使用する専用ディレクトリを作成します。ディレクトリ内の WorkSpaces は、Microsoft Windows Autopilot のユーザードリブンモードによってネイティブの Entra ID に参加し、Microsoft Intune に登録されます。

  > **Note**
  >
  > このようなディレクトリは、現在、Windows 10 および 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces のみをサポートしています。

- 任意の ID プロバイダーを (IAM アイデンティティセンター経由で) ID ソースとして使用する専用ディレクトリを作成します。ディレクトリ内の WorkSpaces は、Microsoft Windows Autopilot のユーザードリブンモードによってネイティブの Entra ID に参加し、Microsoft Intune に登録されます。

  > **Note**
  >
  > このようなディレクトリは、現在、Windows 10 および 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces のみをサポートしています。

ディレクトリを作成したら、個人用 WorkSpace を作成できます。

個人用 WorkSpace を作成するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [WorkSpaces を起動]、[個人] を選択します。
4. [Workspaces の作成] を選択します。
5. [オンボーディング] (オプション) で、[お客様のユースケースに基づいた推奨事項]を選択すると、使用する WorkSpace のタイプに応じて推奨事項を取得できます。個人用 WorkSpaces を使用することがわかっている場合は、この手順を省略できます。
6. [次へ] を選択します。WorkSpaces が AD Connector を登録します。
7. [WorkSpaces の設定] で、次の情報を入力します。

   - [バンドル] で、WorkSpaces に使用するバンドルのタイプを以下から選択します。

- ベースの WorkSpaces バンドルを使用 - ドロップダウンからバンドルを 1 つ選択します。選択したバンドルタイプの詳細を確認するには、[バンドルの詳細] を選択します。プールに提供されるバンドルを比較するには、[すべてのバンドルを比較] を選択します。
- 独自のカスタムバンドルまたは BYOL バンドルを使用 - 過去に作成したバンドルを選択します。カスタムバンドルを作成するには、「WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する」を参照してください。

> **Note**
>
> 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。

- [実行モード] で、個人用 WorkSpaces をすぐに使用できるようにするかどうか、およびその支払い方法 (月単位または時間単位) を、以下から選択して設定します。
  - AlwaysOn — 月単位の固定料金で請求され、WorkSpaces を無制限に利用できます。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 — 時間単位で請求されます。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。
- [タグ] で、使用するキーペアの値を指定します。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。

8. [ディレクトリを選択] で、次の情報を入力します。

- 作成したディレクトリを選択します。ディレクトリを作成するには、[ディレクトリの作成] を選択します。個人用ディレクトリを作成する方法の詳細については、「WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する」を参照してください。
- 以下を実行して、個人用 WorkSpaces をプロビジョニングするユーザーをそのディレクトリから選択します。

  1. [ユーザーを作成] を選択します。
  2. ユーザーの [ユーザー名]、[名]、[姓]、および [E メール] を入力します。ユーザーを追加するには、[追加ユーザーの作成] を選択し、情報を入力します。

9. [カスタマイズ] (オプション) で、すべてのユーザーまたは特定のユーザーのバンドル、ルートおよびユーザーボリュームの暗号化、ユーザーボリュームをカスタマイズできます。
10. [Workspaces の作成] を選択します。WorkSpace の最初のステータスは [PENDING] です。作成が完了すると、ステータスは [使用可能] 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。
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。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。

> **Note**
>
> - AD Connector または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。
> - 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。
> - すべてのリージョンで、招待メールのテキストは英語 (米国) です。次のリージョンでは、英語のテキストの前に 2 番目の言語が付きます。
>   - アジアパシフィック (ソウル): 韓国語
>   - アジアパシフィック (東京): 日本語
>   - カナダ (中部): フランス語 (カナダ )
>   - 中国 (寧夏): 簡体字中国語

## 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 Personal で 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。

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

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 Personal のネットワークプロトコルとアクセス

WorkSpace 管理者は、WorkSpaces のネットワークとアクセスの管理方法を理解しておく必要があります。まずは、プロトコルから見ていきましょう。

## WorkSpaces Personal のプロトコル

Amazon WorkSpaces は PCoIP と DCV の 2 つのプロトコル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 WorkSpaces にアクセスする際に使用するデバイスの種類、WorkSpaces 上のオペレーティングシステム、ユーザーのネットワーク条件、ユーザーが双方向の動画サポートを必要としているかどうかなど、いくつかの要因によって決まります。

### 要件

DCV WorkSpaces は、以下の最小要件でのみサポートされます。

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
- Rocky Linux ホストエージェントバージョン 2.1.0.1628 以降
- Red Hat Enterprise Linux ホストエージェントバージョン 2.1.0.1628 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
- Ubuntu 22.04 クライアントバージョン 2024.x 以降
- Amazon WorkSpaces シンクライアント (詳細については、Amazon WorkSpaces シンクライアントドキュメント」を参照してください )
- Web Access

WorkSpace クライアントのバージョンとホストエージェントの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。

## DCV 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、グローバルに WorkSpaces にアクセスしているユーザーや、信頼性の低いネットワークを使用しているユーザーがいる場合です。
- 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 2022 を搭載した WorkSpaces バンドルで Web Access を使用する必要がある場合。
- Ubuntu WorkSpaces を使用する必要がある場合。
- Windows 11 BYOL WorkSpaces を使用する必要がある場合。
- Windows または Ubuntu の 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。
- YubiKey や Windows Hello などの WebAuthn 認証ツールを使用してセッション内でユーザー認証を行う必要がある場合。

## 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、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) リージョンで WorkSpaces を使用する必要がある場合。

> **Note**
>
> - ディレクトリには、PCoIP WorkSpaces と DCV WorkSpaces を混在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場合に限り、ユーザーは PCoIP WorkSpace と DCV WorkSpace の両方を持つことができます。同じユーザーが PCoIP WorkSpace と DCV WorkSpace を同じディレクトリ内に持つことはできません。ユーザーのための複数の WorkSpaces の作成の詳細については、WorkSpaces Personal で 1 人のユーザーに対して複数の WorkSpaces を作成する を参照してください。
- WorkSpaces 移行機能を使用して、2 つのプロトコル間で WorkSpace を移行できます。これを実行するためには、WorkSpace の再構築が必要です。詳細については、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
- WorkSpace を PCoIP バンドルで作成した場合は、ルートボリュームを保持したまま、再構築することなく 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、Power、PowerPro、GeneralPurpose.4xlarge,または GeneralPurpose.8xlarge バンドルのみを使用することをお勧めします。

以降のトピックでは、WorkSpaces Personal のネットワークとアクセスを管理する方法について詳しく説明します。

## WorkSpaces Personal 用に VPC を設定する

WorkSpaces は、仮想プライベートクラウド (VPC) で WorkSpaces を起動します。

WorkSpaces 用の 2 つのプライベートサブネットと、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、WorkSpaces の 2 つのパブリックサブネットを持つ VPC を作成し、各 WorkSpace にパブリック IP アドレスまたは Elastic IP アドレスを関連付けることもできます。

VPC 設計の考慮事項の詳細については、「Best Practices for VPCs and Networking in Amazon WorkSpaces Deployments」および「Best Practices for Deploying WorkSpaces - VPC Design」を参照してください。

内容

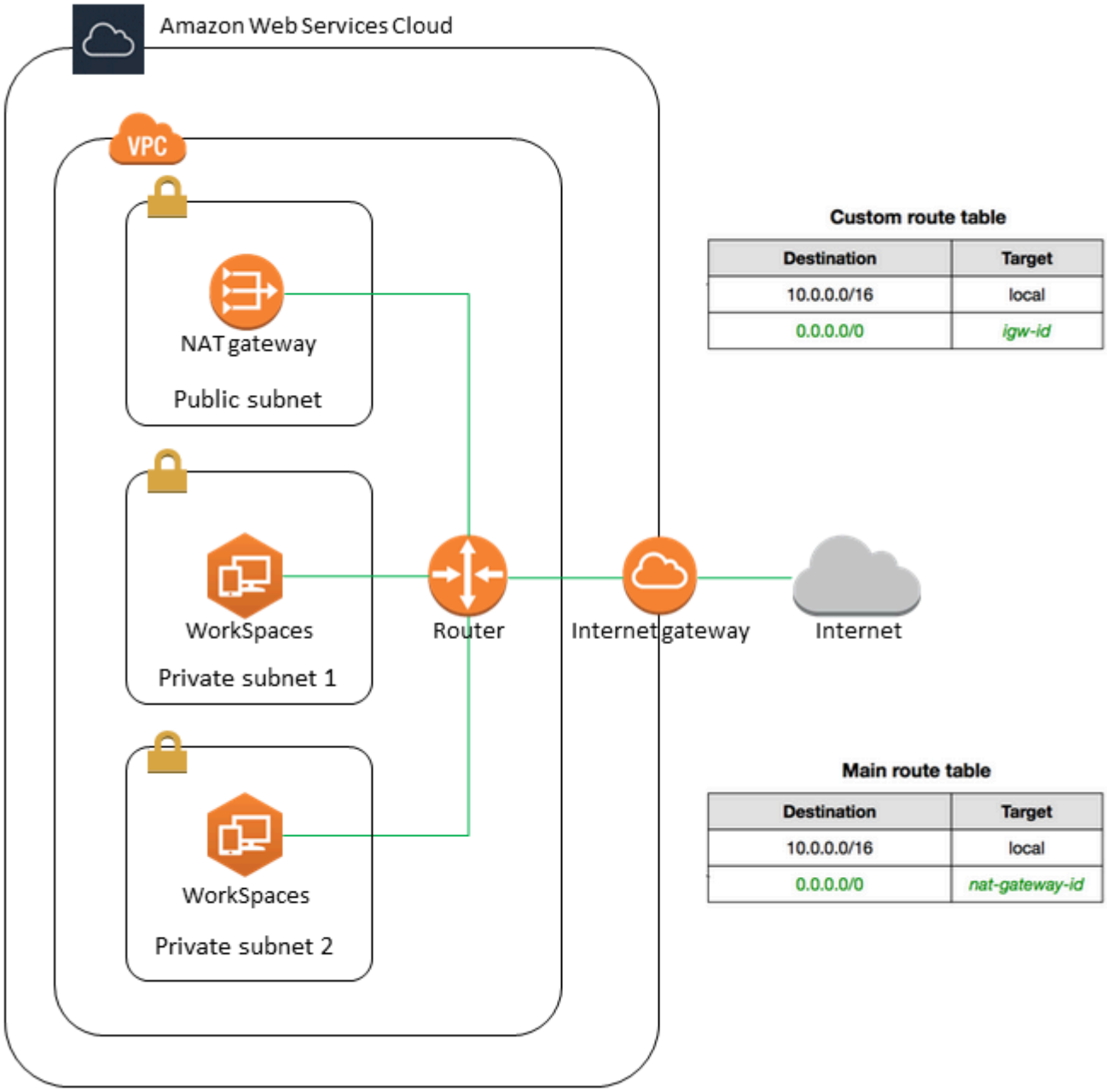
## 要件

VPC のサブネットは、WorkSpaces を起動するリージョン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。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。

> **Note**
>
> Amazon WorkSpaces は、サポートされ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利用できます。WorkSpaces で使用している 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 Personal のアベイラビリティーゾーンを参照してください。

## 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で 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 WorkSpace 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内の WorkSpaces に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に 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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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、「WorkSpaces Personal のアベイラビリティーゾーン」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、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、グラフィックスバンドルを起動する前に WorkSpaces サブネットで [auto-assign IPv6 addresses (IPv6 アドレスの自動割り当て)] 設定を一時的に無効にし 、グラフィックスバンドルの起動後にこの設定を再度有効にして (必要な場合)、他のバンドルに必要な IP アドレスが割り当てられるようにします。

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内の WorkSpaces へのインターネットアクセスを提供するには、ディレクトリを設定して Elastic IP アドレスを自動的に割り当てるか、手動で各 WorkSpace に Elastic IP アドレスを割り当てます。

タスク

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

### 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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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、「WorkSpaces Personal のアベイラビリティーゾーン」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、グラフィックスバンドルを起動する前に WorkSpaces サブネットで [auto-assign IPv6 addresses (IPv6 アドレスの自動割り当て)] 設定を一時的に無効にし 、グラフィックスバンドルの起動後にこの設定を再度有効にして (必要な場合)、他のバンドルに必要な IP アドレスが割り当てられるようにします。

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: WorkSpaces にパブリック IP アドレスを割り当てる

パブリック IP アドレスは、WorkSpaces に自動または手動で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。

WorkSpace にパブリック IP アドレスを手動で割り当てるには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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 の行を展開 (矢印アイコンを選択) し、[WorkSpace IP] の値を書き留めます。これは WorkSpaceのプライマリプライベート IP アドレスです。
4. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
5. ナビゲーションペインで [Elastic IP] を選択してください。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、[Network Interfaces] を選択してください。
7. WorkSpace 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、検索ボックスに [WorkSpace IP] 値 (前に書き留めた値) を入力し、Enter キーを押します。[WorkSpace IP] の値は、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 IP 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 値は、WorkSpaces VPC 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。

# WorkSpaces Personal のグローバル AWS アクセラレーター (AGA) を設定する

AWS Global Accelerator (AGA) は、WorkSpaces ディレクトリレベルまたは DCV プロトコルを実行している個々の WorkSpaces で有効にできます。有効にすると、サービスはストリーミングトラフィックを最も近い AWS エッジロケーションと AWS グローバルネットワークを経由して自動的にルーティングします。これは輻輳がなく冗長です。これにより、応答性と安定したストリーミングエクスペリエンスを実現できます。WorkSpaces サービスは AGA の使用を完全に管理し、アウトバウンドデータボリュームの制限の対象となります。

内容



## 要件

- WorkSpaces は、専用の AWS Global Accelerator (AGA) エンドポイントにさまざまなパブリック IPv4 アドレスを使用します。AGA を介して 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必ず設定してください。AGA エンドポイントがファイアウォールによってブロックされている場合、WorkSpaces ストリーミングトラフィックは AGA 経由でルーティングさ

れません。各 AWS リージョンの AGA エンドポイント IP 範囲の詳細については、「」を参照してくださいDCV ゲートウェイサーバー。

- AGA 経由で WorkSpaces にアクセスするには、ユーザーは WorkSpaces クライアントバージョン 5.23 以降を使用する必要があります。

## 制限

- DCV WorkSpaces に対してのみ AGA を有効にできます。WorkSpaces ディレクトリレベルで AGA を有効にすると、ディレクトリ内の DCV WorkSpaces にのみ適用されます。
- FIPS と IP アクセスコントロールグループの両方が有効になっているディレクトリ (またはディレクトリ内の WorkSpaces) に対して AGA を有効にすることはできません。ディレクトリの AGA を有効にする前に、FIPS または IP アクセスコントロールグループを無効にする必要があります。

## アウトバウンドデータの制限

WorkSpaces バンドルに適用されるデータボリュームの制限は次のとおりです。

- Value、Standard、Performance バンドル： ユーザーあたり 1 か月あたり 20 GB の AGA アウトバウンドデータが含まれます。
- Power、PowerPro、Graphics バンドル： ユーザーあたり 1 か月あたり 50 GB の AGA アウトバウンドデータが含まれます。

これらのアウトバウンドデータ制限は、WorkSpaces からストリーミングするユーザーのデータ使用量をカバーすることを目的としています。制限を超えると、WorkSpaces サービスは AGA の使用を制限し、case-by-caseで WorkSpaces トラフィックを AGA からルーティングすることがあります。

## WorkSpaces ディレクトリの AGA を有効にする

AGA 設定は、ディレクトリレベルで設定できます。この設定は、個々の WorkSpaces によって上書きされない限り、 ディレクトリ内のすべての DCV WorkSpaces に適用されます。

ディレクトリの AGA を有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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 列で、AGA 設定を構成するディレクトリのディレクトリ ID を選択します。

4. ディレクトリの詳細ページで、 AWS Global Accelerator (AGA) 設定セクションまで下にスクロールし、編集を選択します。
5. AGA を有効にする (自動 ) を選択します。
6. AGA がデフォルトで選択されている状態で、常に TCP を使用します。選択を解除すると、WorkSpaces クライアントは、クライアントの DCV ストリーミングプロトコル設定に基づいて、TCP または UDP を AGA で使用するかどうかを判断します。
7. [保存] を選択します。

WorkSpaces ディレクトリの AGA を有効にすると、ディレクトリ内の DCV WorkSpaces は、次のセッションから開始するストリーミングに AGA を使用します。再起動は必要ありません。

### 個々の WorkSpaces の AGA を有効にする

個々の WorkSpaces の AGA 設定を設定できます。これにより、WorkSpaces が関連付けられているディレクトリから継承された設定が上書きされます。

個々の WorkSpaces の AGA を有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com 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、Personal を選択します。
3. WorkSpace ID 列で、AGA 設定を設定する WorkSpace の WorkSpace ID を選択します。
4. WorkSpaces Details ページで、 AWS Global Accelerator (AGA) 設定セクションまで下にスクロールし、編集を選択します。
5. この WorkSpace の AGA 設定を手動で上書きするを選択します。
6. AGA を有効にする (自動 ) を選択します。
7. AGA がデフォルトで選択されている場合は、常に TCP を使用します。選択を解除すると、WorkSpaces クライアントは、クライアントの DCV ストリーミングプロトコル設定に基づいて、TCP または UDP を AGA で使用するかどうかを判断します。
8. [保存] を選択します。

## WorkSpaces Personal のアベイラビリティーゾーン

Amazon WorkSpaces で使用する仮想プライベートクラウド (VPC) を作成する場合、VPC のサブネットは WorkSpaces を起動するリージョン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。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に分散されるように、アベイラビリティーゾーンを各 AWS アカウントの名前に個別にマッピングします。たとえば、us-east-1a AWS アカウントのアベイラビリティーゾーンがus-east-1a別の AWS アカウント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。たとえば、 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利用できます。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 |

| リージョン名 | リージョンコード | サポートされる AZ ID |
| --- | --- | --- |
| 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 |
| 欧州 (パリ) | eu-west-3 | euw3-az1, euw3-az2, euw3-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 |
| 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 ID の詳細については、「Amazon EC2 ユーザーガイド」でリージョン、アベイラビリティーゾーン、およびローカルゾーンの説明を参照してください。

# WorkSpaces Personal の IP アドレスとポートの要件

WorkSpaces に接続するには、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 サービス (サブセットでグループ化) の IP アドレス範囲に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 リージョンによって異なります。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、のAWS 「IP アドレス範囲」を参照してくださいAmazon Web Services 全般のリファレンス。

その他のアーキテクチャ図については、「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。

## 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は、次のポートでアウトバウンドの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 (UDP と 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 が存在するリージョンの 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します。このポートは、WorkSpace があるリージョンのヘルスチェックサーバーと PCoIP ゲートウェイに対して開く必要があります。詳細については、「ヘルスチェックサーバー」および「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、UDP のポート 4172 トラフィック (デスクトップトラフィック) に対するプロキシサーバーの使用も、TLS の復号と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、DCV 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します。このポートは、WorkSpace があるリージョンの DCV ゲートウェイの IP アドレス範囲とヘルスチェックサーバーに対して開放する必要があります。詳細については、「ヘルスチェックサーバー」および「DCV ゲートウェイサーバー」を参照してください。

DCV WorkSpaces の場合、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 トラフィックに対する HTTP プロキシサーバーの使用をサポートしていますが、プロキシの使用はお勧めしません。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 WorkSpaces、および Ubuntu WorkSpaces 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。

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。
- WorkSpaces クライアントアプリケーションは、最適なパフォーマンスを得るために、まず UDP (QUIC) を使用してストリーミングを試みます。クライアントネットワークが TCP

のみを許可する場合、TCP が使用されます。WorkSpaces ウェブクライアントは、TCP ポート 4195 または 443 経由で接続します。ポート 4195 がブロックされている場合、クライアントはポート 443 経由でのみ への接続を試みます。

## Web Access のポート

WorkSpaces Web Access は、次のポートでアウトバウンドアクセスする必要があります。

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。WorkSpace があるリージョンの EC2 サブセット内の IP アドレス範囲をすべて開放する必要があります。

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。WorkSpace があるリージョンの EC2 サブセット内の IP アドレス範囲をすべて開放する必要があります。

ポート 4195 (UDP と TCP)

DCV 用に設定された WorkSpaces では、WorkSpaces デスクトップのストリーミングにこのポートが使用されます。このポートは、DCV ゲートウェイ の 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、「DCV ゲートウェイサーバー」を参照してください。

DCV の Web Access 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 WorkSpaces、または Ubuntu WorkSpaces 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。

> **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。
> - WorkSpaces クライアントアプリケーションは、最適なパフォーマンスを得るために、まず UDP (QUIC) を使用してストリーミングを試みます。クライアントネットワークが TCP のみを許可する場合、TCP が使用されます。WorkSpaces ウェブクライアントは、TCP ポート 4195 または 443 経由で接続します。ポート 4195 がブロックされている場合、クライアントはポート 443 経由でのみ への接続を試みます。

通常、ウェブブラウザは、ストリーミングトラフィックに使用するために、高範囲のソースポートをランダムに選択します。WorkSpaces Web Access は、ブラウザが選択した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 WorkSpaces サービスにアクセスしようとしているネットワーク上の許可リストに、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/<br>• AWS GovCloud (米国西部) リージョンの場合：<br><br>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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン (IPv4):<br>• https://skylight-client-ds.us-east-1.amazonaws.com<br>• https://skylight-client-ds.us-west-2.amazonaws.com<br>• https://skylight-client-ds.ap-south-1.amazonaws.com<br>• https://skylight-client-ds.ap-northeast-2.amazonaws.com<br>• https://skylight-client-ds.ap-southeast-1.amazonaws.com<br>• https://skylight-client-ds.ap-southeast-2.amazonaws.com<br>• https://skylight-client-ds.ap-northeast-1.amazonaws.com<br>• https://skylight-client-ds.ca-central-1.amazonaws.com<br>• https://skylight-client-ds.eu-central-1.amazonaws.com<br>• https://skylight-client-ds.eu-west-1.amazonaws.com<br>• https://skylight-client-ds.eu-west-2.amazonaws.com<br>• https://skylight-client-ds.eu-west-3.amazonaws.com<br>• https://skylight-client-ds.sa-east-1.amazonaws.com<br>• https://skylight-client-ds.af-south-1.amazonaws.com<br>• https://skylight-client-ds.il-central-1.amazonaws.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • AWS GovCloud (米国西部) リージョンの場合：<br><br>https://skylight-client-ds.us-gov-west-1.amazonaws.com<br>• AWS GovCloud (米国東部) リージョンの場合：<br><br>https://skylight-client-ds.us-gov-east-1.amazonaws.com<br><br>• AWS GovCloud (米国西部) リージョンの場合：<br><br>https://skylight-client-ds.us-gov-west-1.amazonaws.com<br>• AWS GovCloud (米国東部) リージョンの場合：<br><br>https://skylight-client-ds.us-gov-east-1.amazonaws.com<br><br>ドメイン (IPv6):<br><br>• https://skylight-client-ds.eu-west-2.api.aws<br>• https://skylight-client-ds.eu-west-1.api.aws<br>• https://skylight-client-ds.us-east-1.api.aws<br>• https://skylight-client-ds.ap-southeast-1.api.aws<br>• https://skylight-client-ds.sa-east-1.api.aws<br>• https://skylight-client-ds.ap-northeast-1.api.aws<br>• https://skylight-client-ds.us-west-2.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://skylight-client-ds.ap-southeast-2.api.aws<br>• https://skylight-client-ds.ap-south-1.api.aws<br>• https://skylight-client-ds.af-south-1.api.aws<br>• https://skylight-client-ds.eu-central-1.api.aws<br>• https://skylight-client-ds.ap-northeast-2.api.aws<br>• https://skylight-client-ds.il-central-1.api.aws<br>• https://skylight-client-ds.ca-central-1.api.aws<br>• https://skylight-client-ds.us-gov-east-1.api.aws<br>• https://skylight-client-ds.us-gov-west-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| ダイナミックメッセージングサービス (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 (IPv4):<br>• https://ws-client-service.us-east-1.amazonaws.com<br>• https://ws-client-service.us-west-2.amazonaws.com<br>• https://ws-client-service.ap-south-1.amazonaws.com<br>• https://ws-client-service.ap-northeast-2.amazonaws.com<br>• https://ws-client-service.ap-southeast-1.amazonaws.com<br>• https://ws-client-service.ap-southeast-2.amazonaws.com<br>• https://ws-client-service.ap-northeast-1.amazonaws.com<br>• https://ws-client-service.ca-central-1.amazonaws.com<br>• https://ws-client-service.eu-central-1.amazonaws.com<br>• https://ws-client-service.eu-west-1.amazonaws.com<br>• https://ws-client-service.eu-west-2.amazonaws.com<br>• https://ws-client-service.eu-west-3.amazonaws.com<br>• https://ws-client-service.sa-east-1.amazonaws.com<br>• https://ws-client-service.af-south-1.amazonaws.com<br>• https://ws-client-service.il-central-1.amazonaws.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • AWS GovCloud (米国西部) リージョンの場合：<br><br>https://ws-client-service.us-gov-west-1.amazonaws.com<br>• AWS GovCloud (米国東部) リージョンの場合：<br><br>https://ws-client-service.us-gov-east-1.amazonaws.com<br><br>ドメイン (IPv6):<br><br>• https://ws-client-service.eu-west-2.api.aws<br>• https://ws-client-service.eu-west-1.api.aws<br>• https://ws-client-service.us-east-1.amazonaws.com<br>• https://ws-client-service.ap-southeast-1.api.aws<br>• https://ws-client-service.sa-east-1.api.aws<br>• https://ws-client-service.ap-northeast-1.api.aws<br>• https://ws-client-service.us-west-2.api.aws<br>• https://ws-client-service.ap-southeast-2.api.aws<br>• https://ws-client-service.ap-south-1.api.aws<br>• https://ws-client-service.af-south-1.api.aws<br>• https://ws-client-service.eu-central-1.api.aws<br>• https://ws-client-service.ap-northeast-2.api.aws<br>• https://ws-client-service.il-central-1.api.aws<br>• https://ws-client-service.ca-central-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://ws-client-service.us-gov-east-1.api.aws<br>• https://ws-client-service.us-gov-west-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/*<region>*/*<directory ID>*<br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• Legacy — https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br>• 米国東部 (バージニア北部) — https://d2h1yryv1jxiq.cloudfront.net/<br>• 米国西部 (オレゴン) — https://d1fq42e1gi7rtq.cloudfront.net/<br>• アジアパシフィック (ムンバイ) — https://d1ctsk4u02kky7.cloudfront.net/<br>• アジアパシフィック (ソウル) — https://dyoj3cw6iktvg.cloudfront.net<br>• アジアパシフィック (シンガポール) — https://d1525ef92caquk.cloudfront.net/<br>• 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/<br>• カナダ (中部) — https://d1ebdk07rro1qy.cloudfront.net/<br>• 欧州 (フランクフルト) — https://d39q4y7cndearu.cloudfront.net/<br>• 欧州 (アイルランド) — https://d2127w6wvrc6l3.cloudfront.net/<br>• 欧州 (ロンドン) — https://df4ahgpxbxqy2.cloudfront.net/<br>• 欧州 (パリ) — https://d2kmf63k5sit88.cloudfront.net/<br>• 南米 (サンパウロ) — https://d2nezqurrjvain.cloudfront.net/<br>• アフリカ (ケープタウン) — https://dr6ry0pwaoy23.cloudfront.net<br>• イスラエル (テルアビブ) — https://d2kmf63k5sit88.cloudfront.net<br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 米国東部 (バージニア北部) — https://d32i4gd7pg4909.cloudfront.net/<br>• 米国西部 (オレゴン) — https://d18af777lco7lp.cloudfront.net/<br>• アジアパシフィック (ムンバイ) — https://d78hovzzqqtsb.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 (ソウル) — https://dtyv4uwoh7ynt.cloudfront.net/<br>• アジアパシフィック (シンガポール) — https://d3qzmd7y07pz0i.cloudfront.net/<br>• アジアパシフィック (シドニー) — https://dwcpoxuuza83q.cloudfront.net/<br>• アジアパシフィック (東京) — https://d2c2t8mxjhq5z1.cloudfront.net/<br>• カナダ (中部) — https://d2wfbsypmqjmog.cloudfront.net/<br>• 欧州 (フランクフルト) — https://d1whcm49570jjw.cloudfront.net/<br>• 欧州 (アイルランド) — https://d3pgffbf39h4k4.cloudfront.net/<br>• 欧州 (ロンドン) — https://d16q6638mh01s7.cloudfront.net/<br>• 欧州 (パリ) — https://d1a3pnge9on3sx.cloudfront.net/<br>• 南米 (サンパウロ) — https://d2lh2qc5bdoq4b.cloudfront.net/<br>• アフリカ (ケープタウン) — https://di5ygl2cs0mrh.cloudfront.net/<br>• イスラエル (テルアビブ) — https://d1a3pnge9on3sx.cloudfront.net<br><br>AWS GovCloud (米国西部) リージョンの場合：<br>• お客様のディレクトリ設定:<br>https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID> |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • 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:<br><br>https://workspace-client-assets-pdt.s3-us-gov-west-1.amazonaws.com<br>• 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:<br><br>https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css<br>• ログインページの JavaScript ファイル:<br><br>該当しない<br><br>AWS GovCloud (米国東部) リージョンの場合：<br>• お客様のディレクトリ設定:<br><br>https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID><br>• 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:<br><br>https://workspace-client-assets-pdt.s3-us-gov-east-1.amazonaws.com<br>• 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:<br><br>https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css<br>• ログインページの JavaScript ファイル:<br><br>該当しません |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| 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.af-south-1.signin.aws<br>• https://smartcard.af-south-1.apps.signin.aws<br>• https://smartcard.ap-south-1.signin.aws<br>• https://smartcard.ap-south-1.apps.signin.aws<br>• https://smartcard.ap-southeast-1.signin.aws<br>• https://smartcard.ap-southeast-1.apps.signin.aws<br>• https://smartcard.ap-southeast-2.signin.aws<br>• https://smartcard.ap-southeast-2.apps.signin.aws<br>• https://smartcard.ap-northeast-1.signin.aws<br>• https://smartcard.ap-northeast-1.apps.signin.aws<br>• https://smartcard.ap-northeast-2.signin.aws<br>• https://smartcard.ap-northeast-2.apps.signin.aws<br>• https://smartcard.ca-central-1.signin.aws<br>• https://smartcard.ca-central-1.apps.signin.aws<br>• https://smartcard.eu-central-1.signin.aws<br>• https://smartcard.eu-central-1.apps.signin.aws<br>• https://smartcard.eu-west-1.signin.aws<br>• https://smartcard.eu-west-1.apps.signin.aws<br>• https://smartcard.eu-west-2.signin.aws<br>• https://smartcard.eu-west-2.apps.signin.aws<br>• https://smartcard.eu-west-3.signin.aws<br>• https://smartcard.eu-west-3.apps.signin.aws<br>• https://smartcard.il-central-1.signin.aws<br>• https://smartcard.il-central-1.apps.signin.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://smartcard.sa-east-1.signin.aws<br>• https://smartcard.sa-east-1.apps.signin.aws<br>• https://smartcard.us-east-1.signin.aws<br>• https://smartcard.us-east-1.apps.signin.aws<br>• https://smartcard.us-west-2.signin.aws<br>• https://smartcard.us-west-2.apps.signin.aws<br>• https://smartcard.us-gov-east-1.signin-fips.amazonaws-us-gov.com<br>• https://smartcard.us-gov-east-1.apps.signin-fips.amazonaws-us-gov.com<br>• https://smartcard.us-gov-west-1.signin.amazonaws-us-gov.com<br>• https://smartcard.us-gov-west-1.apps.signin.amazonaws-us-gov.com<br>• https://smartcard.signin.amazonaws-us-gov.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| ユーザーログインページ | • https://af-south-1.signin.aws<br>• https://af-south-1.signin.aws.amazon.com<br>• https://af-south-1.sso.signin.aws<br>• https://af-south-1.apps.signin.aws<br>• https://ap-south-1.signin.aws<br>• https://ap-south-1.signin.aws.amazon.com<br>• https://ap-south-1.sso.signin.aws<br>• https://ap-south-1.apps.signin.aws<br>• https://ap-southeast-1.signin.aws<br>• https://ap-southeast-1.signin.aws.amazon.com<br>• https://ap-southeast-1.sso.signin.aws<br>• https://ap-southeast-1.apps.signin.aws<br>• https://ap-southeast-2.signin.aws<br>• https://ap-southeast-2.signin.aws.amazon.com<br>• https://ap-southeast-2.sso.signin.aws<br>• https://ap-southeast-2.apps.signin.aws<br>• https://ap-northeast-1.signin.aws<br>• https://ap-northeast-1.signin.aws.amazon.com<br>• https://ap-northeast-1.sso.signin.aws<br>• https://ap-northeast-1.apps.signin.aws<br>• https://ap-northeast-2.signin.aws<br>• https://ap-northeast-2.signin.aws.amazon.com<br>• https://ap-northeast-2.sso.signin.aws<br>• https://ap-northeast-2.apps.signin.aws<br>• https://ca-central-1.signin.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://ca-central-1.signin.aws.amazon.com<br>• https://ca-central-1.sso.signin.aws<br>• https://ca-central-1.apps.signin.aws<br>• https://eu-central-1.signin.aws<br>• https://eu-central-1.signin.aws.amazon.com<br>• https://eu-central-1.sso.signin.aws<br>• https://eu-central-1.apps.signin.aws<br>• https://eu-west-1.signin.aws<br>• https://eu-west-1.signin.aws.amazon.com<br>• https://eu-west-1.sso.signin.aws<br>• https://eu-west-1.apps.signin.aws<br>• https://eu-west-2.signin.aws<br>• https://eu-west-2.signin.aws.amazon.com<br>• https://eu-west-2.sso.signin.aws<br>• https://eu-west-2.apps.signin.aws<br>• https://eu-west-3.signin.aws<br>• https://eu-west-3.signin.aws.amazon.com<br>• https://eu-west-3.sso.signin.aws<br>• https://eu-west-3.apps.signin.aws<br>• https://il-central-1.signin.aws<br>• https://il-central-1.signin.aws.amazon.com<br>• https://il-central-1.sso.signin.aws<br>• https://il-central-1.apps.signin.aws<br>• https://sa-east-1.signin.aws<br>• https://sa-east-1.signin.aws.amazon.com<br>• https://sa-east-1.sso.signin.aws<br>• https://sa-east-1.apps.signin.aws<br>• https://us-east-1.signin.aws<br>• https://us-east-1.signin.aws.amazon.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://us-east-1.sso.signin.aws<br>• https://us-east-1.apps.signin.aws<br>• https://us-west-2.signin.aws<br>• https://us-west-2.signin.aws.amazon.com<br>• https://us-west-2.sso.signin.aws<br>• https://us-west-2.apps.signin.aws<br>• https://us-gov-east-1.signin-fips.amazonaws-us-gov.com<br>• https://us-gov-east-1.sso.signin-fips.aws-us-gov.com<br>• https://us-gov-east-1.apps.signin-fips.aws-us-gov.com<br>• https://us-gov-west-1.signin.amazonaws-us-gov.com<br>• https://us-gov-west-1.sso.signin.aws-us-gov.com<br>• https://us-gov-west-1.apps.signin.aws-us-gov.com<br><br>https://*directory_id* .awsapps.com/<br><br>**Note**<br>ディレクトリ ID はお客様のドメインです。<br><br>AWS GovCloud (米国西部) および AWS GovCloud (米国東部) リージョンの場合：<br><br>https://login.us-gov-home.awsapps.com/directory/*directory id*/ |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | **Note**<br>ディレクトリ 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 (IPv4):<br>• https://ws-broker-service.us-east-1.amazonaws.com<br>• https://ws-broker-service-fips.us-east-1.amazonaws.com<br>• https://ws-broker-service.us-west-2.amazonaws.com<br>• https://ws-broker-service-fips.us-west-2.amazonaws.com<br>• https://ws-broker-service.ap-south-1.amazonaws.com<br>• https://ws-broker-service.ap-northeast-2.amazonaws.com<br>• https://ws-broker-service.ap-southeast-1.amazonaws.com<br>• https://ws-broker-service.ap-southeast-2.amazonaws.com<br>• https://ws-broker-service.ap-northeast-1.amazonaws.com<br>• https://ws-broker-service.ca-central-1.amazonaws.com<br>• https://ws-broker-service.eu-central-1.amazonaws.com<br>• https://ws-broker-service.eu-west-1.amazonaws.com<br>• https://ws-broker-service.eu-west-2.amazonaws.com<br>• https://ws-broker-service.eu-west-3.amazonaws.com<br>• https://ws-broker-service.sa-east-1.amazonaws.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://ws-broker-service.af-south-1.amazonaws.com<br>• https://ws-broker-service.il-central-1.amazonaws.com<br>• https://ws-broker-service.us-gov-west-1.amazonaws.com<br>• https://ws-broker-service-fips.us-gov-west-1.amazonaws.com<br>• https://ws-broker-service.us-gov-east-1.amazonaws.com<br>• https://ws-broker-service-fips.us-gov-east-1.amazonaws.com<br><br>ドメイン (IPv6):<br><br>• https://ws-broker-service.eu-west-3.api.aws<br>• https://ws-broker-service.eu-west-2.api.aws<br>• https://ws-broker-service.eu-west-1.api.aws<br>• https://ws-broker-service.us-east-1.api.aws<br>• https://ws-broker-service.us-west-2.api.aws<br>• https://ws-broker-service.eu-central-1.api.aws<br>• https://ws-broker-service.ap-northeast-1.api.aws<br>• https://ws-broker-service.ap-northeast-2.api.aws<br>• https://ws-broker-service.ap-southeast-1.api.aws<br>• https://ws-broker-service.ap-southeast-2.api.aws<br>• https://ws-broker-service.sa-east-1.api.aws<br>• https://ws-broker-service.ap-south-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://ws-broker-service.af-south-1.api.aws<br>• https://ws-broker-service.ca-central-1.api.aws<br>• https://ws-broker-service.il-central-1.api.aws<br>• https://ws-broker-service.us-gov-west-1.api.aws<br>• https://ws-broker-service.us-gov-east-1.api.aws<br>• https://ws-broker-service-fips.us-west-2.api.aws<br>• https://ws-broker-service-fips.us-east-1.api.aws<br>• https://ws-broker-service-fips.us-gov-west-1.api.aws<br>• https://ws-broker-service-fips.us-gov-east-1.api.aws |

| 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 (IPv4):<br>• https://workspaces.us-east-1.amazonaws.com<br>• https://workspaces-fips.us-east-1.amazonaws.com<br>• https://workspaces.us-west-2.amazonaws.com<br>• https://workspaces-fips.us-west-2.amazonaws.com<br>• https://workspaces.ap-south-1.amazonaws.com<br>• https://workspaces.ap-northeast-2.amazonaws.com<br>• https://workspaces.ap-southeast-1.amazonaws.com<br>• https://workspaces.ap-southeast-2.amazonaws.com<br>• https://workspaces.ap-northeast-1.amazonaws.com<br>• https://workspaces.ca-central-1.amazonaws.com<br>• https://workspaces.eu-central-1.amazonaws.com<br>• https://workspaces.eu-west-1.amazonaws.com<br>• https://workspaces.eu-west-2.amazonaws.com<br>• https://workspaces.eu-west-3.amazonaws.com<br>• https://workspaces.sa-east-1.amazonaws.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://workspaces.af-south-1.amazonaws.com<br>• https://workspaces.il-central-1.amazonaws.com<br>• https://workspaces.us-gov-west-1.amazonaws.com<br>• https://workspaces-fips.us-gov-west-1.amazonaws.com<br>• https://workspaces.us-gov-east-1.amazonaws.com<br>• https://workspaces-fips.us-gov-east-1.amazonaws.com<br><br>ドメイン (IPv6):<br><br>• https://workspaces.eu-west-3.api.aws<br>• https://workspaces.eu-west-2.api.aws<br>• https://workspaces.eu-west-1.api.aws<br>• https://workspaces.us-east-1.api.aws<br>• https://workspaces.us-west-2.api.aws<br>• https://workspaces.eu-central-1.api.aws<br>• https://workspaces.ap-northeast-1.api.aws<br>• https://workspaces.ap-northeast-2.api.aws<br>• https://workspaces.ap-southeast-1.api.aws<br>• https://workspaces.ap-southeast-2.api.aws<br>• https://workspaces.sa-east-1.api.aws<br>• https://workspaces.ap-south-1.api.aws<br>• https://workspaces.af-south-1.api.aws<br>• https://workspaces.ca-central-1.api.aws<br>• https://workspaces.il-central-1.api.aws<br>• https://workspaces.us-gov-west-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://workspaces.us-gov-east-1.api.aws<br>• https://workspaces-fips.us-west-2.api.aws<br>• https://workspaces-fips.us-east-1.api.aws<br>• https://workspaces-fips.us-gov-west-1.api.aws<br>• https://workspaces-fips.us-gov-east-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| SAML シングルサインオン (SSO) 用の Workspaces エンドポイント | ドメイン:<br>• https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.eu-west-3.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.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-fips.us-gov-west-1.amazonaws.com/v1/report-heartbeat<br>• https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/report-heartbeat<br>• 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 (IPv4):<br>• https://skylight-cm.us-east-1.amazonaws.com<br>• https://skylight-cm-fips.us-east-1.amazonaws.com<br>• https://skylight-cm.us-west-2.amazonaws.com<br>• https://skylight-cm-fips.us-west-2.amazonaws.com<br>• https://skylight-cm.ap-south-1.amazonaws.com<br>• https://skylight-cm.ap-northeast-2.amazonaws.com<br>• https://skylight-cm.ap-southeast-1.amazonaws.com<br>• https://skylight-cm.ap-southeast-2.amazonaws.com<br>• https://skylight-cm.ap-northeast-1.amazonaws.com |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://skylight-cm.ca-central-1.amazonaws.com<br>• https://skylight-cm.eu-central-1.amazonaws.com<br>• https://skylight-cm.eu-west-1.amazonaws.com<br>• https://skylight-cm.eu-west-2.amazonaws.com<br>• https://skylight-cm.eu-west-3.amazonaws.com<br>• https://skylight-cm.sa-east-1.amazonaws.com<br>• https://skylight-cm.af-south-1.amazonaws.com<br>• https://skylight-cm.il-central-1.amazonaws.com<br>• https://skylight-cm.us-gov-west-1.amazonaws.com<br>• https://skylight-cm-fips.us-gov-west-1.amazonaws.com<br>• https://skylight-cm.us-gov-east-1.amazonaws.com<br>• https://skylight-cm-fips.us-gov-east-1.amazonaws.com<br><br>ドメイン (IPv6):<br><br>• https://skylight-cm.us-east-1.api.aws<br>• https://skylight-cm.us-west-2.api.aws<br>• https://skylight-cm.eu-west-3.api.aws<br>• https://skylight-cm.eu-west-2.api.aws<br>• https://skylight-cm.eu-west-1.api.aws |

| カテゴリ | ドメインまたは IP アドレス |
| --- | --- |
| | • https://skylight-cm.eu-central-1.api.aws<br>• https://skylight-cm.ap-northeast-1.api.aws<br>• https://skylight-cm.ap-northeast-2.api.aws<br>• https://skylight-cm.ap-southeast-1.api.aws<br>• https://skylight-cm.ap-southeast-2.api.aws<br>• https://skylight-cm.ap-south-1.api.aws<br>• https://skylight-cm.sa-east-1.api.aws<br>• https://skylight-cm.af-south-1.api.aws<br>• https://skylight-cm.ca-central-1.api.aws<br>• https://skylight-cm.il-central-1.api.aws<br>• https://skylight-cm.us-gov-west-1.api.aws<br>• https://skylight-cm.us-gov-east-1.api.aws<br>• https://skylight-cm-fips.us-west-2.api.aws<br>• https://skylight-cm-fips.us-east-1.api.aws<br>• https://skylight-cm-fips.us-gov-west-1.api.aws<br>• https://skylight-cm-fips.us-gov-east-1.api.aws |

| 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:<br>• turn:*.us-east-1.rdn.amazonaws.com<br>• turn:*.us-west-2.rdn.amazonaws.com<br>• 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。<br>• turn:*.ap-northeast-2.rdn.amazonaws.com<br>• turn:*.ap-southeast-1.rdn.amazonaws.com<br>• turn:*.ap-southeast-2.rdn.amazonaws.com<br>• turn:*.ap-northeast-1.rdn.amazonaws.com<br>• turn:*.ca-central-1.rdn.amazonaws.com<br>• turn:*.eu-central-1.rdn.amazonaws.com<br>• turn:*.eu-west-1.rdn.amazonaws.com<br>• turn:*.eu-west-2.rdn.amazonaws.com<br>• turn:*.sa-east-1.rdn.amazonaws.com<br>• アフリカ (ケープタウン) リージョンでは、現在 Web Access をご利用になれません。<br>• イスラエル (テルアビブ) リージョンでは、現在 Web Access をご利用になれません。 |

DCV 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 |
| --- | --- |
| DCV セッションゲートウェイ (WSG) | DCV ゲートウェイサーバー |
| DCV の Web Access TURN サーバー | DCV 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行います。これらのチェックで、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<br>3.212.50.30<br>3.225.55.35<br>3.226.24.234<br>34.200.29.95<br>52.200.219.150 |
| 米国西部 (オレゴン) | drp-pdx.amazonworkspaces.com | 34.217.248.177<br>52.34.160.80<br>54.68.150.54<br>54.185.4.125<br>54.188.171.18<br>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<br>13.234.250.73 |
| アジアパシフィック (ソウル) | drp-icn.amazonworkspaces.com | 13.124.44.166<br>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<br>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<br>18.138.99.116<br>18.140.252.123<br>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<br>13.237.232.125 |
| アジアパシフィック (東京) | drp-nrt.amazonworkspaces.com | 18.178.102.247<br>54.64.174.128 |
| カナダ (中部) | drp-yul.amazonworkspaces.com | 52.60.69.16<br>52.60.80.237<br>52.60.173.117<br>52.60.201.0 |
| 欧州 (フランクフルト) | drp-fra.amazonworkspaces.com | 52.59.191.224<br>52.59.191.225<br>52.59.191.226<br>52.59.191.227 |
| 欧州 (アイルランド) | drp-dub.amazonworkspaces.com | 18.200.177.86<br>52.48.86.38<br>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<br>35.177.255.44<br>52.56.46.102<br>52.56.111.36 |
| 欧州 (パリ) | drp-cdg.amazonworkspaces.com | 51.17.52.90<br>51.17.109.231<br>51.16.190.43 |
| 南米 (サンパウロ ) | drp-gru.amazonworkspaces.com | 18.231.0.105<br>52.67.55.29<br>54.233.156.245<br>54.233.216.234 |
| アフリカ (ケープタウン) | drp-cpt.amazonworkspaces.com/ | 13.244.128.155<br>13.245.205.255<br>13.245.216.116 |
| イスラエル (テルアビブ) | drp-tlv.amazonworkspaces.com/ | 51.17.52.90<br>51.17.109.231<br>51.16.190.43 |

| リージョン | ヘルスチェックホスト名 | IP アドレス |
| --- | --- | --- |
| AWS GovCloud (米国西部 ) | drp-pdt.amazonworkspaces.com | 52.61.60.65<br>52.61.65.14<br>52.61.88.170<br>52.61.137.87<br>52.61.155.110<br>52.222.20.88 |
| AWS GovCloud (米国東部 ) | drp-osu.amazonworkspaces.com | 18.253.251.70<br>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 を介して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、WorkSpaces は少量の Amazon EC2 パブリック IPv4 アドレスと IPv6 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。IPv6 がサポートされ、ゲートウェイに到達可能な場合、WorkSpaces クライアントは IPv6 接続を優先することに注意してください。IPv6 が使用できない場合、IPv4 にフォールバックします。

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| 米国東部 (バージニア北部) | us-east-1 | 3.217.228.0 - 3.217.231.255<br>3.235.112.0 - 3.235.119.255<br>52.23.61.0 - 52.23.62.255<br>2600:1f32:8000::/39 |
| 米国西部 (オレゴン ) | us-west-2 | 35.80.88.0 - 35.80.95.255<br>44.234.54.0 - 44.234.55.255 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| | | 54.244.46.0 - 54.244.47.255<br>2600:1f32:4000::/39 |
| アジアパシフィック (ムンバイ) | ap-south-1 | 13.126.243.0 - 13.126.243.255<br>2406:da32:a000::/40 |
| アジアパシフィック (ソウル) | ap-northeast-2 | 3.34.37.0 - 3.34.37.255<br>3.34.38.0 - 3.34.39.255<br>13.124.247.0 - 13.124.247.255<br>2406:da32:2000::/40 |
| アジアパシフィック (シンガポール) | ap-southeast-1 | 18.141.152.0 - 18.141.152.255<br>18.141.154.0 - 18.141.155.255<br>52.76.127.0 - 52.76.127.255<br>2406:da32:8000::/40 |
| アジアパシフィック (シドニー) | ap-southeast-2 | 3.25.43.0 - 3.25.43.255<br>3.25.44.0 - 3.25.45.255<br>54.153.254.0 - 54.153.254.255<br>2406:da32:c000::/40 |
| アジアパシフィック (東京) | ap-northeast-1 | 18.180.178.0 - 18.180.178.255<br>18.180.180.0 - 18.180.181.255<br>54.250.251.0 - 54.250.251.255<br>2406:da32:4000::/40 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| カナダ (中部) | ca-central-1 | 15.223.100.0 - 15.223.100.255<br>15.223.102.0 - 15.223.103.255<br>35.183.255.0 - 35.183.255.255<br>2600:1f32:1000::/40 |
| 欧州 (フランクフルト) | eu-central-1 | 18.156.52.0 - 18.156.52.255<br>18.156.54.0 - 18.156.55.255<br>52.59.127.0 - 52.59.127.255<br>2a05:d032:4000::/40 |
| 欧州 (アイルランド) | eu-west-1 | 3.249.28.0 - 3.249.29.255<br>52.19.124.0 - 52.19.125.255<br>2a05:d032:8000::/40 |
| 欧州 (ロンドン) | eu-west-2 | 18.132.21.0 - 18.132.21.255<br>18.132.22.0 - 18.132.23.255<br>35.176.32.0 - 35.176.32.255<br>2a05:d032:c000::/40 |
| 欧州 (パリ) | eu-west-3 | 51.44.204.0-51.44.207.255 |
| 南米 (サンパウロ ) | sa-east-1 | 18.230.103.0 - 18.230.103.255<br>18.230.104.0 - 18.230.105.255<br>54.233.204.0 - 54.233.204.255<br>2600:1f32:e000::/40 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| アフリカ (ケープタウン) | af-south-1 | 13.246.120.0 - 13.246.123.255<br>2406:da32:1000::/40 |
| イスラエル (テルアビブ) | il-central-1 | 51.17.28.0-51.17.31.255<br>2a05:d032:5000::/40 |
| AWS GovCloud (米国西部 ) | us-gov-west-1 | 52.61.193.0 - 52.61.193.255<br>2600:1f32:2000::/40 |
| AWS GovCloud (米国東部 ) | us-gov-east-1 | 18.254.140.0 - 18.254.143.255<br>2600:1f32:5000::/40 |

## DCV ゲートウェイサーバー

**Important**

2020 年 6 月から、WorkSpaces は DCV 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ストリーミングします。DCV WorkSpaces を使用する場合は、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。

**Note**

BYOL 以外の WorkSpaces Pools の場合、IP アドレス範囲は保証されません。代わりに、DCV ゲートウェイドメイン名を許可リストに登録する必要があります。詳細については、「DCV ゲートウェイドメイン名」を参照してください。

WorkSpaces は、DCV ゲートウェイサーバーに少量の Amazon EC2 パブリック IPv4 アドレスと IPv6 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。WorkSpaces は、専用の AWS Global Accelerator (AGA) エンドポイントに別の範囲のパブリック IPv4 アドレスを使用します。WorkSpaces で AGA

を有効にする場合は、IP 範囲を許可リストに登録するようにファイアウォールポリシーを設定してください。IPv6 がサポートされ、ゲートウェイに到達可能な場合、WorkSpaces クライアントは IPv6 接続を優先することに注意してください。IPv6 が使用できない場合、IPv4 にフォールバックします。

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| 米国東部 (バージニア北部) | us-east-1 | • 3.227.4.0/22<br>• 44.209.84.0/22<br>• 93.77.138.0/24 (AGA エンドポイント)<br>• 93.77.139.0/24 (AGA エンドポイント)<br>• 2600:1f28:34c::/48 |
| 米国東部 ( オハイオ ) | us-east-2 | • 3.146.84.0/22<br>• 93.77.130.0/24 (AGA エンドポイント)<br>• 93.77.131.0/24 (AGA エンドポイント)<br>• 2600:1f26:28::/48 |
| 米国西部 (オレゴン ) | us-west-2 | • 34.223.96.0/22<br>• 93.77.148.0/24 (AGA エンドポイント)<br>• 93.77.149.0/24 (AGA エンドポイント)<br>• 2600:1f24:34::/48 |
| アジアパシフィック (ムンバイ) | ap-south-1 | • 65.1.156.0/22<br>• 93.77.142.0/24 (AGA エンドポイント)<br>• 93.77.143.0/24 (AGA エンドポイント)<br>• 2406:da2a:14::/48 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| アジアパシフィック (ソウル) | ap-northeast-2 | • 3.35.160.0/22<br>• 93.77.156.0/24 (AGA エンドポイント )<br>• 93.77.157.0/24 (AGA エンドポイント )<br>• 2406:da22:4::/48 |
| アジアパシフィック (シンガポール) | ap-southeast-1 | • 13.212.132.0/22<br>• 93.77.158.0/24 (AGA エンドポイント )<br>• 93.77.159.0/24 (AGA エンドポイント )<br>• 2406:da28:28::/48 |
| アジアパシフィック (シドニー) | ap-southeast-2 | • 3.25.248.0/22<br>• 93.77.150.0/24 (AGA エンドポイント )<br>• 93.77.151.0/24 (AGA エンドポイント )<br>• 2406:da2c:24::/48 |
| アジアパシフィック (東京) | ap-northeast-1 | • 3.114.164.0/22<br>• 93.77.134.0/24 (AGA エンドポイント )<br>• 93.77.135.0/24 (AGA エンドポイント )<br>• 2406:da24:28::/48 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| カナダ (中部) | ca-central-1 | • 3.97.20.0/22<br>• 93.77.128.0/24 (AGA エンドポイント )<br>• 93.77.129.0/24 (AGA エンドポイント )<br>• 2600:1f21:8::/48 |
| 欧州 (フランクフルト) | eu-central-1 | • 18.192.216.0/22<br>• 93.77.154.0/24 (AGA エンドポイント )<br>• 93.77.155.0/24 (AGA エンドポイント )<br>• 2a05:d024:18::/48 |
| 欧州 (アイルランド) | eu-west-1 | • 3.248.176.0/22<br>• 93.77.132.0/24 (AGA エンドポイント )<br>• 93.77.133.0/24 (AGA エンドポイント )<br>• 2a05:d028:40::/48 |
| 欧州 (ロンドン) | eu-west-2 | • 18.134.68.0/22<br>• 93.77.140.0/24 (AGA エンドポイント )<br>• 93.77.141.0/24 (AGA エンドポイント )<br>• 2a05:d02c:8::/48 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| 欧州 (パリ) | eu-west-3 | • 51.44.72.0/22<br>• 93.77.144.0/24 (AGA エンドポイント )<br>• 93.77.145.0/24 (AGA エンドポイント )<br>• 2a05:d022:1c::/48 |
| 南米 (サンパウロ ) | sa-east-1 | • 15.228.64.0/22<br>• 93.77.146.0/24 (AGA エンドポイント )<br>• 93.77.147.0/24 (AGA エンドポイント )<br>• 2600:1f2e:14::/48 |
| アフリカ (ケープタウン) | af-south-1 | • 13.246.108.0/22<br>• 93.77.136.0/24 (AGA エンドポイント )<br>• 93.77.137.0/24 (AGA エンドポイント )<br>• 2406:da21:c::/48 |
| イスラエル (テルアビブ) | il-central-1 | • 51.17.72.0/22<br>• 93.77.152.0/24 (AGA エンドポイント )<br>• 93.77.153.0/24 (AGA エンドポイント )<br>• 2a05:d025:1000::/48 |
| AWS GovCloud (米国西部 ) | us-gov-west-1 | • 3.32.139.0/24<br>• 3.30.129.0/24<br>• 3.30.130.0/23<br>• 2600:1f22:28::/48 |

| リージョン | リージョンコード | パブリック IP アドレス範囲 |
| --- | --- | --- |
| AWS GovCloud (米国東部 ) | us-gov-east-1 | • 18.254.148.0/22<br>• 2600:1f25:14::/48 |

## DCV ゲートウェイドメイン名

次の表に、DCV WorkSpace ゲートウェイドメイン名を示します。WorkSpaces クライアントアプリケーションが WorkSpace DCV サービスにアクセスするためには、これらのドメインが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<br>• (FIPS) *.wsp-fips.prod.us-east-1.highlander.aws.a2z.com |
| 米国西部 (オレゴン ) | • *.prod.us-west-2.highlander.aws.a2z.com<br>• (FIPS) *.wsp-fips.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 |
| 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 |

| リージョン | 分野 |
| --- | --- |
| 欧州 (パリ) | *.prod.eu-west-3.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<br>• (FIPS) *.wsp-fips.prod.us-gov-west-1.highlander.aws.a2z.com |
| AWS GovCloud (米国東部 ) | • *.prod.us-gov-east-1.highlander.aws.a2z.com<br>• (FIPS) *.wsp-fips.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 およびインターネット内でのリソースへの接続を可能にし、WorkSpace とディレクトリとの結合に使用されます。
- 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。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なストリーミングと、WorkSpaces が WorkSpace を管理するために使用されます。

WorkSpaces は、WorkSpaces 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用の IP アドレスを選択します。ディレクトリが登録されるときに、WorkSpaces は VPC CIDR と VPC 内のルートテーブルをテストし、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**
>
> WorkSpace にアタッチされ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。そうすると、WorkSpace にアクセスできなくなったり、インターネットにアクセスできなくなったりすることがあります。たとえば、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、(Amazon が提供するプールからの) Elastic IP アドレスは、起動時に 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 WorkSpace に関連付けた後、その Elastic IP アドレスと WorkSpace 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 WorkSpace に関連付けるには、WorkSpace を再構築する必要があります。WorkSpace を再構築しない場合は、所有する別の Elastic IP アドレスを WorkSpace に関連付ける必要があります。

### 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**
>
> - ライセンス持ち込み (BYOL) Windows WorkSpaces を使用している場合は、次の表の IP アドレスの範囲は適用されません。代わりに、PCoIP BYOL WorkSpaces 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 アドレス範囲を使用します。DCV BYOL Windows WorkSpaces の場合、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 WorkSpaces 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。)
> - パブリックバンドルから作成された DCV WorkSpaces を使用している場合、IP アドレス範囲 10.0.0.0/8 は、次の表に示す PCoIP/DCV 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 |

| リージョン | IP アドレス範囲 |
| --- | --- |
| | 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<br><br>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<br><br>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<br><br>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<br><br>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<br><br>WSP: 10.0.0.0/8 |
| アジアパシフィック (東京) | PCoIP/WSP: 198.19.0.0/16<br><br>WSP: 10.0.0.0/8 |
| カナダ (中部) | PCoIP/WSP: 198.19.0.0/16<br><br>WSP: 10.0.0.0/8 |
| 欧州 (フランクフルト) | PCoIP/WSP: 198.19.0.0/16<br><br>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<br><br>WSP: 10.0.0.0/8 |

| リージョン | IP アドレス範囲 |
| --- | --- |
| 欧州 (ロンドン) | PCoIP/WSP: 198.19.0.0/16<br>WSP: 10.0.0.0/8 |
| 欧州 (パリ) | PCoIP/WSP: 198.19.0.0/16<br>WSP: 10.0.0.0/8 |
| 南米 (サンパウロ) | PCoIP/WSP: 198.19.0.0/16<br>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<br>WSP: 10.0.0.0/8 |
| イスラエル (テルアビブ) | PCoIP/WSP: 198.19.0.0/16<br>WSP: 10.0.0.0/8 |
| AWS GovCloud (米国西部 ) | PCoIP/WSP: 198.19.0.0/16<br>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<br>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 WorkSpaces 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。

- 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、WorkSpace の管理と設定に使用されます。
- 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 DCV 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 DCV 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。
- EC2 メタデータサービスにアクセスするための、ポート 80 での IP アドレス 169.254.169.254 への送信 TCP (「管理インターフェイスの IP 範囲」で定義)。WorkSpaces に割り当てられているすべての HTTP プロキシで、169.254.169.254 も除外されている必要があります。
- 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。ライセンス持ち込み (BYOL) Windows WorkSpaces を使用している場合は、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。
- ポート 1688 での IP アドレス 54.239.236.220 への送信 TCP を使用して、BYOL WorkSpaces の Office 用 Microsoft KMS のアクティベーションのためのアクセスを許可します。

  WorkSpaces パブリックバンドルの 1 つを通じて Office を使用している場合は、Office アクティベーション用の Microsoft KMS の IP アドレスは異なります。その IP アドレスを特定するには、WorkSpace の管理インターフェイスの IP アドレスを検索し、最後の 2 つのオクテットを `64.250` に置き換えます。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における、DCV WorkSpaces 用の IP アドレス 127.0.0.2 への送信 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 WorkSpaces に対してこれらのポートを設定します。これらのいずれかのポートをブロックするセキュリティソフトウェアまたはファイアウォールソフトウェアが WorkSpace にインストールされている場合、WorkSpace は適切に機能することもあれば、アクセスできないこともあります。

プライマリインターフェイスポート

ディレクトリの種類にかかわらず、すべての WorkSpaces 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。

- 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送信と WorkSpaces VPC からの受信に対して開いている必要があります。これらのポートは、インターネットアクセスを許可する場合、WorkSpaces のセキュリティグループに手動で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かれている必要があります。Simple AD ディレクトリの場合、 によって作成されたセキュリティグループでは AWS Directory Service 、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
  - TTCP 3268-3269 - グローバルカタログ

  これらのいずれかのポートをブロックするセキュリティソフトウェアまたはファイアウォールソフトウェアが WorkSpace にインストールされている場合、WorkSpace は適切に機能することもあれば、アクセスできないこともあります。

# 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.us-east-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.us-east-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• 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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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) |
| WS ブローカー | ドメイン:<br>• https://ws-broker-service.us-east-1.amazonaws.com<br>• https://ws-broker-service-fips.us-east-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>https://workspaces.us-east-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• https://skylight-cm.us-east-1.amazonaws.com<br>• 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:<br>• 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<br>• 3.212.50.30<br>• 3.225.55.35<br>• 3.226.24.234<br>• 34.200.29.95<br>• 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<br>• 3.235.112.0 - 3.235.119.255<br>• 52.23.61.0 - 52.23.62.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | • 3.227.4.0/22<br>• 44.209.84.0/22 |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.us-west-2.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.us-west-2.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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><br><br>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:<br><br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br><br>• 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 |
| 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:<br><br>• https://ws-broker-service.us-west-2.amazonaws.com<br>• https://ws-broker-service-fips.us-west-2.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.us-west-2.amazonaws.com<br>• https://workspaces-fips.us-west-2.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• https://skylight-cm.us-west-2.amazonaws.com<br>• 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:<br>• 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<br>• 52.34.160.80<br>• 54.68.150.54<br>• 54.185.4.125<br>• 54.188.171.18<br>• 54.244.158.140 |
| 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<br>• 44.234.54.0 - 44.234.55.255<br>• 54.244.46.0 - 54.244.47.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 34.223.96.0/22 |
| DCV ゲートウェイドメイン名 | *.prod.us-west-2.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 | • PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、198.19.0.0/16<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br>https://skylight-client-ds.ap-south-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br>https://ws-client-service.ap-south-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定: |

| カテゴリ | 詳細 |
| --- | --- |
| | • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br><br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br><br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br><br>• 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 |
| 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:<br><br>• https://ws-broker-service.ap-south-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ap-south-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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<br>• 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 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 65.1.156.0/22 |
| DCV 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<br>• 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/ |

| カテゴリ | 詳細 |
| --- | --- |
| 接続の確認 | https://connectivity.amazonworkspaces.com/ |
| デバイスメトリクス ( 1.0 以上および 2.0 以上の 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.ap-northeast-2.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.ap-northeast-2.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |

| 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:<br>• https://ws-broker-service.ap-northeast-2.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ap-northeast-2.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 13.124.203.105<br>• 52.78.44.253<br>• 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<br>• 3.34.38.0 - 3.34.39.255<br>• 13.124.247.0 - 13.124.247.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 3.35.160.0/22 |

| カテゴリ | 詳細 |
| --- | --- |
| DCV 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<br>• 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/ |
| 接続の確認 | https://connectivity.amazonworkspaces.com/ |
| クライアントメトリクス ( 3.0 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br>https://skylight-client-ds.ap-southeast-1.amazonaws.com |
| ダイナミックメッセージングサービス (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://ws-client-service.ap-southeast-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定: |

| カテゴリ | 詳細 |
| --- | --- |
| | • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br><br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br><br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br><br>• 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 |
| 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:<br><br>• https://ws-broker-service.ap-southeast-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ap-southeast-1.amazonaws.com |
| セッションブローカー（PCM） | ドメイン:<br>• 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:<br>• 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<br>• 18.138.99.116<br>• 18.140.252.123<br>• 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<br>• 18.141.154.0 - 18.141.155.255<br>• 52.76.127.0 - 52.76.127.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 13.212.132.0/22 |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.ap-southeast-2.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.ap-southeast-2.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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) |
| WS ブローカー | ドメイン:<br>• https://ws-broker-service.ap-southeast-2.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ap-southeast-2.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 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<br>• 3.25.44.0 - 3.25.45.255<br>• 54.153.254.0 - 54.153.254.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 3.25.248.0/22 |
| DCV 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<br>• 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/ |

| カテゴリ | 詳細 |
| --- | --- |
| クライアントメトリクス ( 3.0 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.ap-northeast-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.ap-northeast-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |

| カテゴリ | 詳細 |
| --- | --- |
| 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:<br>• https://ws-broker-service.ap-northeast-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ap-northeast-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 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<br>• 18.180.180.0 - 18.180.181.255<br>• 54.250.251.0 - 54.250.251.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 3.114.164.0/22 |

| カテゴリ | 詳細 |
| --- | --- |
| DCV 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<br>• 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/ |
| クライアントメトリクス ( 3.0 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br>https://skylight-client-ds.ca-central-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br>https://ws-client-service.ca-central-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/ |

| カテゴリ | 詳細 |
| --- | --- |
| | お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |
| 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:<br>• https://ws-broker-service.ca-central-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.ca-central-1.amazonaws.com |
| セッションブローカー（PCM） | ドメイン:<br>• 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:<br>• 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<br>• 52.60.80.237<br>• 52.60.173.117<br>• 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<br>• 15.223.102.0 - 15.223.103.255<br>• 35.183.255.0 - 35.183.255.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 3.97.20.0/22 |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.eu-central-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.eu-central-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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:<br>• https://ws-broker-service.eu-central-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.eu-central-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 52.59.191.225<br>• 52.59.191.226<br>• 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<br>• 18.156.54.0 - 18.156.55.255<br>• 52.59.127.0 - 52.59.127.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 18.192.216.0/22 |
| DCV 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<br>• 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/ |

| 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.eu-west-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.eu-west-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |

| カテゴリ | 詳細 |
| --- | --- |
| 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:<br>• https://ws-broker-service.eu-west-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.eu-west-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 52.48.86.38<br>• 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<br>• 52.19.124.0 - 52.19.125.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 3.248.176.0/22 |

| カテゴリ | 詳細 |
| --- | --- |
| DCV 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<br>• 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/ |
| クライアントメトリクス ( 3.0 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br>https://skylight-client-ds.eu-west-2.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br>https://ws-client-service.eu-west-2.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/ |

| カテゴリ | 詳細 |
| --- | --- |
| | お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |
| 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:<br>• https://ws-broker-service.eu-west-2.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.eu-west-2.amazonaws.com |
| セッションブローカー（PCM） | ドメイン:<br>• 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:<br>• 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<br>• 35.177.255.44<br>• 52.56.46.102<br>• 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<br>• 18.132.22.0 - 18.132.23.255<br>• 35.176.32.0 - 35.176.32.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 18.134.68.0/22 |
| DCV 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<br>• WSP: 10.0.0.0/8 |

欧州 (パリ)

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/Client |
| 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.eu-west-3.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.eu-west-3.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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://d2kmf63k5sit88.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br><br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br><br>• 欧州 (パリ) — https://d1a3pnge9on3sx.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:<br><br>• https://ws-broker-service.eu-west-3.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br><br>• https://workspaces.eu-west-3.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| セッションブローカー ( PCM ) | ドメイン:<br>• https://skylight-cm.eu-west-3.amazonaws.com |
| PCoIP のウェブアクセス TURN サーバー | サーバー:<br>• turn:*.eu-west-3.rdn.amazonaws.com |
| ヘルスチェックホスト名 | drp-cdg.amazonworkspaces.com |
| ヘルスチェック IP アドレス | • 51.17.52.90<br>• 51.17.109.231<br>• 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 | • 51.44.204.0-51.44.207.255<br>2a05:d032:2000::/40 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 51.17.72.0/22 |
| DCV ゲートウェイドメイン名 | *.prod.eu-west-3.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<br>• 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/ |

| カテゴリ | 詳細 |
| --- | --- |
| クライアントメトリクス ( 3.0 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.sa-east-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.sa-east-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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 |

| 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:<br>• https://ws-broker-service.sa-east-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.sa-east-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 52.67.55.29<br>• 54.233.156.245<br>• 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<br>• 18.230.104.0 - 18.230.105.255<br>• 54.233.204.0 - 54.233.204.255 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 15.228.64.0/22 |

| カテゴリ | 詳細 |
| --- | --- |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br>https://skylight-client-ds.af-south-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br>https://ws-client-service.af-south-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/ |

| カテゴリ | 詳細 |
| --- | --- |
| | お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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:<br>• https://ws-broker-service.af-south-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.af-south-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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<br>• 52.67.55.29<br>• 54.233.156.245<br>• 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 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 15.228.64.0/22 |
| DCV 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<br>• 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/ |

| 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>https://skylight-client-ds.il-central-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.il-central-1.amazonaws.com |

| カテゴリ | 詳細 |
| --- | --- |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br>• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID><br><br>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:<br>•<br><br>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:<br>• https://d3s98kk2h6f4oh.cloudfront.net/<br>• https://dyqsoz7pkju4e.cloudfront.net/<br><br>ログインページの JavaScript ファイル:<br>• 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:<br>• https://ws-broker-service.il-central-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.il-central-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• 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:<br>• 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<br>• 51.17.109.231<br>• 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 |
| DCV ゲートウェイサーバーの IP アドレス範囲 | 51.17.72.0/22 |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>hhttps://skylight-client-ds.us-gov-west-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.us-gov-west-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace にログインする前のクライアントからお客様のディレクトリへの認証:<br><br>• https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/ |

| カテゴリ | 詳細 |
| --- | --- |
| | お客様のディレクトリ設定:<br>• https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<directory ID><br><br>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:<br>• https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<directory ID><br><br>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:<br>• https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css<br><br>ログインページの JavaScript ファイル:<br>• 該当しません |
| 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) |

| カテゴリ | 詳細 |
| --- | --- |
| WS ブローカー | ドメイン:<br>• https://ws-broker-service.us-gov-west-1.amazonaws.com<br>• https://ws-broker-service-fips.us-gov-west-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.us-gov-west-1.amazonaws.com<br>• https://workspaces-fips.us-gov-west-1.amazonaws.com |
| セッションブローカー（PCM） | ドメイン:<br>• https://skylight-cm.us-gov-west-1.amazonaws.com<br>• 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<br>• 52.61.65.14<br>• 52.61.88.170<br>• 52.61.137.87<br>• 52.61.155.110<br>• 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 |
| --- | --- |
| DCV ゲートウェイサーバーの IP アドレス範囲 | • 3.32.139.0/24<br>• 3.30.129.0/24<br>• 3.30.130.0/23 |
| DCV 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<br>• 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 以上の WorkSpaces クライアントアプリケーション用 ) | ドメイン:<br><br>hhttps://skylight-client-ds.us-gov-east-1.amazonaws.com |
| ダイナミックメッセージングサービス (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:<br><br>https://ws-client-service.us-gov-east-1.amazonaws.com |
| ディレクトリ設定 | WorkSpace に口グインする前のクライアントからお客様のディレクトリへの認証: |

| カテゴリ | 詳細 |
| --- | --- |
| | • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID><br><br>MacOS クライアントからの接続:<br><br>• https://d32i4gd7pg4909.cloudfront.net/<br><br>お客様のディレクトリ設定:<br><br>• https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<directory ID><br><br>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:<br><br>• https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<directory ID><br><br>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:<br><br>• https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css<br><br>ログインページの JavaScript ファイル:<br><br>• 該当しません |
| 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) |
| WS ブローカー | ドメイン:<br>• https://ws-broker-service.us-gov-east-1.amazonaws.com<br>• https://ws-broker-service-fips.us-gov-east-1.amazonaws.com |
| WorkSpaces API エンドポイント | ドメイン:<br>• https://workspaces.us-gov-east-1.amazonaws.com<br>• https://workspaces-fips.us-gov-east-1.amazonaws.com |
| セッションブローカー ( PCM ) | ドメイン:<br>• https://skylight-cm.us-gov-east-1.amazonaws.com<br>• 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<br>• 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 |
| DCV 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 |
| --- | --- |
| DCV 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<br>• WSP: 10.0.0.0/8 |

## WorkSpaces Personal の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、「WorkSpaces Personal の IP アドレスとポートの要件」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。

  DCV で最善のパフォーマンスを確保するためには、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。

  ロケーションからさまざまな AWS リージョンへの RTT を確認するには、Amazon WorkSpaces Connection Health Check を使用します。
- DCV 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、WorkSpaces Personal の IP アドレスとポートの要件 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 Personal で PCoIP ゼロクライアントを設定する」を参照してください。

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<br><br>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。

## WorkSpaces Personal で信頼されたデバイス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デバイスから WorkSpaces にアクセスできます。会社が信頼されたデバイス ( 管理デバイスとも呼ばれます ) への

企業データアクセスを制限している場合、有効な証明書を使用して WorkSpaces へのアクセスを信頼されたデバイスに制限することができます。

> **Note**
>
> この機能は現在、Simple AD、AD Connector、 AWS Managed Microsoft AD ディレクトリ AWS Directory Service を含む WorkSpaces Personal ディレクトリが で管理されている場合にのみ使用できます。

この機能を有効にすると、WorkSpaces は証明書ベースの認証を使用して、デバイスが信頼でき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確認できない場合、デバイスへのログインまたは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、WorkSpaces はそれらをクライアントに提示し、クライアントはいずれかのルート証明書にチェーン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。
>
> - Linux、または iPad 用の WorkSpaces 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、他の不要なデバイスタイプのアクセスをブロックしてください。これを行う方法については、ステップ 3 の手順 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これらの証明書にアクセスする権限を与え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ポスチャ評価を実行して、デバイスが WorkSpaces 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ます。

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。このため、WorkSpaces クライアントアプリケーションは、ユーザーが WorkSpaces にログインする前に、デバイス上の証明書を検証する必要があります。

制限を設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com 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. [デバイスタイプごとに、WorkSpaces にアクセスできるデバイスを指定] で、[信頼されたデバイス] 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. [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. [インポート] を選択します。

7. 他のタイプのデバイスが WorkSpaces にアクセスできるかどうかを指定します。

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 iOS デバイス、Android デバイス、Web Access、Chromebook、および PCoIP ゼロクライアントデバイスから WorkSpaces 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。

## SAML 2.0 と WorkSpaces Personal の統合

> **Note**
>
> SAML 2.0 は、WorkSpaces Personal ディレクトリが Simple AD、AD Connector、 AWS Managed Microsoft AD ディレクトリ AWS Directory Service を含む を介して管理されている場合にのみ使用できます。この機能は、Amazon WorkSpaces によって管理されるディレクトリには適用されません。このようなディレクトリでは、通常、SAML 2.0 フェデレーションではなく IAM アイデンティティセンターがユーザー認証に使用されます。

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。

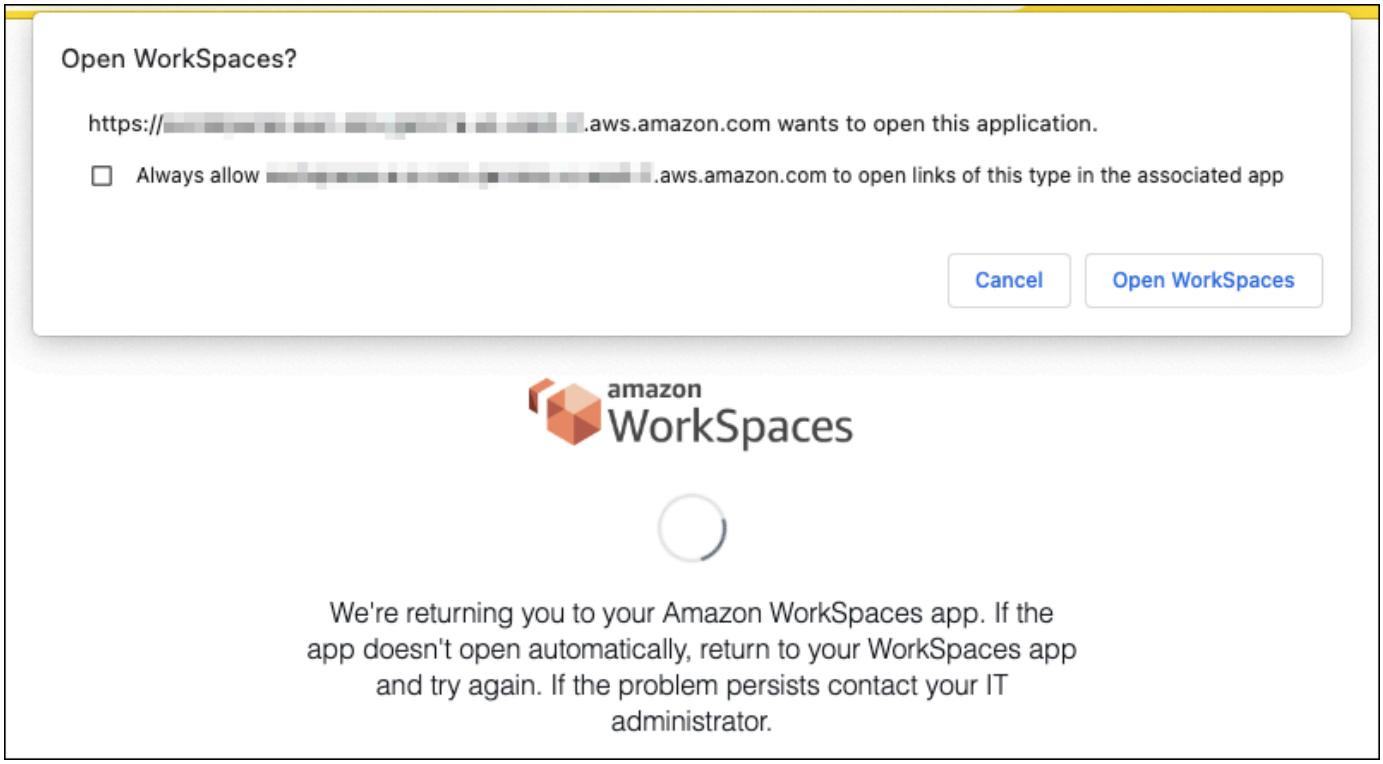

4. WorkSpaces クライアントアプリケーションが登録されました。ユーザーは、WorkSpaces Web Access からサインインを続行できます。

### 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。

## WorkSpaces Personal で SAML 2.0 を設定する

SAML 2.0 を使用して ID フェデレーションを設定することにより、ユーザーの SAML 2.0 ID プロバイダー (IdP) 認証情報と認証方法を使用して WorkSpaces クライアントアプリケーションの登録と 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、フェデレーションユーザーに対して WorkSpaces ディレクトリへのアクセス権が付与されます。リレーステートは、 AWSに正常にサインインした後にユーザーが転送される WorkSpaces ディレクトリエンドポイントです。

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 )
- WorkSpaces で SAML 2.0 認証を使用する場合、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の URL を使用して、未承諾の IdP を起点とする SSO をサポートする必要があります。IdP の例には、ADFS、Azure AD、Duo Single Sign-On、Okta、PingFederate、および PingOne などがあります。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 を使用して起動された WorkSpaces で機能しますが、Simple AD は SAML 2.0 IdP と統合されないため、これは推奨されません。
- 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 の [クライアントダウンロード] 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 以降向けの Linux クライアント
  - Web Access

  他のクライアントバージョンは、フォールバックが有効になっていない限り、SAML 2.0 認証が有効になっている WorkSpaces 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、Duo Single Sign-On、Okta、OneLogin、PingFederate、PingOne for Enterprise を使用して SAML 2.0 を WorkSpaces と統合する手順については、「Amazon WorkSpaces SAML Authentication Implementation Guide」(Amazon WorkSpaces SAML 認証実装ガイド) 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、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。

1. WorkSpaces ディレクトリで使用する Microsoft Active Directory からのユーザー ID を統合するように IdP を設定します。WorkSpace を持つユーザーの場合、IdP を使用して WorkSpaces にサインインするには、Active Directory ユーザーおよび SAML クレーム値の sAMAccountName 属性と email 属性が一致している必要があります。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 管理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 管理コンソールを使用して、WorkSpaces 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、「WorkSpaces のディレクトリを管理する」を参照してください。WorkSpaces の SAML 2.0 認証は、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ユーザー用の WorkSpace を作成します。WorkSpaces 管理コンソール、 AWS CLI、または WorkSpaces API を使用して WorkSpace を作成できます。詳細については、「WorkSpaces を使用して仮想デスクトップを起動する」を参照してください。

ステップ 1: IAM で SAML ID AWS プロバイダーを作成する

まず、IAM で SAML IdP AWS 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。 AWS GovCloud (米国西部) および GovCloud AWS GovCloud (米国東部) で SAML IdPsAWS 「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、値が persistent 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、「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) [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. 新しい IAM ロールの信頼ポリシーに sts:TagSession アクセス権限を追加します。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。信頼関係の編集ポリシーエディタが開いたら、[sts:TagSession*] アクセス許可を次のように設定します。

```
{
    "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、フェデレーションユーザーに 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。WorkSpaces の IP アクセスコントロールを管理するには、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は、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。以下のポリシーでは、"Action": "workspaces:Stream" は、WorkSpaces ディレクトリのデスクトップセッションに接続する権限を WorkSpaces ユーザーに提供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 WorkSpaces 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。DIRECTORY-ID を WorkSpaces 管理コンソールで確認できる WorkSpaces ディレクトリ ID に置換します。 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 によっては、https://signin.aws.amazon.com/static/saml-metadata.xml://www.2 でファイルを 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 saml-metadata.xml 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 IdP では、すでに更新が設定されています。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**
>
> このとき、IdP のユーザーに、IdP で設定した WorkSpaces アプリケーションへのアクセスを許可することもできます。ディレクトリの WorkSpaces アプリケーションにアクセスする権限を与えられているユーザーに対して、自動的に WorkSpace が作成されるわけではありません。同様に、WorkSpace が作成されるユーザーに対して、自動的に WorkSpaces アプリケーションへのアクセス権が与えられるわけではありません。SAML 2.0 認証を使用して WorkSpace に正常に接続するには、ユーザーが IdP によって承認され、WorkSpace が作成され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ます。通常は、Active Directory ユーザー用の 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 に設定されている 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 1 つの`AttributeValue`要素が含まれています。`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。この値は、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。corp\username、corp.example.com\username、username@corp.example.com などのユーザー名形式を必要とするユースケースで、WorkSpaces クライアントを使用してログインする場合は、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。
- **Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain (オプション) に設定された **Attribute** 要素 – この要素には、サインインしているユーザーの 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** 要素 (**Name** 属性が https://aws.amazon.com/SAML/Attributes/SessionDuration に設定) (オプション) – この要素には、再認証が必要となる前にユーザーがアクティブでいられるフェデレーティッドストリーミングセッションの最大時間を特定する 1 つの AttributeValue 要素が含まれています。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、セッション継続時間はデフォルト値の

3,600 秒 (60 分) に設定されます。WorkSpaces デスクトップセッションは、セッションの有効期限が切れると切断されます。

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 ディレクトリのリレーステートの 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 認証レスポンスのリレー状態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
```

WorkSpaces ディレクトリ登録コード、およびディレクトリが位置するリージョンと関連付けられたリレーステートのエンドポイントから、リレーステートの URL を構築します。登録コードは WorkSpaces 管理コンソールで確認できます。

必要に応じて、WorkSpaces でクロスリージョンリダイレクトを使用している場合は、登録コードをプライマリリージョンおよび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 WorkSpaces のクロスリージョンリダイレクト」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 を正しく構成でき、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。

次の表は、WorkSpaces SAML 2.0 認証を利用できるリージョンのリレーステートエンドポイントを示しています。

## 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<br>• (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<br>• (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<br>• (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com<br><br>**Note**<br>詳細については、「AWS GovCloud (US) ユーザーガイド」の「Amazon WorkSpaces」を参照してください。 |
| AWS GovCloud (米国東部 ) | • workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com<br>• (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com<br><br>**Note**<br>詳細については、「AWS GovCloud (US) ユーザーガイド」の「Amazon WorkSpaces」を参照してください。 |

ID プロバイダー (IdP) によって開始されるフローでは、SAML 2.0 フェデレーションに使用するクライアントを指定できます。これを行うには、リレー状態 URL の末尾の `&client=` の後に、`native` または `web` を指定します。このパラメータがリレー状態の URL で指定されている場合、対応するセッションは指定されたクライアントで自動的に開始されます。

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 ディレクトリで SAML 2.0 認証を有効にするには、WorkSpaces コンソールを使用できます。

SAML 2.0 との統合を有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. WorkSpaces のディレクトリ ID を選択します。
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を省略すると、デフォルトで「RelayState」という名前になります。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/` |

| ID プロバイダー | パラメータ | ユーザーアクセス URL |
| --- | --- | --- |
| | | <app_id>?tenantId=<tenant_id> |
| Duo Single Sign-On | RelayState | https://<sub-domain>.sso.duosecurity.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 for Enterprise | 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。テスト URL をコピーして現在のブラウザのプライベートウィンドウまたは別のブラウザに貼り付け、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 を起点とするフローが開いたら、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。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を使用しているユーザーに WorkSpaces へのアクセスを引き続き提供する場合や、ユーザーが最新のクライアントバージョンにアップグレードする時間が必要な場合に、この設定をオンにします。

> **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 を有効化および設定する」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 WorkSpaces ディレクトリで SAML 2.0 との統合が有効になりました。IdP およびクライアントアプリケーションを起点とするフローを使用して WorkSpaces クライアントアプリケーションを登録し、WorkSpaces にサインインできます。

## 証明書ベースの認証と WorkSpaces Personal

WorkSpaces で証明書ベースの認証を使用すると、Active Directory ドメインパスワードの入力を求める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 や下位 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 クライアントアプリケーション、および macOS クライアントアプリケーションを使用している Windows WorkSpaces DCV バンドルでサポートされます。Amazon WorkSpaces の [Client downloads] (クライアントダウンロード) を開いて、最新バージョンを確認します。

- 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 WorkSpaces での証明書ベースの認証の設定については、「How to configure certificate-based authentication for Amazon WorkSpaces」および「Design considerations in highly regulated environments for Certificate Based Authentication with AppStream 2.0 and WorkSpaces」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. SAML 2.0 統合を使用して、証明書ベースの認証を使用するように WorkSpaces のディレクトリを設定します。詳細については、「WorkSpaces と SAML 2.0 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 ユーザーに対して強力なマッピングを実行するために必要です。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。

   > **Note**
   >
   > Microsoft KB5014754 によると、 `ObjectSid` 属性は 2025 年 9 月 10 日以降、証明書ベースの認証に必須になります。

4. SAML 2.0 設定で使用している IAM ロールの信頼ポリシーに sts:TagSession アクセス許可がまだ存在しない場合は、これを追加します。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」と「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最も一般的な AWS Private CA 設定は次のとおりです。

   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 エントリ用に設定した Amazon S3 バケットへの認証されていないアクセスが必要です。S3 バケットがパブリックアクセスをブロックしている場合は、このバ

ケットにアクセスできる CloudFront 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、使用時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 の追加の設定タスクは、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することです。これにより、TCP ポート 135 と 49152-65535「」および「」で証明書の自動登録を有効にすることができます。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**
>
> - WorkSpaces デスクトップがドメインに参加している場合、Active Directory は、WorkSpaces デスクトップで、信頼されたルート認証局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. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. WorkSpaces のディレクトリ ID を選択します。
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 にあり AWS リージョン、リストに表示されるには euc-private-ca という名前の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 DCV バンドルを再起動し、変更を反映します。詳細については、「WorkSpaces の再起動」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を有効にして WorkSpaces にサインインすると、多要素認証 (MFA) がディレクトリで有効になっていても、ユーザーは 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「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

WorkSpaces 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証明書は、更新や取り消しを必要としません。これらは使用期間が短い証明書です。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、WorkSpaces AWS Private CA による への API コールを記録できます。詳細については、「CloudTrail の使用」を参照してください。CloudTrail イベント履歴では、WorkSpaces の `EcmAssumeRoleSession` ユーザー名で作成した `acm-pca.amazonaws.com` イベントソースの `GetCertificate` および `IssueCertificate` イベント名を確認できます。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。

PCA のクロスアカウント共有を有効にする

プライベート CA のクロスアカウント共有を使用する場合、一元的な 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ます。これにより、アカウントごとのプライベート CA は不要になります。CA は、AWS Resource Access Manager を使用して証明書を生成および発行し、アクセス許可を管理できます。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 の CBA で共有プライベート 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と WorkSpaces Personal」を参照してください。
2. 「How to use RAM to share your ACM Private CA cross-account」の手順に従って、WorkSpaces リソース AWS 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ステップ 3 の証明書を作成する手順は実行する必要はありません。プライベート 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 API を使用して、リソースアカウントの共有プライベート 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プライベート CA の RAM リソース共有で `AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority` のマネージド型アクセス許可テンプレートが使用され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ています。
3. 共有が成功すると、リソースアカウントのプライベート CA コンソールを使用して、共有プライベート 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 の 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 の ARN の選択をサポートしていません。CLI コマンドの例を以下に示します。

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

## Microsoft Entra ID に参加済みの WorkSpaces Personal にアクセスする

Microsoft Entra ID に参加済みで Intune に登録されている、Windows 10 または 11 の BYOL 個人用 WorkSpaces を作成できます。詳細については、WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成するを参照してください。

### 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) の Microsoft Entra ID 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。例えば、ユーザーが Entra ID 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.onmicrosoft.com」と入力して IdP にサインインします。Entra ID では、エンタープライズアプリケーションが IAM アイデンティティセンターと統合されるように設定されています。ユーザーは、IAM アイデンティティセンターを ID ソースとして使用して Entra ID テナントに接続するディレクトリに、ユーザー名の 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 (Microsoft Entra ID) にサインインします 。
2. IdP にサインインすると、ユーザーは AWS IdP ユーザーポータルから IAM Identity Center アプリケーションを選択します。
3. ユーザーはブラウザの AWS アクセスポータルにリダイレクトされます。ここで WorkSpaces アイコンを選択します。
4. ユーザーはブラウザで以下に示す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。クライアントアプリケーションが自動的に開かない場合は、[Amazon WorkSpaces アプリを開く] を選択します。


5. 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 にサインインすると、ユーザーは AWS IdP ユーザーポータルから IAM Identity Center アプリケーションをクリックします。
3. ユーザーはブラウザの AWS アクセスポータルにリダイレクトされます。ここで WorkSpaces アイコンを選択します。
4. 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。


5. 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の Windows ログイン画面にリダイレクトされます。

5. ユーザーは、Entra ID のユーザー名と認証情報を使用して Windows へのサインインを完了します。

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の Windows ログイン画面にリダイレクトされます。
5. ユーザーは、Entra ID のユーザー名と認証情報を使用して Windows へのサインインを完了します。

### 初めてログインする場合

Microsoft Entra ID に参加済みの Windows WorkSpaces に初めてログインする場合は、Out of Box Experience (OOBE) を実施する必要があります。OOBE の過程で、WorkSpaces が Entra ID に参加することになります。WorkSpaces 用に作成した Microsoft Intune デバイスグループに割り当てられた Autopilot プロファイルを設定することで、OOBE エクスペリエンスをカスタマイズできます。詳細については、「ステップ 3: Windows Autopilot のユーザードリブンモードを設定する」を参照してください。

## WorkSpaces Personal での認証にスマートカードを使用する

Windows および Linux WorkSpaces DCV バンドルでは、認証に Common Access Card (CAC) および Personal Identity Verification (PIV) スマートカードを使用できます。

Amazon WorkSpaces 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をサポートします。セッション前認証とは、ユーザーが WorkSpaces 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いいます。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 WorkSpace に対する管理アクセス許可を持っている場合、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身を認証できます。

内容



## 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 WorkSpace でスマートカードを使用するには、Amazon WorkSpaces Windows クライアントバージョン 3.1.1 以降または WorkSpaces MacOS クライアントのバージョン 3.1.5 以降を使用する必要があります。Windows および MacOSクライアントでスマートカードを使用する方法の詳細については、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 WorkSpaces 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、以下の属性を含める必要があります。

  - 証明書の subjectAltName (SAN) フィールドの AD ユーザーの userPrincipalName (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

- 現在、WorkSpaces の 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、スマートカード認証をサポートしています。
- 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 WorkSpaces は現在スマートカード認証をサポートしていません。
- 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、DCV 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
- 現在、Linux または Windows WorkSpaces でのセッション内認証およびセッション前認証では、一度に 1 つのスマートカードのみが許可されています。
- 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、DCV 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、同じユーザーの sAMAccountName と一致している必要があります。sAMAccountName 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 WorkSpaces のスマートカードを有効にする

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、スマートカードのセッション前認証が有効になっている Windows WorkSpaces のロックをユーザーが解除できるようにするには、ユーザーのセッションで Windows ロック画面の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、「DCV の画面ロック時におけるセッションの切断を有効または無効にする」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するために有効化されていません。必要に応じグループポリシー設定を使用して、Windows WorkSpaces のセッション前認証およびセッション内認証を有効にできます。詳細については、「DCV 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」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。GitHub では、これらの Firefox グループポリシーテンプレートを使用できます。

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 WorkSpaces のスマートカードを有効にする

> **Note**
>
> 現在、Linux WorkSpaces DCV バンドルには、次の制限があります。
>
> - 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。
> - DCV の Linux WorkSpaces に接続するには、WorkSpaces Windows 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 WorkSpaces でスマートカードを使用できるようにするには、ルート CA 証明書ファイルを PEM 形式で WorkSpace イメージに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 WorkSpaces にルート CA 証明書を追加するには

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 DCV 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。
- WorkSpace プロビジョニング中の pkinit 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 WorkSpaces にルート CA 証明書を追加し、Linux WorkSpaces でスマートカードを有効にする方法について説明します。

1. DCV プロトコルを有効にして新しい Linux WorkSpace を作成します。Amazon WorkSpaces コンソールで WorkSpace を起動する際に、[バンドルを選択] ページで、プロトコルとして [DCV] を選択し、いずれかの Amazon Linux 2 パブリックバンドルを選択します。
2. 新しい WorkSpace で、次のコマンドをルートとして実行します。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 WorkSpaces では、スマートカード上の証明書が、ユーザーのデフォルトのユーザープリンシパル名 (UPN) について発行されることを前提としています (*sAMAccountName*@*domain* など)。ここで、*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 WorkSpace で個別に実行する必要があります。

3. (オプション) デフォルトでは、Linux WorkSpaces ですべてのサービスについてスマートカード認証が使用できるように設定されています。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. WorkSpace に追加のカスタマイズを実行します。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、ユーザー自身が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 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。
5. WorkSpace からカスタム WorkSpace イメージとバンドルを作成します。
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の Firefox への追加の詳細については、GitHub の Mozilla のポリシーテンプレートをご参照ください。

1. WorkSpace イメージの作成に使用している WorkSpace で、`policies.json` という名前の新しいファイルを `/usr/lib64/firefox/distribution/` で作成します。
2. JSON ファイルで、次の SecurityDevices ポリシーを追加します。ここで、*`NAME_OF_DEVICE`* は `pkcs` モジュールの識別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いです。[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。

## WorkSpaces Personal でのインターネットアクセス

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。次のいずれかのオプションを使用して、Virtual Private Cloud (VPC) の WorkSpaces 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で WorkSpaces 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。
- パブリックサブネットで WorkSpaces を起動し、WorkSpaces にパブリック IP アドレスを自動的または手動で割り当てます。

これらのオプションの詳細については、WorkSpaces Personal 用に VPC を設定する 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、WorkSpaces のセキュリティグループがすべての宛先（0.0.0.0/0）へのポート 80（HTTP）および 443（HTTPS）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。

Amazon Linux Extras Library

Amazon Linux リポジトリを使用している場合は、Amazon Linux WorkSpaces がインターネットにアクセスできるか、このリポジトリおよびメイン 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/*"
        ]
    }
  ]
}
```

## WorkSpaces Personal 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、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で、もう 1 つはディレクトリ内の WorkSpaces 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)。WorkSpaces 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 _workspacesMembers が続きます (たとえば、d-123456fc11_workspacesMembers)。

> **Warning**
>
> _controllers および _workspacesMembers セキュリティグループを変更、削除、デタッチしないでください。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、新しい WorkSpaces を起動したときや、既存の WorkSpaces を再構築したときに、新しいセキュリティグループが追加されます。このトピックで後ほど説明するように、既存の WorkSpaces を再構築することなく、この新しいデフォルトのセキュリティグループを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、すべてのセキュリティグループのルールが効率的にまとめられて 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。

WorkSpaces ディレクトリにセキュリティグループを追加するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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 WorkSpaces を再構築せずにそこにセキュリティグループを追加するには、新しいセキュリティグループを WorkSpaces の Elastic Network Interface (ENI) に割り当てます。

既存の WorkSpace にセキュリティグループを追加するには

1. 更新が必要な各 WorkSpace の IP アドレスを確認します。
    a. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
    b. 各 WorkSpace を展開し、その WorkSpace IP アドレスを記録します。
2. 各 WorkSpace の ENI を見つけ、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. 他の WorkSpaces についても、必要に応じてこのプロセスを繰り返します。

# WorkSpaces Personal 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 アカウントごとにリージョンごとに最大 100 個の IP アクセスコントロールグループを作成できます。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/v2/home「https://www.com」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/v2/home「https://www.com」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/v2/home「https://www.com」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/v2/home「https://www.com」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 Personal で PCoIP ゼロクライアントを設定する

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 WorkSpaces Personal の多要素認証 (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。

## WorkSpaces Personal で Chromebook 用の Android を設定する

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 アプリ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はこれ以上更新されず、その使用はサポートされません。

Android アプリケーションのインストールに対応している Chromebook では、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。

2019 年より前に発売された一部の Chromebook では、ユーザーが Amazon WorkSpaces Android クライアントアプリケーションをインストールするには、事前に Android アプリ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、「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。

## WorkSpaces Personal で WorkSpaces Web Access を有効にして設定する

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**

- Windows および Ubuntu WorkSpaces の DCV による Web Access は、DCV WorkSpaces 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 WorkSpaces の DCV は、 AWS GovCloud (米国西部) でのみ使用できます。
- 最高のストリーミング品質とユーザーエクスペリエンスを実現するために、DCV WorkSpaces 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、次のような制限があります。
  - PCoIP によるウェブアクセスは AWS GovCloud (US) Regions、、アジアパシフィック (ムンバイ ) 、アフリカ (ケープタウン ) 、欧州 (フランクフルト ) 、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 Web Access は、Windows WorkSpaces でのみサポートされ、Amazon Linux または Ubuntu WorkSpaces ではサポートされません。
  - Web Access は、PCoIP プロトコルを使用する一部の Windows 10 WorkSpaces では使用できません。PCoIP WorkSpaces が Windows Server 2019 または 2022 を搭載している場合、Web Access は使用できません。
  - PCoIP による Web Access は、機能が制限されています。ビデオ出力、オーディオ出力、キーボード、マウスはサポートされていますが、ビデオ入力、オーディオ入力、クリップボードリダイレクト、ウェブカメラなど、多くの機能はサポートされていません。
- VPN で macOS を使用し、Firefox ウェブブラウザを使用している場合、このウェブブラウザでは WorkSpaces Web Access を使用した PCoIP WorkSpaces のストリーミングはサポートされません。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) WorkSpaces に接続できなくなります。

## ステップ 1: WorkSpaces で Web Access を有効にする

WorkSpaces への Web Access は、ディレクトリレベルで制御します。Web Access クライアント経由のアクセスをユーザーに許可する WorkSpaces を含むディレクトリごとに、以下のステップを実行します。

WorkSpaces への Web Access を有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home://www.com 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**
>
> ウェブアクセスを有効にしたら、WorkSpace を再起動して変更を適用します。

## 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、特定のポートに対するインバウンドおよびアウトバウンド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 では、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、専用のログオン画面設定を使用しています。

Web Access ユーザーが WorkSpaces にログオンできるようにするには、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構成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

と、ログオン時間が長くなったり、WorkSpaces にログオンする際にブラックスクリーンがユーザーに表示されたりする場合があります。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 (GPO) 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。WorkSpaces コンピュータオブジェクト用の組織単位と WorkSpaces ユーザーオブジェクト用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を有効にしてユーザーを切り替えるには

ほとんどの場合、ユーザーが WorkSpace にログオンする際、そのユーザーの名前にユーザー名フィールドがあらかじめ設定されています。ただし、管理者が WorkSpace への RDP 接続を確立してメンテナンスタスクを実行した場合、ユーザー名フィールドには管理者の名前が追加されます。

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で [Switch User] 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追加することができます。

1. グループポリシー管理ツール (gpmc.msc) を開き、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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。WorkSpace の設定によって、このリストは [Other User] タイルに表示されない場合があります。リストが表示されない場合や、あらかじめ設定されたユーザー名が正しくない場合

は、WorkSpaces ログオンエージェントを使用してフィールドに正しい名前を追加することはできません。

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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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 Web Access では、ユーザーがログオンする前に Ctrl+Alt+Del キーを押す必要があります。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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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、ユーザーの名前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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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

グループポリシーおよびセキュリティポリシー設定の変更は、WorkSpace の次回のグループポリシーの更新後、および WorkSpace セッションの再起動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。

- WorkSpace を再起動します (Amazon WorkSpaces コンソールで、WorkSpace を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

## WorkSpaces シンクライアントの設定

ほとんどの WorkSpaces バンドルは Amazon WorkSpaces シンクライアントアクセス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 WorkSpaces のリストについては、「どの Amazon WorkSpaces バンドルがシンクライアント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。

## ステップ 1: Amazon WorkSpaces シンクライアントへのアクセスコントロールを有効にする

ユーザーエージェントベースのアクセスコントロールを使用して、ディレクトリレベルで WorkSpaces へのシンクライアントアクセスを制御します。ユーザーにシンクライアントアクセスクライアントを介したアクセスを許可する WorkSpaces を含むディレクトリごとに、次の手順を実行します。

WorkSpaces へのシンクライアントアクセスを有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. 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 ID 列で、シンクライアントアクセス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. WorkSpaces シンクライアントを選択します。
6. [保存] を選択します。

## ステップ 2: シンクライアントアクセスのポートへのインバウンドアクセスとアウトバウンドアクセスを設定する

Amazon WorkSpaces シンクライアントアクセスには、特定のポートのインバウンドアクセスとアウトバウンド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、特定のログオン画面設定を使用して、ユーザーがシンクライアントアクセスクライアントから正常にログオンできるようにします。

シンクライアントアクセスユーザーが WorkSpaces にログオンできるようにするには、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と、ログオン時間が長くなったり、WorkSpaces にログオンする際にブラックスクリーンがユーザーに表示されたりする場合があります。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 (GPO) 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。WorkSpaces コンピュータオブジェクト用の組織単位と WorkSpaces ユーザーオブジェクト用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を有効にしてユーザーを切り替えるには

ほとんどの場合、ユーザーが WorkSpace にログオンする際、そのユーザーの名前にユーザー名フィールドがあらかじめ設定されています。ただし、管理者が WorkSpace への RDP 接続を確立してメンテナンスタスクを実行した場合、ユーザー名フィールドには管理者の名前が追加されます。

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で [Switch User] 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追加することができます。

1. グループポリシー管理ツール (gpmc.msc) を開き、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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。WorkSpace の設定によって、このリストは [Other User] タイルに表示されない場合があります。リストが表示されない場合や、あらかじめ設定されたユーザー名が正しくない場合は、WorkSpaces ログオンエージェントを使用してフィールドに正しい名前を追加することはできません。

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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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 シンクライアントアクセスでは、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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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、ユーザーの名前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、WorkSpaces 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 (ドメインに WorkSpaces グループポリシー管理用テンプレートがインストールされている場合は、WorkSpaces マシンアカウント用の 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

グループポリシーおよびセキュリティポリシー設定の変更は、WorkSpace の次回のグループポリシーの更新後、および WorkSpace セッションの再起動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。

- WorkSpace を再起動します (Amazon WorkSpaces コンソールで、WorkSpace を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

## WorkSpaces Personal で FedRAMP 認証または DoD SRG コンプライアンスを設定する

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 認可を持っているか、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 認可レベル (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 認可と DoD SRG コンプライアンスのレベルについては、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。

> **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、「WorkSpaces Personal の暗号化された WorkSpaces」を参照してください。

要件

- WorkSpaces は、FedRAMP 認可または DoD SRG 準拠の米国 AWS リージョンで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。
  > ディレクトリの検証方法の詳細については、以下のステップ 3 を参照してください。

- 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: PCoIP WorkSpaces の場合は 2.4.3 以降、DCV WorkSpaces の場合は 5.21.0 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/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [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。

## WorkSpaces Personal で Linux WorkSpaces の SSH 接続を有効にする

コマンドラインを使用して Linux WorkSpaces に接続する場合は、SSH 接続を使用します。SSH 接続は、ディレクトリのすべての WorkSpaces、またはディレクトリの各 WorkSpaces に対して有効にすることができます。

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したら、ユーザーは、PuTTY などのターミナルを使用して、デバイスから Linux WorkSpaces に接続することができます。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。

ビデオチュートリアルについては、 AWS ナレッジセンターの「SSH を使用して Linux Amazon WorkSpaces 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。このチュートリアルは Amazon Linux 2 WorkSpaces 専用です。

内容

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

## Linux WorkSpaces に SSH 接続するための前提条件

- WorkSpace へのインバウンド SSH トラフィックを有効にする — 1 つ以上の Linux WorkSpaces 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 IP アドレスまたはプライベート IP アドレスがあることを確認してください。たとえば、Virtual Private Cloud (VPC) の外部にあるデバイスのパブリック IP アドレス、または WorkSpace 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。

  ローカルデバイスから WorkSpace に接続する場合は、インターネットブラウザで「私の IP アドレスは何ですか?」と検索するか、Check IP サービスを使用できます。
- WorkSpace に接続する — デバイスから Linux WorkSpace への SSH 接続を開始するには、次の情報が必要です。
  - 接続先の Active Directory ドメインの NetBIOS 名。
  - WorkSpace のユーザー名。
  - 接続する WorkSpace の IP アドレス (パブリックまたはプライベート)。

    プライベート: VPC が企業のネットワークに接続されており、そのネットワークへのアクセス権がある場合は、WorkSpace のプライベート IP アドレスを指定することができます。

パブリック: WorkSpace にパブリック IP アドレスが割り当てられている場合は、次の手順に示されているように、WorkSpaces コンソールを使用して、パブリック IP アドレスを見つけることができます。

接続する Linux WorkSpace 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/v2/home「https://www.com」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. WorkSpaces のリストで、SSH 接続を有効にする WorkSpace を選択します。
4. [実行モード] 列で、WorkSpace ステータスが [Available] になっていることを確認します。
5. WorkSpace 名の左側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。WorkSpace のプライベート IP アドレスです。

     WorkSpace が関連付けられている Elastic Network Interface の取得に必要なプライベート IP アドレス。ネットワークインターフェイスは、WorkSpace に関連付けられている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 の [ユーザー名]。WorkSpace に接続するために指定するユーザー名。
6. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
7. ナビゲーションペインで、[Network Interfaces] を選択してください。
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. WorkSpace にパブリック IP アドレスが割り当てられている場合は、[IPv4 Public 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. AWS Directory Service コンソールを https://console.aws.amazon.com/directoryservicev2/:// https://https://https://https://https
2. ディレクトリのリストで、WorkSpace 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。
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。

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

ディレクトリ内のすべての Linux WorkSpaces への SSH 接続を有効にするには、以下の操作を行います。

ディレクトリ内のすべての Linux WorkSpaces 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 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
2. ナビゲーションペインで、[Security Groups] を選択してください。
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 接続を有効にする WorkSpaces 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 WorkSpaces 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。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. [作成] を選択します。
8. このセキュリティグループを WorkSpaces にアタッチします。このセキュリティグループを WorkSpaces に追加する詳しい方法については、「WorkSpaces Personal のセキュリティグループ」を参照してください。WorkSpaces に追加のセキュリティグループを自動的にアタッチする場合は、こちらのブログ記事を参照してください。

## WorkSpaces でのパスワードベースの認証

新しく作成された Linux WorkSpaces 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、WorkSpace にログインします。
2. ターミナルウィンドウを開きます。
3. ターミナルウィンドウで次のコマンドを実行し、cloud-init で SSH パスワード認証を有効にします。

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 true" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

このスクリプトは以下の処理を実行します。

- cloud-init ディレクトリ `/etc/cloud/cloud.cfg.d/` に設定ファイルを作成します。
- 設定ファイルを変更して、SSH パスワード認証を有効にするよう cloud-init に指定します。
- `set-passwords` cloud-init モジュールをリセットして、再度実行できるようにします。
- `set-passwords` cloud-init モジュールを単独で実行します。これにより、SSH パスワード認証を有効にするファイルが SSH 設定ディレクトリ `/etc/ssh/sshd_config.d/` に書き込まれ、SSHD が再起動されて、設定がすぐに有効になります。

これで、SSH パスワード認証が WorkSpace で有効になり、カスタムイメージによって保持されます。cloud-init を設定せずに SSH 設定ファイルでのみ SSH パスワード認証を有効にすると、一部の Linux WorkSpaces ではイメージングによって設定が保持されません。詳細については、cloud-init ドキュメントの「Set Passwords」を参照してください。

既存の Linux WorkSpaces 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、WorkSpace にログインします。
2. ターミナルウィンドウを開きます。
3. ターミナルウィンドウで次のコマンドを実行し、cloud-init で SSH パスワード認証を無効にします。

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 false" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single –name set-passwords'
```

このスクリプトは以下の処理を実行します。

- cloud-init ディレクトリ `/etc/cloud/cloud.cfg.d/` に設定ファイルを作成します。
- 設定ファイルを変更して、SSH パスワード認証を無効にするよう cloud-init に指定します。
- `set-passwords` cloud-init モジュールをリセットして、再度実行できるようにします。

- `set-passwords` cloud-init モジュールを単独で実行します。これにより、SSH パスワード認証を有効にするファイルが SSH 設定ディレクトリ `/etc/ssh/sshd_config.d/` に書き込まれ、SSHD が再起動されて、設定がすぐに有効になります。

これで、SSH が WorkSpace で直ちに無効になり、カスタムイメージによって保持されます。

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

特定の Linux WorkSpace への SSH 接続を有効にするには、以下の操作を行います。

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

1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
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. 検索バーに、SSH 接続を有効にする WorkSpace 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 を使用して Linux WorkSpace に接続する

セキュリティグループを作成または更新し、必要なルールを追加したら、ユーザーは、Linux または PuTTY を使用して、デバイスから WorkSpaces に接続することができます。

> **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。
> - WorkSpace への接続に使用するユーザー名。
> - 接続する WorkSpace の IP アドレス (パブリックまたはプライベート)。
>
> この情報の取得方法に関する手順については、このトピック前半の「Linux WorkSpaces に SSH 接続するための前提条件」を参照してください。

Linux を使用して Linux WorkSpace 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、適切な値を入力します。

   ```
   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

   ```
   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のと同じパスワード (Active Directory のパスワード) を入力します。

PuTTY を使用して Linux WorkSpace 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。これらの値を、接続先の Active Directory ドメインの NetBIOS 名、WorkSpace への接続に使用するユーザー名、および接続する WorkSpace 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のと同じパスワード (Active Directory のパスワード) を入力します。

## WorkSpaces Personal に必須の設定とサービスコンポーネント

WorkSpace 管理者は、必須の設定とサービスコンポーネントについて以下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”
- the section called “Rocky Linux のコンポーネント ”
- the section called “Red Hat Enterprise Linux のコンポーネント ”

### 必須のルーティングテーブルの設定

WorkSpace 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は変更しないことをお勧めします。WorkSpaces サービスでは、このテーブル内の事前設定済みルートが、システム状態のモニタリングとシステムコンポーネントの更新に必要です。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 WorkSpaces では、サービスコンポーネントは以下の場所にインストールされています。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。そのような操作をした場合、WorkSpace は正しく機能しなくなります。

WorkSpace 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、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と干渉しないようにしてください。

- `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`

WorkSpaces Core 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、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と干渉しないようにしてください。

- C:\Program Files\Amazon
- C:\ProgramData\Amazon

### 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 WorkSpaces の場合、このことは Teradici ファイルの場所が `C:\Program Files (x86)\Teradici` から `C:\Program Files\Teradici` に変更されることを意味します。PCoIP エージェントは定期的なメンテナンス期間中に更新されたため、移行中、一部の WorkSpaces が他の WorkSpaces よりも長く 32 ビットエージェントを使用していた可能性があります。

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。WorkSpaces がすべて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。置き換えると、WorkSpaces の一部が機能しない可能性があります。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 Arbiter サービスの変更 — WorkSpaces が 64 ビットエージェントを使用するように更新されると、PCoIP Arbiter サービス (`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe`) 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 WorkSpaces は、Windows レジストリを通じて 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。

## Linux 向けの必須のサービスコンポーネント

Amazon Linux WorkSpaces では、サービスコンポーネントは以下の場所にインストールされています。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。そのような操作をした場合、WorkSpace は正しく機能しなくなります。

> **Note**
>
> `/etc/pcoip-agent/pcoip-agent.conf` 以外のファイルを変更すると、WorkSpaces の動作が停止し、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、WorkSpaces Personal で Amazon Linux 2 WorkSpaces を管理する 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 WorkSpaces では、サービスコンポーネントは以下の場所にインストールされています。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。そのような操作をした場合、WorkSpace は正しく機能しなくなります。

- /etc/X11/default-display-manager
- /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/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

## Rocky Linux に必要なサービスコンポーネント

Red Hat Enterprise Linux WorkSpaces では、サービスコンポーネントは以下の場所にインストールされています。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。そのような操作をした場合、WorkSpace は正しく機能しなくなります。

- /etc/dcv
- /etc/os-release
- /etc/pam.d/dcv-graphical-sso
- /etc/pam.d/dcv
- /etc/systemd/system/euc-analytic-agent.service
- /etc/wsp
- /usr/bin/euc-analytics-agent
- /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.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/share/X11
- /var/lib/skylight
- /var/log/eucanalytics

- /var/log/skylight

### Red Hat Enterprise Linux 向けの必須のサービスコンポーネント

Red Hat Enterprise Linux WorkSpaces では、サービスコンポーネントは以下の場所にインストールされています。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。そのような操作をした場合、WorkSpace は正しく機能しなくなります。

- /etc/dcv
- /etc/os-release
- /etc/pam.d/dcv-graphical-sso
- /etc/pam.d/dcv
- /etc/systemd/system/euc-analytic-agent.service
- /etc/wsp
- /usr/bin/euc-analytics-agent
- /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.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/share/X11
- /var/log/eucanalytics
- /var/log/skylight

## WorkSpaces Personal 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 — でホストされている Microsoft Active Directory を作成します AWS。
- Simple AD — Samba 4 を搭載し、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の間に信頼関係を作成します。
- Microsoft Entra ID — Microsoft Entra ID を (IAM アイデンティティセンター経由で) ID ソースとして使用するディレクトリを作成します。ディレクトリ内の個人用 WorkSpaces は、Microsoft Windows Autopilot のユーザードリブンモードによって、Microsoft Entra ネイティブ認証を用いて追加され、Microsoft Intune に登録されます。Microsoft Entra ID を使用するディレクトリは、Windows 10 および 11 の Bring Your Own License (BYOL) の WorkSpaces のみをサポートしています。
- カスタム — ID プロバイダーを (IAM アイデンティティセンター経由で) ID ソースとして使用するディレクトリを作成します。ディレクトリ内の WorkSpaces は、JumpCloud などの任意のデバイス管理ソリューションを使用して管理されます。カスタム ID プロバイダーを使用するディレクトリは、Windows 10 および 11 の Bring Your Own License (BYOL) の WorkSpaces のみをサポートしています。

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 Personal のディレクトリを作成する」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 Personal のユーザーを管理する および WorkSpaces Personal で 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、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 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内の Amazon WorkSpaces での使用は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 Personal でディレクトリを削除する 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。

内容

# WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する

WorkSpaces が既存の AWS Directory Service ディレクトリを使用できるようにするには、WorkSpaces に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、ディレクトリが WorkSpaces がある VPC にアクセスできる限り、ディレクトリは専用のプライベートサブネットにあることができます。

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 Personal でディレクトリを削除する 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。

既存の AWS Directory Service ディレクトリを登録するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [Create directory] (ディレクトリの作成) を選択します。
4. [ディレクトリの作成] ページの [WorkSpaces タイプ] で、[個人] を選択します。[WorkSpace デバイス管理] で [AWS Directory Service] を選択します。

5. [ AWS Directory Serviceのディレクトリ] テーブルで登録するディレクトリを選択します。
6. 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、「WorkSpaces Personal のアベイラビリティーゾーン」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。

7. [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。
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。

AWS Directory Service ディレクトリを登録したら、個人用 WorkSpace を作成できます。詳細については、「WorkSpaces Personal で WorkSpace を作成する」を参照してください。

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/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [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. 確認を求められたら、[確認] を選択します。登録解除が完了すると、ディレクトリは登録が解除され、リストから削除されます。

# WorkSpaces Personal の組織単位を選択する

> **Note**
>
> この機能は、AD Connector、 AWS マネージド Microsoft AD、Simple AD など、 AWS Directory Service で管理されるディレクトリでのみ使用できます。

WorkSpaces コンピュータアカウントは、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、作成または再構築されたすべての WorkSpaces 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/v2/home「https://www.com」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 を検索するには、[ターゲットドメインと組織単位] で、OU 名の全部または一部の入力を開始し、使用する OU を選択します。
6. (オプション) OU の識別名を選択して、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 WorkSpaces を再ビルドして OU を更新します。詳細については、「WorkSpaces Personal の WorkSpace を再構築する」を参照してください。

# WorkSpaces Personal の自動パブリック 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、起動する各 WorkSpace に、Amazon が提供した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の WorkSpace 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している WorkSpaces は、それらを再構築するまでパブリックアドレスを受け取りません。

WorkSpaces がプライベートサブネットにあり、仮想プライベートクラウド (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、「WorkSpaces Personal 用に VPC を設定する」を参照してください。

> **Warning**
>
> 所有している Elastic IP アドレスを WorkSpaces に関連付けた後、その Elastic IP アドレスと WorkSpaces との関連付けを解除すると、WorkSpaces はパブリック IP アドレスを失い、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 WorkSpaces に関連付けるには、WorkSpaces を再構築する必要があります。WorkSpaces を再構築しない場合は、所有する別の Elastic IP アドレスを WorkSpaces に関連付ける必要があります。

Elastic IP アドレスを設定するには

1. https://console.aws.amazon.com/workspaces/v2/home://www.com 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. WorkSpaces のディレクトリを選択します。
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。

## WorkSpaces Personal のデバイスのアクセスコントロール

デバイスプラットフォームに基づいて、WorkSpaces にアクセスできるデバイスのタイプを指定できます。証明書を使用して、WorkSpaces 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) に制限できます。

WorkSpaces へのデバイスアクセスを制御するには

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

2. 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. [信頼されたデバイス] で、[すべて許可]、[信頼されたデバイス]、[すべて拒否] のいずれかを選択して、WorkSpaces にアクセスできるデバイスの種類を指定します。詳細については、「WorkSpaces Personal で信頼されたデバイス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。

## WorkSpaces Personal でローカル管理者のアクセス許可を管理する

> **Note**
>
> この機能は、AD Connector、 AWS マネージド Microsoft AD、Simple AD など、 AWS Directory Service で管理されるディレクトリでのみ使用できます。

ユーザーが WorkSpaces でローカル管理者であるかどうかを指定して、アプリケーションをインストールして WorkSpaces で設定を変更できるようにすることができます。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、作成したすべての新しいワークスペースと再ビルドしたワークスペース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/v2/home「https://www.com」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、[ローカル管理者の設定を有効にする] を選択します。
6. [保存] を選択します。

# WorkSpaces Personal の 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に使用する AD Connector アカウントを更新し、WorkSpaces マシンアカウントを AD Connector ディレクトリに参加させることができます。

AD Connector アカウントを更新するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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、[詳細を表示] 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。

# WorkSpaces Personal の多要素認証 (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。での多要素認証の使用の詳細については AWS Directory Service、「AD Connector および AD Connector の多要素認証を有効にする」の前提条件を参照してください。

> **Note**
>
> - RADIUS サーバーは、 によってホスト AWS 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/v2/home「https://www.com」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。多要素認証が設定されている間、ユーザーは WorkSpaces にログインできません。

## WorkSpaces Personal のディレクトリを作成する

WorkSpaces Personal では、 で管理されるディレクトリを使用して AWS Directory Service 、WorkSpaces とユーザーの情報を保存および管理できます。WorkSpaces Personal のディレクトリを作成するには、次のオプションを使用します。

- Simple AD ディレクトリを作成します。
- Microsoft Active Directory 用 AWS Directory Service を作成します。これは AWS Managed Microsoft AD とも呼ばれます。
- 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。
- 専用の Microsoft Entra ID WorkSpaces ディレクトリを作成します。
- 専用のカスタム WorkSpaces ディレクトリを作成します。

> **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、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の Amazon WorkSpaces での使用は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。

## ディレクトリを作成する前に

- 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。サポートされているリージョンの詳細については、AWS 「リージョン別の WorkSpaces 料金表」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、「WorkSpaces Personal 用に VPC を設定する」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、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

空のディレクトリを削除する方法については、「WorkSpaces Personal でディレクトリを削除する」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。

内容

- WorkSpaces Personal ディレクトリのコンピュータ名を特定する

- WorkSpaces Personal 用の AWS Managed Microsoft AD ディレクトリを作成する
- WorkSpaces Personal で Simple AD ディレクトリを作成する
- WorkSpaces Personal の AD Connector を作成する
- WorkSpaces Personal の AWS Managed Microsoft AD ディレクトリとオンプレミスドメインの間に信頼関係を作成する
- WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する
- WorkSpaces Personal で専用のカスタムディレクトリを作成する

## WorkSpaces Personal ディレクトリのコンピュータ名を特定する

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*
- Red Hat Enterprise Linux: R-*xxxxxxxxxxxxx*
- Rocky Linux: R-*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、WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成するを参照してください。

> **Important**
>
> WorkSpace を作成したら、コンピュータ名を安全に変更できます。例えば、WorkSpace またはリモートでコマンド `Rename-Computer` を使用して PowerShell スクリプトを実行できます。更新されたコンピュータ名の値は、Amazon WorkSpaces コンソールの WorkSpace に表示されます。

## WorkSpaces Personal 用の AWS Managed Microsoft AD ディレクトリを作成する

このチュートリアルでは、 AWS Managed Microsoft AD ディレクトリを作成します。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 Personal のディレクトリを作成する」を参照してください。

まず、 AWS Managed Microsoft AD ディレクトリを作成します。 は、VPC のプライベートサブネットごとに 1 つずつ、2 つのディレクトリサーバー AWS Directory Service 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。
> - AWS Managed Microsoft AD ディレクトリがマルチリージョンレプリケーション用に設定されている場合、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 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内の Amazon WorkSpaces での使用は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/v2/home「https://www.com」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. [Create directory] (ディレクトリの作成) を選択します。
4. [ディレクトリの作成] ページの [WorkSpaces タイプ] で、[個人] を選択します。次に、[WorkSpace デバイス管理] で [AWS Directory Service] を選択します。
5. ディレクトリの作成を選択すると、 AWS ディレクトリサービスでディレクトリのセットアップページが開きます。
6. [AWS Managed Microsoft AD] を選択し、[次へ] を選択します。
7. 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、WorkSpaces Personal の DNS サーバーを更新する 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。パスワード要件の詳細については、「 管理ガイド」の AWS 「マネージド Microsoft AD ディレクトリの作成」を参照してください。 AWS Directory Service

   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 ] (次のステップ) をクリックします。

8. [Create directory] (ディレクトリの作成) を選択します。
9. WorkSpaces コンソールのディレクトリの作成ページに戻ります。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 (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。

AWS Managed Microsoft AD ディレクトリを作成したら、Amazon WorkSpaces に登録できます。詳細については、WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する を参照してください。

## WorkSpaces Personal で Simple AD ディレクトリを作成する

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 Personal のディレクトリを作成する」を参照してください。

> **Note**
>
> - 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 でサポートされてい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。
> - 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。

Simple AD ディレクトリを作成すると、 は 2 つのディレクトリサーバー AWS Directory Service を作成します。1 つは VPC のプライベートサブネットごとに作成されます。最初はディレクトリにユーザーはいません。WorkSpace を作成した後で、ユーザーを追加します。詳細については、WorkSpaces Personal で WorkSpace を作成するを参照してください。

Simple AD ディレクトリを作成するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com 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. [Create directory] (ディレクトリの作成) を選択します。
4. [ディレクトリの作成] ページの [WorkSpaces タイプ] で、[個人] を選択します。次に、[WorkSpace デバイス管理] で [AWS Directory Service] を選択します。
5. ディレクトリの作成を選択すると、 AWS ディレクトリサービスでディレクトリのセットアップページが開きます。

6. [Simple AD] を選択して、[次へ] を選択します。
7. 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、WorkSpaces Personal の DNS サーバーを更新する 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。

8. [Create directory] (ディレクトリの作成) を選択します。
9. WorkSpaces コンソールのディレクトリの作成ページに戻ります。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 (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。

Simple AD ディレクトリを作成したら、Amazon WorkSpaces に登録できます。詳細については、WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する を参照してください。

## WorkSpaces Personal の AD Connector を作成する

このチュートリアルでは、AD Connector を作成します。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 Personal のディレクトリを作成する」を参照してください。

AD Connector を作成する

> **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 Personal でディレクトリを削除する 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/v2/home://www.com 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. [Create directory] (ディレクトリの作成) を選択します。

4. [ディレクトリの作成] ページの [WorkSpaces タイプ] で、[個人] を選択します。次に、[WorkSpace デバイス管理] で [AWS Directory Service] を選択します。
5. ディレクトリの作成を選択すると、 AWS ディレクトリサービスでディレクトリのセットアップページが開きます。
6. [AWS Managed Microsoft AD] を選択し、[次へ] を選択します。
7. [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。
8. [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。
9. [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。
10. [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。
11. [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。
12. [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、WorkSpaces Personal の DNS サーバーを更新する 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。

13. （オプション）[Description] に、ディレクトリの説明を入力します。
14. [Size] を [Small] のままにします。
15. [VPC] で、自分の VPC を選択します。
16. [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。
17. [Create directory] (ディレクトリの作成) を選択します。

18. WorkSpaces コンソールのディレクトリの作成ページに戻ります。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 (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。

## WorkSpaces Personal の AWS Managed Microsoft AD ディレクトリとオンプレミスドメインの間に信頼関係を作成する

このチュートリアルでは、 AWS Managed Microsoft AD ディレクトリとオンプレミスドメインの間の信頼関係を作成します。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 Personal のディレクトリを作成する」を参照してください。

> **Note**
>
> 別の信頼されたドメイン AWS アカウント で を使用して WorkSpaces を起動すると、オンプレミスディレクトリとの信頼関係で設定されている場合、 AWS Managed Microsoft AD と連携します。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。

信頼関係をセットアップするには

1. Virtual Private Cloud (VPC) で AWS Managed Microsoft AD を設定します。詳細については、「 管理ガイド」の AWS 「 Managed Microsoft AD ディレクトリの作成」を参照してください。 AWS Directory Service

   > **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。
   > - AWS Managed Microsoft AD ディレクトリがマルチリージョンレプリケーション用に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の Amazon WorkSpaces での使用は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の間に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の間に信頼関係を作成する」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、AWS 「 Directory Service で一方向信頼リソースドメインを使用して Amazon WorkSpaces をデプロイする」を参照してください。

> **Note**
>
> - Red Hat Enterprise Linux、Rocky Linux、および Ubuntu WorkSpaces は、Active Directory 統合に System Security Services Daemon (SSSD) を使用し、SSSD はフォレストの信頼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、Ubuntu、Rocky Linux、Red Hat Enterprise Linux WorkSpaces では、双方向の信頼をお勧めします。
> - ウェブブラウザ (Web Access) を使用して Linux WorkSpaces に接続することはできません。

## WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する

このチュートリアルでは、Microsoft Entra ID に参加し、Microsoft Intune に登録されている Bring Your Own License (BYOL) の Windows 10 および 11 個人用 WorkSpaces を作成します。このような WorkSpaces を作成する前に、まず Entra ID に参加している WorkSpaces 専用の WorkSpaces Personal ディレクトリを作成する必要があります。

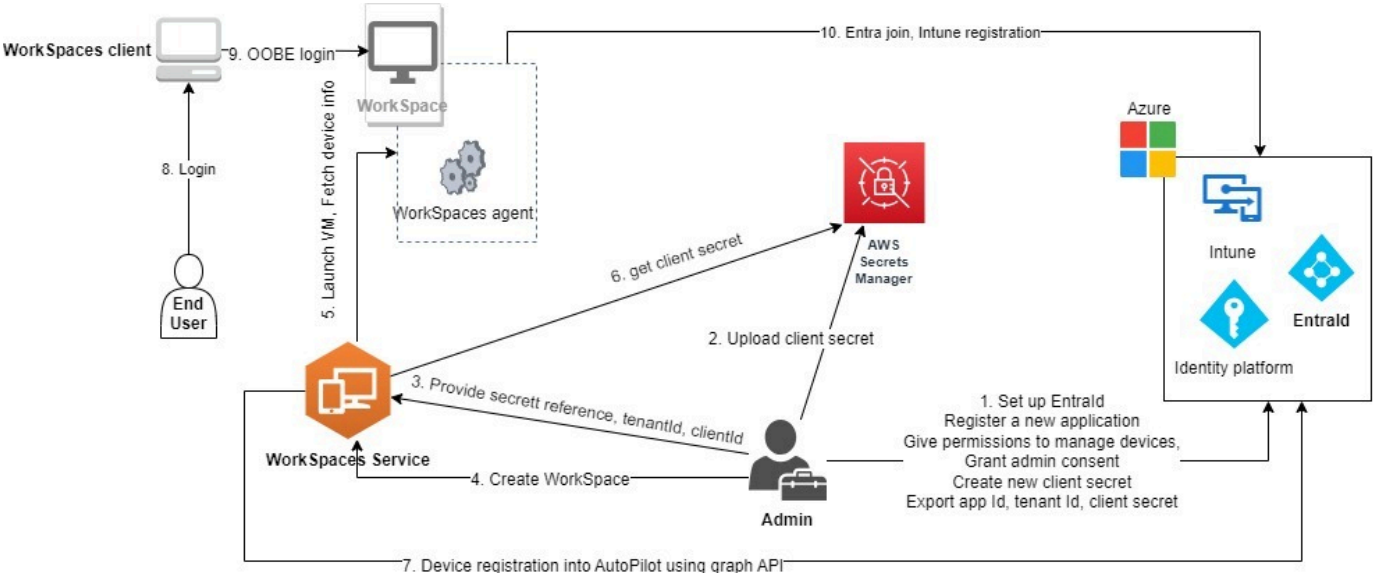
> **Note**
>
> Microsoft Entra に参加している個人用 WorkSpaces は、アフリカ (ケープタウン ) 、イスラエル (テルアビブ ) 、中国 (寧夏) を除く、Amazon WorkSpaces が提供されているすべての AWS リージョンで利用できます。

内容

- 要件と制限
- ステップ 1: IAM アイデンティティセンターを有効にして Microsoft Entra ID と同期する
- ステップ 2: Microsoft Entra ID アプリケーションを登録して Windows Autopilot のアクセス許可を付与する
- ステップ 3: Windows Autopilot のユーザードリブンモードを設定する
- ステップ 4: AWS Secrets Manager シークレットを作成する
- ステップ 5: 専用の Microsoft Entra ID WorkSpaces ディレクトリを作成する
- WorkSpaces ディレクトリの IAM アイデンティティセンターアプリケーションを設定する (オプション)
- クロスリージョン IAM アイデンティティセンター統合を作成する (オプション )

## 概要

Microsoft Entra ID 個人用 WorkSpaces ディレクトリには、Microsoft Entra ID で管理されているユーザーに割り当てられた Microsoft Entra ID 参加済みの WorkSpaces を起動するために必要なすべての情報が含まれます。ユーザー情報は、IAM Identity Center AWS を通じて WorkSpaces で利用できるようになります。IAM Identity Center は、従業員 ID を Entra ID から に持ち込むための ID ブローカーとして機能します AWS。WorkSpaces の Intune への登録と Entra への参加は、Microsoft Windows Autopilot のユーザードリブンモードを使って実行します。以下の図は、Autopilot のプロセスを示したものです。




## 要件と制限

- Microsoft Entra ID P1 プラン以上。

- Microsoft Entra ID と Intune が有効になっており、ロールが割り当てられていること。
- Intune 管理者 - Autopilot デプロイプロファイルの管理に必要です。
- グローバル管理者 - ステップ 3 で作成されたアプリケーションに割り当てられる API アクセス許可に対して、管理者の同意を付与するために必要です。アプリケーションは、このアクセス許可なしで作成できます。ただし、グローバル管理者がアプリケーションのアクセス許可について管理者の同意を付与する必要があります。
- WorkSpaces ユーザーに Windows 10/11 VDA E3 または E5 ユーザーサブスクリプションライセンスを割り当てます。
- Entra ID ディレクトリは、Windows 10 または 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces のみをサポートします。サポートされているバージョンは次のとおりです。
  - 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 11 Enterprise 23H2 (2023 年 10 月リリース)
  - Windows 11 Enterprise 22H2 (2022 年 10 月リリース)
- Bring Your Own License (BYOL) が AWS アカウントに対して有効になっており、有効な Windows 10 または 11 BYOL イメージがアカウントにインポートされている。詳細については、「WorkSpaces で自分の Windows デスクトップライセンスを使用する」を参照してください。
- Microsoft Entra ID ディレクトリは、Windows 10 または 11 の BYOL の個人用 WorkSpaces のみをサポートします。
- Microsoft Entra ID ディレクトリは DCV プロトコルのみをサポートします。

ステップ 1: IAM アイデンティティセンターを有効にして Microsoft Entra ID と同期する

Microsoft Entra ID に参加している個人用 WorkSpaces を作成して Entra ID ユーザーに割り当てるには、IAM Identity Center AWS を介してユーザー情報を で使用できるようにする必要があります。IAM Identity Center は、 AWS リソースへのユーザーアクセスを管理するために推奨される AWS サービスです。詳細については、「IAM アイデンティティセンターとは」を参照してください。これは 1 回限りの設定です。

WorkSpaces と統合する既存の IAM Identity Center インスタンスがない場合は、WorkSpaces と同じリージョンにインスタンスを作成することをお勧めします。別のリージョンに既存の AWS Identity Center インスタンスがある場合は、クロスリージョン統合を設定できます。クロスリージョン設定の詳細については、「」を参照してくださいthe section called “ クロスリージョン IAM アイデンティティセンター統合を作成する (オプション ) ”。

> **Note**
>
> WorkSpaces と IAM Identity Center 間のクロスリージョン統合は、 ではサポートされていません AWS GovCloud (US) Region。

1. 特にマルチアカウント環境を使用している場合は、 AWS Organizations で IAM Identity Center を有効にします。IAM アイデンティティセンターのアカウントインスタンスを作成することもできます。詳細については、「IAM Identity Center AWS の有効化」を参照してください。WorkSpaces の各ディレクトリは、IAM アイデンティティセンターの 1 つのインスタンス、組織、またはアカウントに関連付けることができます。

   組織インスタンスを使用して、メンバーアカウントの 1 つに WorkSpaces ディレクトリを作成しようとしている場合は、次の IAM アイデンティティセンターのアクセス許可があることを確認してください。

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`
   - `"sso:PutApplicationAuthenticationMethod"`
   - `"sso:DeleteApplication"`
   - `"sso:DescribeApplication"`
   - `"sso:getApplicationGrant"`

   詳細については、「IAM アイデンティティセンターリソースへのアクセス許可の管理の概要」を参照してください。また、これらのアクセス許可をブロックするサービスコントロールポリシー (SCP) がないことを確認してください。SCP の詳細については、「サービスコントロールポリシー (SCP)」を参照してください。
2. Entra ID テナントから選択したユーザーまたはすべてのユーザーを IAM アイデンティティセンターのインスタンスに自動的に同期するように、IAM アイデンティティセンターと Microsoft Entra ID を設定します。詳細については、「Microsoft Entra ID と IAM アイデンティティセンターで SAML と SCIM を設定する」および「チュートリアル: 自動ユーザープロビジョニング用に AWS IAM アイデンティティセンターを設定する」を参照してください。
3. Microsoft Entra ID で設定したユーザーが IAM Identity Center AWS インスタンスに正しく同期されていることを確認します。Microsoft Entra ID にエラーメッセージが表示された場合は、Entra

ID のユーザーの設定が、IAM アイデンティティセンターでサポートされていないことを示しています。この問題はエラーメッセージによって識別できます。例えば、Entra ID のユーザーオブジェクトに、姓、名、または表示名がない場合、次のようなエラーメッセージが表示されます。"2 validation errors detected: Value at 'name.givenName' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+; Value at 'name.givenName' failed to satisfy constraint: Member must have length greater than or equal to 1"。詳細については、「特定のユーザーが外部 SCIM プロバイダーから IAM アイデンティティセンターに同期できない」を参照してください。

> **Note**
>
> WorkSpaces は Entra ID の UserPrincipalName (UPN) 属性を使用して個々のユーザーを識別します。UPN の制限事項は次のとおりです。
>
> - UPN の長さが 63 文字を超えることはできません。
> - WorkSpace をユーザーに割り当てた後に UPN を変更した場合、UPN を元に戻さない限り、ユーザーは WorkSpace に接続できません。

ステップ 2: Microsoft Entra ID アプリケーションを登録して Windows Autopilot のアクセス許可を付与する

WorkSpaces Personal は、Microsoft Windows Autopilot のユーザードリブンモードを使用して WorkSpaces を Microsoft Intune に登録し、Microsoft Entra ID に参加させます。

Amazon WorkSpaces で WorkSpaces Personal を Autopilot に登録できるようにするには、必要な Microsoft Graph API アクセス許可を付与する Microsoft Entra ID アプリケーションを登録する必要があります。Entra ID アプリケーションの登録の詳細については、「クイック スタート: Microsoft ID プラットフォームにアプリケーションを登録する」を参照してください。

Entra ID アプリケーションで次の API アクセス許可を付与することをお勧めします。

- Entra ID に参加させる新しい個人用 WorkSpace を作成する場合は、次の API アクセス許可が必要です。
  - `DeviceManagementServiceConfig.ReadWrite.All`
- 個人用 WorkSpace を終了または再構築する場合は、次のアクセス許可が使用されます。

> **Note**
>
> これらのアクセス許可を付与しなくても WorkSpace は終了できますが、Intune テナントおよび Entra ID テナントからは削除されないため、個別に削除する必要があります。

  - `DeviceManagementServiceConfig.ReadWrite.All`
  - `Device.ReadWrite.All`
  - `DeviceManagementManagedDevices.ReadWrite.All`
- これらのアクセス許可には管理者の同意が必要です。詳細については、「アプリケーションに対してテナント全体の管理者の同意を付与する」を参照してください。

次に、Entra ID アプリケーションのクライアントシークレットを追加する必要があります。詳細については、「資格情報を追加する」を参照してください。ステップ 4 で AWS Secrets Manager シークレットを作成するときに必要になるため、クライアントシークレットの文字列を必ず覚えておいてください。

ステップ 3: Windows Autopilot のユーザードリブンモードを設定する

Windows Autopilot のユーザードリブンモードによって Intune で Microsoft Entra への参加を実行する方法について、チュートリアルをよく確認しておいてください。

Autopilot のために Microsoft Intune を設定するには

1. Microsoft Intune 管理センターにサインインします。
2. 個人用 WorkSpaces 向けに新しい Autopilot のデバイスグループを作成します。詳細については、「Windows Autopilot のデバイスグループを作成する」を参照してください。
   a. [グループ]、[新しいグループ] の順に選択します。
   b. [Group type] (グループの種類) で、[Security] (セキュリティ) を選択します。
   c. [メンバーシップの種類] で [動的デバイス] を選択します。
   d. [Edit dynamic query] を選択して、動的メンバーシップルールを作成します。ルールは次のような形式になります。

```
(device.devicePhysicalIds -any (_ -eq "[OrderID]:WorkSpacesDirectoryName"))
```

> **Important**
>
> `WorkSpacesDirectoryName` は、ステップ 5 で作成する Entra ID WorkSpaces Personal ディレクトリのディレクトリ名と一致している必要があります。これは、WorkSpaces が仮想デスクトップを Autopilot に登録するときに、ディレクトリ名の文字列がグループタグとして使用されるためです。さらに、グループタグは Microsoft Entra デバイスの `OrderID` 属性にマッピングされます。

3. [デバイス]、[Windows]、[登録] の順に選択します。[登録オプション] で [自動登録] を選択します。[MDM ユーザースコープ] で [すべて] を選択します。
4. Autopilot デプロイプロファイルを作成します。詳細については、「Autopilot Deployment プロファイルを作成する」を参照してください。

   a. [Windows Autopilot] で [デプロイプロファイル]、[プロファイルの作成] の順に選択します。

   b. [Windows AutoPilot Deployment プロファイル] 画面で、[プロファイルの作成] ドロップダウンメニューを選択し、[Windows PC] を選択します。

   c. [プロファイルの作成] 画面の [On the Out-of-box experience (OOBE)] ページを開きます。[配置モード] で [ユーザードリブン] を選択します。[Microsoft Entra ID に参加] で [Microsoft Entra 参加済み] を選択します。Entra ID に参加済みの個人用 WorkSpaces でコンピュータ名をカスタマイズするには、[デバイス名テンプレートを適用する] で [はい] を選択し、登録時のデバイスの名前付けに使用するテンプレートを作成します。

   d. [割り当て] ページの [割り当てる] で、[選択したグループ] を選択します。[含めるグループを選択する] を選択し、2 で作成した Autopilot デバイスグループを選択します。

### ステップ 4: AWS Secrets Manager シークレットを作成する

で作成した Entra ID アプリケーションのアプリケーション ID やクライアントシークレットなどの情報を安全に保存 AWS Secrets Manager するには、 にシークレットを作成する必要がありますステップ 2: Microsoft Entra ID アプリケーションを登録して Windows Autopilot のアクセス許可を付与する。これは 1 回限りの設定です。

AWS Secrets Manager シークレットを作成するには

1. カスタマーマネージドキーを AWS Key Management Service で作成します。キーは後で AWS Secrets Manager シークレットの暗号化に使用されます。WorkSpaces サービスではデフォルト

のキーにアクセスできないため、デフォルトのキーを使用してシークレットを暗号化しないでください。キーは以下の手順で作成します。

a. AWS KMS コンソールを https://console.aws.amazon.com/kms://https://https://https://https://https://https を

b. 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ーを使用します。

c. [Create key] (キーの作成) を選択します。

d. [キーを設定] ページの [キーのタイプ] で、[対称] を選択します。[キーの使用方法] で [暗号化および復号化] を選択します。

e. [確認] ページのキーポリシーエディタで、キーポリシーに次のアクセス許可が含まれ、WorkSpaces サービスのプリンシパル `workspaces.amazonaws.com` からキーへのアクセスが許可されていることを確認します。

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "workspaces.amazonaws.com"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*"
 }
```

2. 前のステップで作成した AWS KMS キーを使用して AWS Secrets Manager、 にシークレットを作成します。

a. Secrets Manager のコンソール (https://console.aws.amazon.com/secretsmanager/) を開きます。

b. [Store a new secret] (新しいシークレットを保存する) を選択します。

c. [シークレットタイプの選択] ページの[シークレットタイプ] で[その他のシークレットタイプ] を選択します。

d. [キー/値のペア] の キーボックスに「application_id」と入力し、値ボックスにステップ 2 の Entra ID アプリケーションの ID をコピーして貼り付けます。

e. キーボックスで [行を追加] を選択して「application_password」と入力し、値ボックスにステップ 2 の Entra ID アプリケーションのクライアントシークレットをコピーして貼り付けます。

f. 前のステップで作成した AWS KMS キーを暗号化キードロップダウンリストから選択します。

g. [次へ] を選択します。

h. [シークレットを設定] ページで、[シークレットの名前] と [説明] を入力します。

i. [リソースのアクセス許可] セクションで、[許可を編集] を選択します。

j. リソースのアクセス許可に次のリソースポリシーを含め、WorkSpaces サービスのプリンシパル `workspaces.amazonaws.com` にシークレットへのアクセスを必ず許可します。

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : [ "workspaces.amazonaws.com"]
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*"
  } ]
}
```

ステップ 5: 専用の Microsoft Entra ID WorkSpaces ディレクトリを作成する

Microsoft Entra ID に参加済みの WorkSpaces および Entra ID ユーザーの情報を保存する専用の WorkSpaces ディレクトリを作成します。

Entra ID WorkSpaces ディレクトリを作成するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com 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. [ディレクトリの作成] ページの [WorkSpaces タイプ] で、[個人] を選択します。[WorkSpace デバイス管理] で [Microsoft Entra ID] を選択します。

4. Microsoft Entra テナント ID には、ディレクトリの WorkSpaces を結合する Microsoft Entra ID テナント ID を入力します。ディレクトリの作成後にテナント ID を変更することはできません。
5. Entra ID アプリケーション ID とパスワードで、ステップ 4 で作成した AWS Secrets Manager シークレットをドロップダウンリストから選択します。ディレクトリの作成後に、ディレクトリに関連付けられたシークレットを変更することはできません。ただし、Entra ID アプリケーション ID やパスワードなど、シークレットの内容は、いつでも https://console.aws.amazon.com/secretsmanager/://www.com の AWS Secrets Manager コンソールから更新できます。
6. IAM Identity Center インスタンスが WorkSpaces ディレクトリと同じ AWS リージョンにある場合、ユーザー ID ソースとして、ステップ 1 で設定した IAM Identity Center インスタンスをドロップダウンリストから選択します。ディレクトリの作成後に、ディレクトリに関連付けられた IAM アイデンティティセンターのインスタンスを変更することはできません。

   IAM Identity Center インスタンスが WorkSpaces ディレクトリとは異なる AWS リージョンにある場合は、クロスリージョンを有効にするを選択し、ドロップダウンリストからリージョンを選択します。

   > **Note**
   >
   > 別のリージョンに既存の IAM Identity Center インスタンスがある場合は、クロスリージョン統合をセットアップするためにオプトインする必要があります。クロスリージョン設定の詳細については、「」を参照してくださいthe section called “ クロスリージョン IAM アイデンティティセンター統合を作成する (オプション ) ”。

7. [ディレクトリ名] に、ディレクトリの一意の名前 (`WorkSpacesDirectoryName` など) を入力します。

   > **Important**
   >
   > ディレクトリ名は、ステップ 3 で Microsoft Intune を使って作成した Autopilot デバイスグループの動的クエリを作成するのに使用される `OrderID` と一致している必要があります。ディレクトリ名の文字列は、個人用 WorkSpaces を Windows Autopilot に登録するときにグループタグとして使用されます。グループタグは、Microsoft Entra デバイスの `OrderID` 属性にマッピングされます。

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

9. [VPC] で、WorkSpaces の起動に使用した VPC を選択します。詳細については、「WorkSpaces Personal 用に VPC を設定する」を参照してください。
10. [サブネット] で、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個人用 WorkSpaces の起動に使用されます。詳細については、「WorkSpaces Personal のアベイラビリティーゾーン」を参照してください。

> **Important**
>
> サブネットで起動された WorkSpaces にインターネットアクセスがあることを確認します。インターネットアクセスは、ユーザーが Windows デスクトップにログインするときに必要です。詳細については、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

11. [設定] で、[専用 WorkSpace を有効化] を選択します。専用の WorkSpaces Personal ディレクトリを作成して、Windows 10 または 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces を起動するには、これを有効にする必要があります。

> **Note**
>
> [設定] に [専用 WorkSpace を有効化] オプションが表示されない場合、アカウントで BYOL が有効になっていません。アカウントで BYOL を有効にするには、「WorkSpaces で自分の Windows デスクトップライセンスを使用する」を参照してください。

12. (オプション) [タグ] で、ディレクトリ内の個人用 WorkSpaces に使用するキーペアの値を指定します。
13. ディレクトリの概要を確認し、[ディレクトリの作成] を選択します。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 `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。

ディレクトリが作成されると、IAM アイデンティティセンターアプリケーションも自動的に作成されます。アプリケーションの ARN を検索するには、ディレクトリの概要ページに移動します。

これで、Microsoft Intune に登録され、Microsoft Entra ID に参加している Windows 10 または 11 の個人用 WorkSpaces を、ディレクトリを使用して起動できるようになりました。詳細については、「WorkSpaces Personal で WorkSpace を作成する」を参照してください。

WorkSpaces Personal ディレクトリを作成したら、個人用 WorkSpaces を作成できます。詳細については、WorkSpaces Personal で WorkSpace を作成するを参照してください。

WorkSpaces ディレクトリの IAM アイデンティティセンターアプリケーションを設定する (オプション)

ディレクトリが作成されると、対応する IAM アイデンティティセンターアプリケーションが自動的に作成されます。アプリケーションの ARN は、ディレクトリの詳細ページの [概要] セクションにあります。デフォルトでは、アイデンティティセンターインスタンスのすべてのユーザーは、対応するアイデンティティセンターアプリケーションを設定しなくても、割り当てられた WorkSpaces にアクセスできます。ただし、IAM アイデンティティセンターアプリケーションのユーザー割り当てを設定することで、ディレクトリ内の WorkSpaces へのユーザーアクセスを管理できます。

IAM アイデンティティセンターアプリケーションのユーザー割り当てを設定するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. [AWS マネージドアプリケーション] タブで、WorkSpaces ディレクトリのアプリケーションを選択します。アプリケーション名は `WorkSpaces.wsd-xxxxx` の形式です。`wsd-xxxxx` は WorkSpaces ディレクトリ ID です。
3. [アクション]、[詳細を編集] の順に選択します。
4. [ユーザーとグループの割り当て方法] を、[割り当ては不要] から [割り当てが必要] に変更します。
5. [Save changes] (変更の保存) をクリックします。

この変更を行うと、アイデンティティセンターインスタンスのユーザーは、アプリケーションに割り当てられていない限り、割り当てられた WorkSpaces にアクセスできなくなります。ユーザーをアプリケーションに割り当てるには、 AWS CLI コマンドを使用してユーザーまたはグループをアプリケーションに`create-application-assignment`割り当てます。詳細については、『AWS CLI コマンドリファレンス』を参照してください。

クロスリージョン IAM アイデンティティセンター統合を作成する (オプション )

WorkSpaces と関連する IAM Identity Center インスタンスが同じ AWS リージョンにあることをお勧めします。ただし、WorkSpaces リージョンとは異なるリージョンに IAM Identity Center インスタンスがすでに設定されている場合は、クロスリージョン統合を作成できます。クロスリージョン WorkSpaces と IAM Identity Center の統合を作成すると、WorkSpaces がクロスリージョン呼び出しを実行して、ユーザー属性やグループ属性などの IAM Identity Center インスタンスから情報にアクセスして保存できるようになります。

> **Important**
>
> Amazon WorkSpaces は、組織レベルのインスタンスに対してのみ、クロスリージョン IAM アイデンティティセンターと WorkSpaces の統合をサポートします。WorkSpaces は、アカウントレベルのインスタンスのクロスリージョン IAM アイデンティティセンター統合をサポートしていません。IAM Identity Center インスタンスタイプとそのユースケースの詳細については、「IAM Identity Center インスタンスのタイプを理解する」を参照してください。

WorkSpaces ディレクトリと IAM Identity Center インスタンスの間にクロスリージョン統合を作成すると、クロスリージョン呼び出しにより、WorkSpaces をデプロイするときやログイン中にレイテンシーが高くなる可能性があります。レイテンシーの増加は、WorkSpaces リージョンと IAM アイデンティティセンターリージョン間の距離に比例します。特定のユースケースに対してレイテンシーテストを実行することをお勧めします。

クロスリージョン IAM Identity Center 統合を作成する前に、オプトインプロセスを完了して、 AWS アカウントがこの機能を使用できるようにする必要があります。開始するには、 AWS アカウントマネージャー、販売担当者、または AWS サポートセンターにお問い合わせください。このプロセスを完了するまで、WorkSpaces ディレクトリの作成時に Amazon WorkSpaces コンソールでクロスリージョン IAM WorkSpaces アイデンティティセンターサポートを有効にするオプションは使用できません。

> **Note**
>
> このオプトインプロセスを完了するには、少なくとも 1 営業日が必要です。

オプトインしたら、ステップ 5: 専用の Microsoft Entra ID WorkSpaces ディレクトリを作成するときに、クロスリージョン IAM アイデンティティセンター接続を有効にできます。ユーザー ID ソースで、ドロップダウンメニューthe section called “ステップ 1: IAM アイデンティティセンターを有効にして Microsoft Entra ID と同期する”から で設定した IAM Identity Center インスタンスを選択します。

> **Important**
>
> ディレクトリの作成後に、そのディレクトリに関連付けられた IAM Identity Center インスタンスを変更することはできません。

# WorkSpaces Personal で専用のカスタムディレクトリを作成する

Windows 10 および 11 BYOL 個人用 WorkSpaces を作成し、IAM Identity Center Identity Providers (IdPs AWS で管理されているユーザーに割り当てる前に、専用のカスタム WorkSpaces ディレクトリを作成する必要があります。個人用 WorkSpaces が Microsoft Active Directory に参加していなくても、JumpCloud などの任意のモバイルデバイス管理 (MDM) ソリューションで管理できます。JumpCloud の詳細については、こちらの記事を参照してください。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 Personal のディレクトリを作成する」を参照してください。

> **Note**
>
> - Amazon WorkSpaces では、カスタムディレクトリで起動された個人用 WorkSpaces でユーザーアカウントを作成したり管理したりすることはできません。ユーザーアカウントは管理者が管理する必要があります。
> - カスタム WorkSpaces ディレクトリは、アフリカ (ケープタウン ) 、イスラエル (テルアビブ ) 、中国 (寧夏) を除く、Amazon WorkSpaces が提供されているすべての AWS リージョンで利用できます。
> - Amazon WorkSpaces では、カスタムディレクトリを使用した WorkSpaces でユーザーアカウントを作成したり管理したりすることはできません。使用している MDM エージェントソフトウェアによって Windows WorkSpaces でユーザープロファイルを作成できるようにするには、MDM ソリューションプロバイダーにお問い合わせください。ユーザープロファイルを作成すると、ユーザーは Windows ログイン画面から Windows デスクトップにサインインできます。

内容



## 要件と制限

- WorkSpaces カスタムディレクトリは、Windows 10 または 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces のみをサポートします。
- WorkSpaces カスタムディレクトリは DCV プロトコルのみをサポートします。

- AWS アカウントで BYOL を有効にし、個人用 WorkSpaces が Windows 10 および 11 アクティベーションのためにアクセスできる独自の AWS KMS サーバーがあることを確認します。詳細については、「WorkSpaces で自分の Windows デスクトップライセンスを使用する」を参照してください。
- AWS アカウントにインポートした BYOL イメージに MDM エージェントソフトウェアをプリインストールしてください。

### ステップ 1: IAM アイデンティティセンター を有効にして ID プロバイダーに接続する

ID プロバイダーで管理されているユーザーに WorkSpaces を割り当てるには、 AWS IAM Identity Center AWS を通じてユーザー情報を で利用できるようにする必要があります。IAM Identity Center を使用して、 AWS リソースへのユーザーのアクセスを管理することをお勧めします。詳細については、「IAM アイデンティティセンターとは」を参照してください。これは 1 回限りの設定です。

#### ユーザー情報を で利用できるようにするには AWS

1. で IAM アイデンティティセンターを有効にします AWS。特にマルチアカウント環境を使用している場合は、 AWS 組織で IAM アイデンティティセンターを有効にできます。IAM アイデンティティセンターのアカウントインスタンスを作成することもできます。詳細については、「IAM Identity Center AWS の有効化」を参照してください。WorkSpaces の各ディレクトリは、IAM アイデンティティセンターの 1 つの組織またはアカウントインスタンスに関連付けることができます。IAM アイデンティティセンターの各インスタンスは、1 つ以上の WorkSpaces Personal ディレクトリに関連付けることができます。

   組織インスタンスを使用して、メンバーアカウントの 1 つに WorkSpaces ディレクトリを作成しようとしている場合は、次の IAM アイデンティティセンターのアクセス許可があることを確認してください。

   - `"sso:DescribeInstance"`
   - `"sso:CreateApplication"`
   - `"sso:PutApplicationGrant"`
   - `"sso:PutApplicationAuthenticationMethod"`
   - `"sso:DeleteApplication"`
   - `"sso:DescribeApplication"`
   - `"sso:getApplicationGrant"`

詳細については、「IAM アイデンティティセンターリソースへのアクセス許可の管理の概要」を参照してください。これらのアクセス許可をブロックするサービスコントロールポリシー (SCP) がないことを確認してください。SCP の詳細については、「サービスコントロールポリシー (SCP)」を参照してください。

2. ID プロバイダー (IdP) から IAM アイデンティティセンターのインスタンスにユーザーを自動的に同期するように、IAM アイデンティティセンター と IdP を設定します。詳細については、入門チュートリアルから、使用する IdP の特定のチュートリアルを選択してください。例えば、「IAM アイデンティティセンターを使用して JumpCloud ディレクトリプラットフォームに接続する」を参照できます。
3. IdP で設定したユーザーが IAM Identity Center AWS インスタンスに正しく同期されていることを確認します。IdP の設定によっては、最初の同期に最大 1 時間かかる場合があります。

### ステップ 2: 専用のカスタム WorkSpaces ディレクトリを作成する

個人用 WorkSpaces とユーザーに関する情報を保存する専用の WorkSpaces Personal ディレクトリを作成します。

専用のカスタム WorkSpaces ディレクトリを作成するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [Create directory] (ディレクトリの作成) を選択します。
4. [ディレクトリの作成] ページの [WorkSpaces] タイプで、[個人] を選択します。[WorkSpace デバイス管理] で、[カスタム] を選択します。
5. [ユーザー ID ソース] で、ドロップダウンリストからステップ 1 で設定した IAM アイデンティティセンターのインスタンスを選択します。ディレクトリが作成されると、ディレクトリに関連付けられた IAM アイデンティティセンターのインスタンスは変更できなくなります。

> **Note**
>
> ディレクトリには IAM アイデンティティセンターのインスタンスを指定する必要があります。指定しないと、WorkSpaces コンソールを使用してディレクトリで個人用 WorkSpaces を起動できません。アイデンティティセンターが関連付けられていない

WorkSpaces ディレクトリは、WorkSpaces Core パートナーソリューションにだけ対応します。

6. [ディレクトリ名] に、ディレクトリの一意の名前を入力します。
7. [VPC] で、WorkSpaces の起動に使用した VPC を選択します。詳細については、「WorkSpaces Personal 用に VPC を設定する」を参照してください。
8. [サブネット] で、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個人用 WorkSpaces の起動に使用されます。詳細については、「WorkSpaces Personal のアベイラビリティーゾーン」を参照してください。

> **Important**
>
> サブネットで起動された WorkSpaces にインターネットアクセスがあることを確認します。インターネットアクセスは、ユーザーが Windows デスクトップにログインするときに必要です。詳細については、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

9. [設定] で、[専用 WorkSpace を有効化] を選択します。専用の WorkSpaces Personal ディレクトリを作成して、Windows 10 または 11 の Bring Your Own License (BYOL) の個人用 WorkSpaces を起動するには、これを有効にする必要があります。
10. (オプション) [タグ] で、ディレクトリ内の個人用 WorkSpaces に使用するキーペアの値を指定します。
11. ディレクトリの概要を確認し、[ディレクトリの作成] を選択します。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 `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。

ディレクトリが作成されると、IAM アイデンティティセンターアプリケーションも自動的に作成されます。アプリケーションの ARN を検索するには、ディレクトリの概要ページに移動します。

これで、Microsoft Intune に登録され、Microsoft Entra ID に参加している Windows 10 または 11 の個人用 WorkSpaces を、ディレクトリを使用して起動できるようになりました。詳細については、「WorkSpaces Personal で WorkSpace を作成する」を参照してください。

WorkSpaces Personal ディレクトリを作成したら、個人用 WorkSpaces を作成できます。詳細については、WorkSpaces Personal で WorkSpace を作成する を参照してください。

# WorkSpaces Personal の DNS サーバーを更新する

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)、WorkSpaces Personal の WorkSpace を再構築する 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、WorkSpaces Personal で Windows WorkSpaces を管理する 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。

### Amazon Linux 2 WorkSpaces の DNS サーバー設定を更新する

Amazon Linux 2 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、Ansible を使用できます。

Amazon Linux 2 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。
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。

### Ubuntu WorkSpaces の DNS サーバー設定を更新する

Ubuntu 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、Landscape を使用できます。

Ubuntu WorkSpace で DNS サーバー設定を更新するには

1. Ubuntu WorkSpace でターミナルウィンドウを開き、次のコマンドを実行します。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/netplan/zz-workspaces-domain.yaml
   ```

2. yaml ファイルに、次の nameserver コマンドが表示されます。

   ```
   nameservers:
       search:[Your domain FQDN]
       addresses:[OldIP1, OldIP2]
   ```

   *OldIP1* と *OldIP2* を *NewIP1* と *NewIP2* に置き換えます。

   複数の DNS サーバーの IP アドレスがある場合は、カンマで区切って値を追加します。例えば、[*NewDNSIP1*, *NewDNSIP2*, *NewDNSIP3*] と指定します。

3. yaml ファイルを保存します。
4. コマンド sudo netplan apply を実行して変更を適用します。
5. コマンド resolvectl status を実行して、新しい DNS IP アドレスが使用されていることを確認します。
6. ステップ 2 に進み、Active Directory の DNS サーバー設定を更新します。

Red Hat Enterprise Linux WorkSpaces の DNS サーバー設定を更新する

Red Hat Enterprise 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、Ansible を使用できます。

Red Hat Enterprise Linux WorkSpace で DNS サーバー設定を更新するには

1. Red Hat Enterprise Linux WorkSpace でターミナルウィンドウを開き、次のコマンドを実行します。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 nmcli conn modify CustomerNIC ipv4.dns 'NewIP1 NewIP2'
   ```

2. 以下のコマンドを実行してください。

```
sudo systemctl restart NetworkManager
```

3. 更新された DNS とネットワーク設定を確認するために、次のコマンドを実行します。

```
nmcli device show eth1
```

4. ステップ 2 に進み、Active Directory の DNS サーバー設定を更新します。

### 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 Managed 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。

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 Personal でディレクトリを削除する

> **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、すべてのディレクトリデータとスナップショットが削除され、復元できなくなります。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。インスタンスにローカル AWS アカウント な を使用して、これらのインスタンスにログイン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。

### Entra ID またはカスタム WorkSpaces ディレクトリを削除する

Entra ID WorkSpaces ディレクトリを使用すると、Entra ID に参加している Windows 10 または 11 の BYOL WorkSpaces を作成できます。詳細については、「WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する」を参照してください。

カスタム WorkSpaces ディレクトリを使用すると、Active Directory ドメインに参加せずに、独自のデバイス管理ソフトウェアと IAM アイデンティティセンターを使用する WorkSpaces を作成できます。詳細については、「WorkSpaces Personal で専用のカスタムディレクトリを作成する」を参照してください。

Entra ID またはカスタム WorkSpaces 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、「WorkSpaces Personal で WorkSpace を削除する」を参照してください。
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. [アクション]、[削除] の順に選択します。
5. 確認を求められたら、[削除] をクリックします。

## AWS Directory Service ディレクトリを削除する

WorkSpaces の AWS Directory Service ディレクトリは、他の WorkSpaces や WorkDocs Amazon WorkMail 、Amazon Chime などの他のアプリケーションで使用されなくなった場合に削除できます。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。

ディレクトリの登録を解除するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. 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。

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、「WorkSpaces Personal で WorkSpace を削除する」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/v2/home 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 Personal で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 Personal で 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 Personal 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一元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 ですAdmin。

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 には適用されません。 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「Manage Users and Groups in AWS Managed Microsoft AD」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、「WorkSpaces Personal で WorkSpace を削除する」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「Manage Users and Groups in AWS Managed Microsoft AD」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 AWS GovCloud (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 Personal で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。

内容

# WorkSpaces Personal のユーザーを管理する

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使用できます。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。Microsoft Entra ID またはカスタム WorkSpaces ディレクトリを使用する場合は、Microsoft Entra ID または ID プロバイダー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/v2/home「https://www.com」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 Personal で 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、「WorkSpaces Personal で WorkSpace を削除する」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、「 管理ガイド」の「Manage Users and Groups in AWS Managed Microsoft AD」を参照してください。 AWS Directory Service
- 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/v2/home「https://www.com」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。

## WorkSpaces Personal で 1 人のユーザーに対して複数の 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場合に限り、ユーザーは PCoIP WorkSpace と DCV WorkSpace の両方を持つことができます。同じユーザーが PCoIP WorkSpace と DCV 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 を設定し、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、WorkSpaces Personal のクロスリージョンリダイレクト 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。

## WorkSpaces Personal の WorkSpaces へのユーザーログイン方法をカスタマイズする

Uniform Resource Identifier (URI) を使用して WorkSpaces へのユーザーのアクセスをカスタマイズして、組織内の既存のワークフローと統合された、簡素化されたログインエクスペリエンスを提供します。たとえば、WorkSpaces の登録コードを使用してユーザーを登録するログイン URI 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、WorkSpaces Personal のクロスリージョンリダイレクト を参照してください。

サポートされている次のデバイス上でのクライアントアプリケーションの、WorkSpaces 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

URI を使用して WorkSpaces にアクセスするには、まずユーザーが https://clients.amazonworkspaces.com/ を開き、手順に従って、デバイス用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 コンピュータ上の Firefox および Chrome ブラウザ、Ubuntu Linux 18.04、20.04、および 22.04 コンピュータ上の Firefox ブラウザ、および Windows コンピュータ上の 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。

WorkSpaces への URI アクセスを設定するには、次の表に説明するいずれかの URI 形式を使用します。

> **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 の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 の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 の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 の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**
>
> ユーザーがすでに Windows クライアントから WorkSpace 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 セッションが開いたままになります。ユーザーが macOS、iPad、または Android クライアントから WorkSpace に接続しているときに URI リンクを開くと、新しいセッションは開きません。元の WorkSpaces セッションのみが開いたままになります。

## WorkSpaces Personal でユーザーを対象とした WorkSpaces の自己管理機能を有効にする

WorkSpaces で、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。WorkSpaces 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。自己管理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、以下のタスクを 1 つ以上実行できるようになります。

- 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、ユーザーは認証情報を再度入力することなく、WorkSpace に再接続することができます。
- WorkSpace を再起動します。
- WorkSpace 上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。

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/v2/home「https://www.com」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. [セルフサービスアクセス許可] まで下にスクロールし、[編集] を選択ます。ユーザーが自分のクライアントから実行できる WorkSpace 管理タスクを確認するために、必要に応じて次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。認証情報をキャッシュするように設定すると、ユーザーは認証情報を再入力することなく、WorkSpaces 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。
   - Restart WorkSpace from client (WorkSpace をクライアントから再起動) — ユーザーは、WorkSpace を再起動できます。再起動すると、WorkSpace からユーザーを切断してシャットダウンしてから、再起動します。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。
   - Increase volume size (ボリュームサイズの拡張) — ユーザーは、WorkSpace のルートボリュームとユーザーボリュームを指定のサイズに拡張できます。IT サポートに連絡する必要はありません。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 175 GB まで、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 100 GB まで増やすことができます。セットグループに付属の WorkSpace ルートボリュームおよびユーザーボリュームは変更できません。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、「WorkSpaces Personal で WorkSpace を変更する」を参照してください

     新しく作成された WorkSpace の場合、これらのドライブのサイズを拡張するには、6 時間ほど待機する必要があります。それ以降、6 時間に 1 度のみ行うことができます。ボリュームサイズを拡大中の場合でも、ユーザーは自分の WorkSpace でほとんどのタスクを実行できます。WorkSpace の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、WorkSpace の再起動、WorkSpace の再構築のタスクは実行できません。プロセスが終了

したら、変更を有効にするために WorkSpace を再起動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**
>
> ユーザーが自分の WorkSpace のボリュームサイズを拡張すると、WorkSpace の請求レートも上がります。

- Change compute type (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) 間で WorkSpace を切り替えることができます。新しく作成された WorkSpace の場合、別のバンドルに切り替えるには、6 時間ほど待機する必要があります。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が変更中の場合、ユーザーは WorkSpace から切断されるため、WorkSpace を使用または変更することはできません。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、WorkSpace の請求レートが変わります。

- Switch running mode (実行モードの切り替え) — ユーザーは、[AlwaysOn] と [AutoStop] 実行モードの間で WorkSpace を切り替えることができます。詳細については、「WorkSpaces Personal 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 WorkSpace の実行モードを切り替えると、その WorkSpace の請求レートが変わります。

- Rebuild WorkSpace from client (クライアントから WorkSpace を再構築する) — WorkSpace のオペレーティングシステムは、元の状態に再構築できます。WorkSpace を再構築すると、ユーザーボリューム (D: ドライブ) は、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 WorkSpace の場合、WorkSpace を再構築するには、12 時間ほど待機する必要があります。WorkSpace の再構築が進行中の場合、ユーザーは WorkSpace から切断される

ため、WorkSpace を使用したり、変更を加えたりすることはできません。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、WorkSpaces クライアントの使用を中断することなく WorkSpaces クライアントのログファイルを直接 WorkSpaces にアップロードして、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、ユーザー自身でアップロードすると、ログファイルは自動的に WorkSpaces に送信されます。WorkSpaces ストリーミングセッション前または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。

5. [保存] を選択します。

## WorkSpaces Personal でユーザーの 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 DCV 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/v2/home「https://www.com」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/v2/home「https://www.com」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. [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. [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/v2/home「https://www.com」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。

## WorkSpaces Personal で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、Linux、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 (北米西部) 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により、WorkSpaces クライアントの使用を中断することなく WorkSpaces クライアントのログファイルを直接 WorkSpaces にアップロードして、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、ユーザー自身でアップロードすると、ログファイルは自動的に WorkSpaces に送信されます。WorkSpaces ストリーミングセッション前または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 WorkSpaces クライアントをインストールします。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/v2/home「https://www.com」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、WorkSpaces Windows、macOS、Linux クライアントによる API コールを使用した診断ログの自動アップロードを有効または無効にできます。有効にすると、クライアントで問題が発生すると、ユーザーの操作なしにログが WorkSpaces 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 クライアントバージョン 5.4.0 以降
>   - macOS クライアントバージョン 5.8.0 以降
>   - Ubuntu 22.04 クライアント 2023.1
>   - Ubuntu 20.04 クライアント 2023.1
>   - Web Access クライアントでも診断ログのアップロード機能にアクセスできます。

# WorkSpaces Personal の管理

WorkSpaces コンソールを使用して WorkSpaces 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**
>
> - ENA、NVMe、PV ドライバーなど、WorkSpaces のネットワーク依存関係ドライバーを必ず更新してください。この作業は、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)、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に関する説明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。この作業は、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 および EC2Launch の更新」を参照してください。

内容

- WorkSpaces Personal で WorkSpace を削除する

## WorkSpaces Personal で Windows WorkSpaces を管理する

グループポリシーオブジェクト (GPO) 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**
>
> - Microsoft Entra ID またはカスタム WorkSpaces ディレクトリを使用する場合は、Microsoft Entra ID または ID プロバイダーを使用してユーザーとグループを管理できます。詳細については、「WorkSpaces Personal で専用の Microsoft Entra ID ディレクトリを作成する」を参照してください。
> - Linux インスタンスはグループポリシーに従いません。Amazon Linux WorkSpaces の管理については、WorkSpaces Personal で Amazon Linux 2 WorkSpaces を管理する を参照してください。

WorkSpaces コンピュータオブジェクト用の組織単位と WorkSpaces ユーザーオブジェクト用の組織単位を作成することをお勧めします。

Amazon WorkSpaces に固有のグループポリシー設定を使用するには、使用しているプロトコル (PCoIP または DCV) 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必要があります。

> **Warning**
>
> グループポリシー設定は、WorkSpaces のユーザーエクスペリエンスに次のように影響する場合があります。
>
> - ログオンバナーを表示するためにインタラクティブなログオンメッセージを実装すると、ユーザーは自分の WorkSpaces にアクセスできなくなります。現在、インタラクティブなログオンメッセージのグループポリシー設定は PCoIP WorkSpaces でサポートされていません。ログオンメッセージは DCV WorkSpaces でサポートされており、ユーザーはログオンバナーを承諾した後に再度ログインする必要があります。証明書ベースのログオンが有効になっている場合、ログオンメッセージはサポートされていません。

- 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、そのユーザーは WorkSpaces クライアントアプリケーションを使用して認証できなくなります。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。
- 組み込みの Users グループを [Allow log on locally] (ローカルログオンを許可) セキュリティポリシーから削除すると、PCoIP WorkSpaces ユーザーは WorkSpaces クライアントアプリケーションを介して WorkSpaces に接続できなくなります。PCoIP WorkSpaces も、PCoIP エージェントソフトウェアの更新を受信しなくなります。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たり、WorkSpaces の新機能を有効にするものであったりする場合があります。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行うと、ユーザーは WorkSpaces にアクセスできません。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 のオーディオ入力機能を使用するには、WorkSpaces 内のローカルログオンアクセスが必要です。Windows WorkSpaces 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。ただし、WorkSpaces での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、オーディオ入力は WorkSpaces では機能しません。そのグループポリシー設定を削除すると、WorkSpaces の次回再起動後にオーディオ入力機能が有効になります。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 DCV 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 を参照してください。
- グループポリシーを使用して Windows の電源プランを [Balanced] (バランス) または [Power saver] (省電力) に設定すると、WorkSpaces がアイドル状態になると、WorkSpaces がスリープ状態になる場合があります。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 をアイドル状態のままにすると、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 WorkSpaces で開いているすべてのアプリケーションが閉じられます。
- DCV WorkSpaces では、「アクティブだが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する」は現在サポートされていません。DCV 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します。

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 Personal で Active Directory 管理ツールを設定する を参照してください。

内容

# DCV 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

DCV を使用しているときに WorkSpaces に固有のグループポリシー設定を使用するには、DCV 用のグループポリシー管理用テンプレートの `wsp.admx` ファイルと `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。ディレクトリ管理用の WorkSpaces 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、次の手順を実行します。

DCV 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 WorkSpace から、`wsp.admx` ディレクトリの `wsp.adml` および `C:\Program Files\Amazon\WSP` ファイルのコピーを作成します。
2. ディレクトリ管理 WorkSpaces 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 エクスプローラーを開き、アドレスバーに `\\example.com` のような組織の完全修飾ドメイン名 (FQDN) を入力します。
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 WorkSpaces 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) を開きます。

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**
>
> WorkSpaces をサポートするドメインが 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、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*#######*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、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
8. これで、この DCV グループポリシーオブジェクトを使用して、DCV を使用しているときに WorkSpaces 固有のグループポリシー設定を変更できます。

## DCV 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って、DCV を使用する Windows WorkSpaces を管理するには

1. DCV の最新の WorkSpaces グループポリシー管理用テンプレートが、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. 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します。詳細については、「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」を参照してください。

### DCV のプリンターサポートを設定する

デフォルトでは、WorkSpaces は基本的なリモート印刷を可能にします。印刷の互換性を確実にするため、ホスト側の汎用プリンタードライバーを使用するため、提供される印刷機能は限られています。

Windows クライアントの高度なリモート印刷 (DCV 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 WorkSpaces の場合、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. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Configure remote printing] 設定を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

- WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### DCV 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、WorkSpaces 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をサポートしています。Windows WorkSpaces の場合、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、クリップボードリダイレクトを許可する方向を設定したりできます。

Windows WorkSpaces のクリップボードリダイレクトを設定するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Configure clipboard redirection] 設定を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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

WorkSpaces でクリップボードのリダイレクトが有効になっていると、Microsoft Office アプリケーションから 890 KB よりも大きいコンテンツをコピーした場合に、アプリケーションが遅くなったり最大 5 秒応答しなくなったりすることがあります。

### DCV 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切断されると、アクティブな WorkSpaces クライアントセッションが切断されます。Windows と 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回復すればセッションを自動的に再接続するように試行します。デフォルト設定のセッション再起動タイムアウトは 20 分 (1,200 秒) ですが、ドメインのグループポリシー設定で制御される WorkSpaces では、この値の変更ができます。

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. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Enable/disable automatic reconnect] (自動再接続を有効/無効にする) 設定を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### DCV のビデオ入力リダイレクトを有効または無効にする

デフォルトでは、WorkSpaces はローカルカメラから取得されたデータのリダイレクトをサポートしています。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

Windows WorkSpaces 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

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。
   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

DCV 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

デフォルトでは、WorkSpaces では、ローカルマイクから取得されたデータのリダイレクトをサポートしています。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

Windows WorkSpaces 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

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

- WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### DCV 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

デフォルトでは、WorkSpaces はデータをローカルスピーカーにリダイレクトします。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

#### Windows WorkSpaces 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

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpace を再起動します。Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] の順に選択します。
   - 管理コマンドプロンプトで、**gpupdate /force** と入力します。

### DCV 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、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。

- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

Windows WorkSpaces のタイムゾーンのリダイレクトを無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。
   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。
6. WorkSpaces のタイムゾーンを目的のタイムゾーンに設定します。

WorkSpaces のタイムゾーンは静的になり、クライアントマシンのタイムゾーンは反映されなくなります。

DCV のセキュリティ設定を構成する

DCV 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 WorkSpaces では、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に追加または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、[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。

DCV のセキュリティ設定を構成するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [セキュリティ設定の構成] を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動するには、Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] 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。

DCV 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、以下の方法で拡張機能を使用するように WorkSpace 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 WorkSpaces では、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。

DCV の拡張機能を設定するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [拡張機能の設定] を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpace を再起動します。Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] 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。

DCV 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

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のサポートを有効化していません。セッション前認証とは、ユーザーが WorkSpaces 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いいます。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。

必要に応じグループポリシー設定を使用して、Windows WorkSpaces のセッション前認証およびセッション内認証を有効にします。セッション前認証は、EnableClientAuthenticationAPI アクションまたは enable-client-authentication AWS CLI コマンドを使用して AD Connector ディレクトリ設定でも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 WorkSpaces でスマートカードを使用できるようにするには、追加の手順が必要です。詳細については、「WorkSpaces Personal での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 WorkSpaces のスマートカードのリダイレクトを有効または無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces セッションの再開後に有効になります。グループポリシー設定の変更を適用するには、WorkSpaces を再起動します (Amazon WorkSpaces コンソールで WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) の順に選択します)。

## DCV 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 のセッション内認証に WebAuthn 認証システムを使用できます。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

DCV の WebAuthn (FIDO2) リダイレクトには、以下が必要です。

- DCV 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 WebAuthn リダイレクト拡張機能を実行している WorkSpaces 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 WorkSpaces の WebAuthn (FIDO2) リダイレクトを有効化/無効化する

必要に応じて、グループポリシー設定を使用することで、Windows WorkSpaces の WebAuthn 認証によるセッション内認証のサポートを有効化/無効化できます。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 WorkSpace 内でローカル認証を利用できるようになります。

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 や YubiKey のようなローカルにアタッチされたセキュリティデバイスなど、FIDO2 に準拠した認証システムを使用して、認証プロセスを完了できます。

#### Windows WorkSpaces の WebAuthn (FIDO2) リダイレクトを有効または無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [WebAuthn リダイレクトを有効/無効にする] 設定を開きます。
3. [WebAuthn 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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

#### Amazon DCV WebAuthn リダイレクト拡張機能をインストールする

WebAuthn を使用するには、機能が有効にされた後、ユーザーが 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。次のいずれかの方法があります。

- ブラウザでブラウザ拡張機能を有効にするように求めるプロンプトがユーザーに表示されます。

> **Note**
>
> これは 1 回限りのブラウザプロンプトです。DCV 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られます。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 ポリ

シーを使用して、WebAuthn 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、ユーザーのリダイレクト拡張機能を強制的にインストールできます。GPO ポリシーを有効にすると、ユーザーがサポートされているブラウザを起動したときに、インターネットアクセスを使って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 ウェブストアを使用して拡張機能を手動でインストールできます。

### WebAuthn リダイレクト拡張機能のネイティブメッセージングについて

Chrome および Edge ブラウザでの WebAuthn リダイレクトは、ブラウザ拡張機能とネイティブメッセージングホストを使用します。ネイティブメッセージングホストは、拡張機能とホストアプリケーション間の通信を許可するコンポーネントです。一般的な設定では、すべてのネイティブメッセージングホストはデフォルトでブラウザで許可されます。ただし、ネイティブメッセージングブロックリストを使用することを選択できます。* の値は、明示的に許可されない限り、すべてのネイティブメッセージングホストが拒否されることを意味します。この場合、許可リスト`com.dcv.webauthnredirection.nativemessagehost`で値を明示的に指定して、Amazon DCV WebAuthn Redirection ネイティブメッセージングホストを有効にする必要があります。

詳細については、ブラウザのガイダンスに従ってください。

- Google Chrome については、「ネイティブメッセージングが許可されているホスト」を参照してください。
- Microsoft Edge については、「ネイティブメッセージング」を参照してください。

### 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場合はドメインから一元的に、または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 管理用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 WorkSpaces 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. [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. [コンピューターの構成]、[管理用テンプレート]、[Microsoft Edge]、[拡張機能] の順に選択します。
9. [拡張機能の管理設定を構成する] を開いて、[有効] に設定します。
10. [拡張機能の管理設定を構成する] に以下を入力します。

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. [OK] を選択してください。
12. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

> **Note**
>
> 次の構成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 管理用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、「管理対象パソコンに Chrome ブラウザのポリシーを設定する」を参照してください。
2. ディレクトリ管理 WorkSpaces 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. [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. [コンピューターの構成]、[管理用テンプレート]、[Google Chrome]、[拡張機能] の順に選択します。
9. [拡張機能の管理設定を構成する] を開いて、[有効] に設定します。
10. [拡張機能の管理設定を構成する] に以下を入力します。

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. [OK] を選択してください。
12. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

> **Note**
>
> 次の構成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"}}
> ```

### DCV の WebRTC リダイレクトを有効または無効にする

WebRTC リダイレクトでは、WorkSpaces からローカルクライアントにオーディオおよびビデオ処理をオフロードすることでリアルタイム通信が強化されるため、パフォーマンスが向上し、レイテンシーが低減します。ただし、WebRTC リダイレクトに汎用性はなく、サードパーティーのアプリケーションベンダーが WorkSpaces との固有の統合を開発する必要があります。デフォルトで

は、WebRTC リダイレクトは WorkSpaces で有効になっていません。WebRTC リダイレクトを使用するには、以下を確認します。

- サードパーティーアプリケーションベンダーによる統合
- WorkSpaces 拡張機能が、グループポリシー設定を通じて有効になっていること
- WebRTC リダイレクトが有効になっていること
- WebRTC リダイレクトブラウザ拡張機能がインストールされ有効になっていること

> **Note**
>
> このリダイレクトは拡張機能として実装されるため、グループポリシー設定を使用して WorkSpaces 拡張機能のサポートを有効にする必要があります。拡張機能が無効になっている場合、WebRTC リダイレクトは機能しません。

### 要件

DCV の WebRTC リダイレクトには、以下が必要です。

- DCV ホストエージェントバージョン 2.0.0.1622 以降
- WorkSpaces クライアント
  - Windows 5.21.0 以降
  - ウェブクライアント
- Amazon DCV WebRTC リダイレクト拡張機能を実行している WorkSpaces 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 WorkSpaces の WebRTC リダイレクトを有効化/無効化する

必要に応じて、グループポリシー設定を使用して、Windows WorkSpaces の WebRTC リダイレクトのサポートを有効または無効にできます。この設定を無効にするか指定しない場合、WebRTC リダイレクトは無効になります。

この機能を有効にすると、Amazon WorkSpaces と統合されているウェブアプリケーションは、WebRTC API コールをローカルクライアントにリダイレクトできるようになります。

### Windows WorkSpaces の WebRTC リダイレクトを有効または無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Configure WebRTC Redirection] 設定を開きます。
3. [Configure WebRTC Redirection] ダイアログボックスで、[Enabled] または [Disabled] を選択します。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

## Amazon DCV WebRTC リダイレクト拡張機能をインストールする

WebRTC を使用するには、機能が有効にされた後、ユーザーが Amazon DCV WebRTC 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。次のいずれかの方法があります。

- ブラウザでブラウザ拡張機能を有効にするように求めるプロンプトがユーザーに表示されます。

> **Note**
>
> WebRTC リダイレクトを有効にすると、1 回限りのブラウザプロンプトとしてユーザーに通知が送られます。

- 以下の GPO ポリシーを使用して、ユーザーのリダイレクト拡張機能を強制的にインストールできます。GPO ポリシーを有効にすると、ユーザーがサポートされているブラウザを起動したときに、インターネットアクセスを使って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 ウェブストア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 WebRTC 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場合はドメインから一元的に、または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 管理用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 WorkSpaces 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. [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. [コンピューターの構成]、[管理用テンプレート]、[Microsoft Edge]、[拡張機能] の順に選択します。
9. [拡張機能の管理設定を構成する] を開いて、[有効] に設定します。
10. [拡張機能の管理設定を構成する] に以下を入力します。

```
{"kjbbkjjiecchbcdoollhgffghfjnbhef":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. [OK] を選択してください。
12. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

> **Note**
>
> 次の構成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。
>
> ```
> {"kjbbkjjiecchbcdoollhgffghfjnbhef":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

Google Chrome の場合

1. Google Chrome 管理用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、「管理対象パソコンに Chrome ブラウザのポリシーを設定する」を参照してください。
2. ディレクトリ管理 WorkSpaces 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. [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. [コンピューターの構成]、[管理用テンプレート]、[Google Chrome]、[拡張機能] の順に選択します。
9. [拡張機能の管理設定を構成する] を開いて、[有効] に設定します。
10. [拡張機能の管理設定を構成する] に以下を入力します。

```
{"diilpfplcnhehakckkpmcmibmhbingnd":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. [OK] を選択してください。
12. グループポリシー設定の変更は、WorkSpaces セッションの再開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 コンソールに移動し、WorkSpace を選択して WorkSpace を再起動します。次に、[アクション]、[WorkSpaces を再起動] の順に選択します。

> **Note**
>
> 次の構成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。
>
> ```
> {"diilpfplcnhehakckkpmcmibmhbingnd":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

### DCV の画面ロック時におけるセッションの切断を有効または無効にする

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には、WorkSpaces で有効になっている認証の種類に応じて、ユーザーはパスワードまたはスマートカードを使用して自分自身を認証できます。

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を使用して、Windows WorkSpaces の Windows ロック画面が検出された場合における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 WorkSpaces でスマートカードを使用できるようにするには、追加の手順が必要です。詳細については、「WorkSpaces Personal での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 WorkSpaces の画面ロックの場合のセッションの切断を有効または無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [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。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### DCV 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 WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

Windows WorkSpaces 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

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. 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。
3. Enable the AWS Indirect Display Driver ダイアログボックスで、Enabled または Disabled を選択します。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

    a. WorkSpace を再起動します (WorkSpaces コンソールで、WorkSpace を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### DCV の表示設定を構成する

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、さまざまな表示設定を構成できます。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 WorkSpaces では、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、および最大画質の値を設定できます。

Windows WorkSpaces の表示設定を構成するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [ディスプレイ設定の構成] を開きます。
3. [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。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します。Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] 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。

DCV 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、WorkSpaces は AWS 仮想ディスプレイ専用ドライバーの VSync 機能の使用をサポートしています。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

Windows WorkSpaces の VSync を有効または無効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. Virtual  AWS Display Only Driver 設定の Enable VSync 機能を開きます。

3. Virtual  AWS Display Only Driver ダイアログボックスの Enable VSync 機能で、Enabled または Disabled を選択します。
4. [OK] を選択してください。
5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、以下を実行します。

   a. 次のいずれかを実行して WorkSpace 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]、[WorkSpaces を再起動] の順に選択します。

      ii. オプション 2 — 管理コマンドプロンプトで、`gpupdate /force` と入力します。

   b. 設定を適用するために WorkSpace に再接続します。

   c. WorkSpace をもう一度再起動します。

### DCV のログ詳細度を設定する

デフォルトでは、DCV WorkSpaces のログ詳細度は [情報] に設定されています。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 WorkSpaces では、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 WorkSpaces のログ詳細度レベルを設定するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [ログ詳細度の設定] を開きます。
3. [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。
4. [OK] を選択してください。

5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpace を再起動します。Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] 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。

DCV のアイドル切断タイムアウトを設定する

WorkSpaces では、WorkSpace への接続中にユーザーの非アクティブ状態が所定の長さに達したら接続を解除するように設定できます。ユーザーアクティビティ入力の例は次のとおりです。

- キーボードイベント
- マウスイベント (カーソルの移動、スクロール、クリック)
- スタイラスイベント
- タッチイベント (タッチスクリーン、タブレットのタップ)
- ゲームパッドイベント
- ファイルストレージオペレーション (アップロード、ダウンロード、ディレクトリ作成、リスト項目)
- ウェブカメラストリーミング

オーディオ入力、オーディオ出力、ピクセルの変更は、ユーザーアクティビティにはなりません。

アイドル切断タイムアウトを有効にする場合、オプションで、アクティビティが発生しない限り、設定された時間内にセッションが切断されることをユーザーに通知できます。

デフォルトでは、アイドル切断タイムアウトは無効になっており、タイムアウト値は 0 分に設定され、通知は無効になっています。このポリシー設定を有効にすると、アイドル切断タイムアウトの値はデフォルトで 60 分、アイドル切断タイムアウト警告の値はデフォルトで 60 秒になります。Windows WorkSpaces では、グループポリシー設定を使用してこの機能を設定できます。

Windows WorkSpaces のアイドル切断タイムアウトを設定するには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Configure Idle Disconnect Timeout] 設定を開きます。

3. [Configure Idle Disconnect Timeout] ダイアログボックスで [Enabled]を選択し、切断タイムアウトの値 (分単位) と、オプションの警告タイマーの値 (秒単位) を設定します。
4. [適用]、[OK] の順に選択します。
5. グループポリシー設定の変更は、変更を適用するとすぐに有効になります。

### DCV のファイル転送を設定する

デフォルトでは、Amazon WorkSpaces のファイル転送機能は無効になっています。これを有効にすると、ユーザーはローカルコンピュータと WorkSpaces セッションの間でファイルをアップロードおよびダウンロードできます。ファイルは WorkSpaces セッションの [ストレージ] フォルダに保存されます。

Windows WorkSpaces のファイル転送を有効にするには

1. グループポリシー管理エディタで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Amazon]、[DCV] の順に選択します。
2. [Configure session storage] 設定を開きます。
3. [Configure session storage] ダイアログボックスで、[Enabled] を選択します。
4. (オプション) セッションストレージのフォルダを指定します (`c:/session-storage` など)。指定しない場合、セッションストレージのデフォルトフォルダはホームフォルダになります。
5. WorkSpace は、次のいずれかのファイル転送オプションを使用して設定できます。
   - 双方向ファイル転送を許可する場合は、`Download and Upload` を選択します。
   - ローカルコンピュータから WorkSpaces セッションへのファイルアップロードのみを許可する場合は、`Upload Only` を選択します。
   - WorkSpaces セッションからローカルコンピュータへのファイルダウンロードのみを許可する場合は、`Download Only` を選択します。
6. [OK] を選択してください。
7. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。
   - WorkSpace を再起動します。Amazon WorkSpaces コンソールで、WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] 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ときに Amazon WorkSpaces に固有のグループポリシー設定を使用するには、WorkSpaces で使用されている PCoIP エージェントのバージョン ( 32 ビットまたは 64 ビット ) に適したグループポリシー管理用テンプレートを追加する必要があります。

> **Note**
>
> 32 ビットと 64 ビットのエージェントの WorkSpaces が混在している場合は、32 ビットエージェント用のグループポリシー管理用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 ビットと 64 ビットの両方のエージェントに適用されます。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を使用するように切り替えることができます。

WorkSpaces に 32 ビットエージェントがあるかどうか、 64 ビットのエージェントがあるかどうかを調べるには

1. WorkSpaces にログインし、[表示]、[Ctrl + Alt + Delete で送信] 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] を選択することで、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が、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)

PCoIP プロトコルを 32 ビット PCoIP エージェントで使用するとき、WorkSpaces に固有のグループポリシー設定を使用するには、PCoIP 用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必要があります。ディレクトリの管理 WorkSpaces 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。

.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 WorkSpaces から、`pcoip.adm` ディレクトリの `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` ファイルのコピーを作成します。
2. ディレクトリ管理用の WorkSpaces 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 マシンアカウントが含まれている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. [New GPO] ダイアログボックスで、GPO のわかりやすい名前 (「WorkSpaces Machine Policies」など) を入力し、[Source Starter GPO] は [(none)] のままにします。[OK] を選択してください。
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。これで、この GPO を使用して、WorkSpaces に固有のグループポリシーの設定を変更できます。

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. ディレクトリ管理用の WorkSpaces 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 WorkSpaces GPO 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。
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. これで、この PCoIP セッション変数グループポリシーオブジェクトを使用して、PCoIP を使用しているときに Amazon WorkSpaces 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す。

> **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 プロトコルを使用しているときに WorkSpaces に固有のグループポリシー設定を使用するには、グループポリシー管理用テンプレート `PCoIP.admx` および PCoIP 用 `PCoIP.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。ディレクトリ管理用の WorkSpaces 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、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 WorkSpace から、`PCoIP.admx` ディレクトリの `PCoIP.adml` および `C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions` 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 WorkSpaces 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 エクスプローラーを開き、アドレスバーに `\\example.com` のような組織の完全修飾ドメイン名 (FQDN) を入力します。
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 WorkSpaces 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) を開きます。
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**
>
> WorkSpaces をサポートするドメインが 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、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########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. これで、この PCoIP セッション変数グループポリシーオブジェクトを使用して、PCoIP を使用しているときに WorkSpaces 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す。

> **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って、PCoIP を使用する Windows WorkSpaces を管理します。

### PCoIP のプリンタサポートを設定する

デフォルトでは、WorkSpaces は基本的なリモート印刷を可能にします。印刷の互換性を確実にするため、ホスト側の汎用プリンタードライバーを使用するため、提供される印刷機能は限られています。

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 WorkSpaces の場合、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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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] を選択してください。
6. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。
   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。グループポリシーの設定を使用して、この機能を有効にすることができます。有効にすると、WorkSpaces に接続するたびに、ローカルプリンターがデフォルトプリンターとして設定されます。

> **Note**
>
> ローカルプリンターのリダイレクトは Amazon Linux WorkSpaces ではご利用になれません。

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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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/ペースト) を有効または無効にする

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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有効 (WorkSpaces からローカルコンピュータ)
- クライアントからエージェントのみ有効 (ローカルコンピュータから WorkSpaces)
- 双方向で有効

5. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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

WorkSpaces でクリップボードのリダイレクトが有効になっていると、Microsoft Office アプリケーションから 890 KB よりも大きいコンテンツをコピーした場合に、アプリケーションが遅くなったり最大 5 秒応答しなくなったりすることがあります。

### 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切断されると、アクティブな WorkSpaces クライアントセッションが切断されます。Windows と 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回復すればセッションを自動的に再接続するように試行します。デフォルト設定のセッション再起動タイムアウトは 20 分ですが、ドメインのグループポリシー設定で制御される WorkSpaces では、この値の変更ができます。

#### 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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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 WorkSpaces では、ローカルマイクから取得されたデータのリダイレクトをサポートしています。Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、この機能を無効にすることができます。

> **Note**
>
> WorkSpaces での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、オーディオ入力は WorkSpaces では機能しません。そのグループポリシー設定を削除すると、WorkSpaces の次回再起動後にオーディオ入力機能が有効になります。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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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 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] を選択してください。

6. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

Windows WorkSpaces では必要に応じて、グループポリシーの設定を使用し、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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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] を選択してください。

6. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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. WorkSpaces のタイムゾーンを目的のタイムゾーンに設定します。

WorkSpaces のタイムゾーンは静的になり、クライアントマシンのタイムゾーンは反映されなくなります。

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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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] を選択してください。
7. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

### YubiKey U2F の USB リダイレクトを有効にする

> **Note**
>
> Amazon WorkSpaces は現在、YubiKey U2F に対してのみ 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. インストールしたPCoIP (32 ビット) 用の WorkSpaces グループポリシー管理用テンプレート、または PCoIP (64 ビット) 用の WorkSpaces グループポリシー管理用テンプレートが最新であることを確認します。
2. ディレクトリ管理 WorkSpaces 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 認可テーブルを入力 (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。YubiKey USB の値の詳細については、YubiKey USB ID Values を参照してください。

7. [USB 認可テーブルを入力 (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] を選択してください。
9. グループポリシー設定の変更は、WorkSpaces の次回のグループポリシーの更新後、および WorkSpaces 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、次のいずれかを実行します。

   - WorkSpaces を再起動します (Amazon WorkSpaces コンソールで、WorkSpaces を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

この設定が有効になると、USB デバイスのルール設定で制限されていない限り、サポートされているすべての USB デバイスが WorkSpaces にリダイレクトできるようになります。

## Kerberos チケットの最大ライフタイムを設定する

Windows WorkSpaces の [Remember Me] (情報を記憶する) 機能を無効にしていない場合、WorkSpaces ユーザーは WorkSpaces クライアントアプリケーションの [Remember Me] (情報を記憶する) または [Keep me logged in] (ログイン状態を保つ) チェックボックスを使用して、認証情報を保存することができます。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が実行中

であれば簡単に WorkSpaces に接続できます。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。

WorkSpaces で AD Connector ディレクトリを使用している場合は、Microsoft Windows ドキュメントの「チケットの最長有効期間」の手順に従って、グループポリシーを使用して WorkSpaces 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、WorkSpaces Personal でユーザーを対象とした WorkSpaces の自己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、デバイスオペレーティングシステム設定で HTTPS (ポート 443) トラフィック用に指定した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の構成」の手順に従って、グループポリシーを通じて Windows WorkSpaces のデバイスプロキシサーバー設定を構成できます。

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構成の詳細については、「Amazon WorkSpaces 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 macOS クライアントアプリケーションでのプロキシ設定の構成の詳細については、「Amazon WorkSpaces 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 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構成の詳細については、「Amazon WorkSpaces 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。

### 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) に対するプロキシサーバーの使用も、TLS の復号と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。

DCV WorkSpaces の場合、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 トラフィックに対する 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。

DCV 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 トラフィックに対する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 Web Access 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のプロキシサーバーの使用はお勧めしません。

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、プロキシを使用してもセキュリティは向上しません。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は設計されていないため、ストリーミングの品質と安定性に影響す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の増大を避けるため、プロキシサーバーを WorkSpace クライアントのできるだけ近く、できれば同じネットワーク内に配置してください。

## Amazon WorkSpaces で Zoom Meeting Media 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、Windows ベースの DCV および PCoIP WorkSpaces での最適化されたリアルタイム通信をサポートしています。クライアントとの直接通信によってビデオ通話はクラウドベースの仮想デスクトップを迂回できるため、ユーザーの WorkSpace 内で会議が行われていてもローカルのような Zoom エクスペリエンスを提供できます。

### DCV の Zoom Meeting Media プラグインを有効にする

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、以下の要件を満たし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
- WorkSpaces 内 — VDI 版 Zoom 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、「DCV 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、「DCV 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、Zoom が提供する 2 つのコンポーネントを Windows WorkSpaces にインストールします。詳細については、「Using Zoom for Amazon WorkSpaces」を参照してください。

1. WorkSpace に VDI 版 Zoom 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。
2. WorkSpace 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 以降をインストールします。
3. VDI 版 Zoom クライアントで VDI プラグインのステータスが [接続済み] として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、「How to confirm Amazon WorkSpaces optimization」を参照してください。

### PCoIP の Zoom Meeting Media プラグインを有効にする

Active Directory への管理者アクセス許可を持つユーザーは、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

内のすべての Windows WorkSpaces 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、以下の要件を満たし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
- WorkSpaces 内 — VDI 版 Zoom Meeting クライアントバージョン 5.12.6 以降

### Windows WorkSpaces ホストにレジストリキーを作成する

次の手順に従って、Windows WorkSpaces ホストにレジストリキーを作成します。Windows WorkSpaces で Zoom を使用するには、レジストリキーが必要です。

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 をクリックし、[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 WorkSpaces 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。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 WorkSpaces での Zoom のトラブルシューティングを行うには、以下のアクションを実行してください。

- レジストリキーがアクティブ化され、正しく適用されていることを確認します。

- 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、 サポート センター サポート を使用して にお問い合わせください。

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>
```

# WorkSpaces Personal で Amazon Linux 2 WorkSpaces を管理する

RPM Package Manager (RPM) を必要とするワークロードの場合は、Red Hat Enterprise Linux または Rocky Linux を使用することをお勧めします。Amazon Linux 2 では、Firefox や glibc など、必要な一部のアプリケーションやライブラリの最新バージョンが提供されない場合があります。

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、Ansible を使用できます。

> **Note**
>
> ローカルプリンターのリダイレクトは Amazon Linux WorkSpaces ではご利用になれません。

## Amazon Linux WorkSpaces で DCV の動作を制御する

DCV 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**
>
> - 誤った変更またはサポートされていない変更を `wsp.conf` ファイルに加えた場合、ポリシー変更は WorkSpaces に新たに確立された接続に適用されない場合があります。
> - 現在、Amazon Linux WorkSpaces DCV バンドルには、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。

## DCV Amazon Linux WorkSpaces のクリップボードリダイレクトを設定する

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。必要に応じて、DCV 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、WorkSpace を切断して再接続したときに有効になります。

DCV Amazon Linux WorkSpaces のクリップボードリダイレクトを設定するには

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。

## DCV Amazon Linux WorkSpaces 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

デフォルトでは、WorkSpaces はオーディオインリダイレクトをサポートしています。必要に応じて、DCV 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、WorkSpace を切断して再接続したときに有効になります。

DCV Amazon Linux WorkSpaces 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

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

## DCV Amazon Linux WorkSpaces のタイムゾーンのリダイレクトを有効または無効にする

デフォルトでは、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

必要に応じて、DCV 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、WorkSpace を切断して再接続した後に有効になります。

DCV Amazon Linux WorkSpaces のタイムゾーンのリダイレクトを有効または無効にするには

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 WorkSpaces で PCoIP エージェントの動作を制御する

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、WorkSpace を再起動することをお勧めします。

> **Note**
>
> pcoip-agent.conf ファイルに正しくない変更またはサポートされていない変更を加えた場合、WorkSpace が動作しなくなる可能性があります。WorkSpace が動作しなくなった場合は、SSH を使用して WorkSpace に接続して変更をロールバックするか、WorkSpace を再構築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。利用可能な設定の一覧については、Amazon Linux WorkSpace のターミナルから man pcoip-agent.conf を実行します。

## PCoIP Amazon Linux WorkSpaces のクリップボードリダイレクトを設定する

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。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、WorkSpace を再起動したときに有効になります。

PCoIP Amazon Linux WorkSpaces のクリップボードリダイレクトを設定するには

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 WorkSpaces 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、WorkSpaces はオーディオインリダイレクトをサポートしています。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、WorkSpace を再起動したときに有効になります。

PCoIP Amazon Linux WorkSpaces のオーディオ入力リダイレクトを有効化/無効化するには

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 WorkSpaces のタイムゾーンのリダイレクトを有効化/無効化する

デフォルトでは、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

Linux WorkSpaces のために必要な場合は、PCoIP エージェントの設定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、WorkSpace を再起動したときに有効になります。

PCoIP Amazon Linux WorkSpaces のタイムゾーンのリダイレクトを有効化/無効化するには

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、割り当て済みユーザーおよびドメイン管理者グループのアカウントのみが SSH を使用して Amazon Linux WorkSpaces 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。

```
[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、WorkSpaces Personal で Linux WorkSpaces の SSH 接続を有効にする を参照してください。

## Amazon Linux WorkSpaces のデフォルトシェルを上書きする

Linux WorkSpaces のデフォルトシェルを上書きするには、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、WorkSpace を再起動するか (切断だけでなく) WorkSpace からログアウトし、再度ログインして変更を有効に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 がインターネットにアクセスできるか、このリポジトリおよびメイン Amazon Linux リポジトリへの仮想プライベートクラウド (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、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

### Linux WorkSpaces での認証にスマートカードを使用する

Linux WorkSpaces DCV バンドルでは、認証に Common Access Card (CAC) および Personal Identity Verification (PIV) スマートカードを使用できます。詳細については、「WorkSpaces Personal での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、デバイスオペレーティングシステム設定で HTTPS (ポート 443) トラフィック用に指定した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の構成」の手順に従って、グループポリシーを通じて Linux WorkSpaces のデバイスプロキシサーバー設定を構成できます。

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構成の詳細については、「Amazon WorkSpaces 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 macOS クライアントアプリケーションでのプロキシ設定の構成の詳細については、「Amazon WorkSpaces 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 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構成の詳細については、「Amazon WorkSpaces 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。

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) に対するプロキシサーバーの使用も、TLS の復号と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。

DCV WorkSpaces の場合、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 トラフィックに対する 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。

DCV 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 トラフィックに対する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 Web Access 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のプロキシサーバーの使用はお勧めしません。

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、プロキシを使用してもセキュリティは向上しません。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は設計されていないため、ストリーミングの品質と安定性に影響す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の増大を避けるため、プロキシサーバーを WorkSpace クライアントのできるだけ近く、できれば同じネットワーク内に配置してください。

## WorkSpaces Personal で Ubuntu WorkSpaces を管理する

Ubuntu WorkSpaces バンドルには、Canonical からの Ubuntu Pro のサブスクリプションが含まれています。Windows や Amazon Linux WorkSpaces と同様に、Ubuntu WorkSpaces はドメイン結合されているため、Active Directory ユーザーとグループを使用して以下を実行できます。

- Ubuntu WorkSpaces を管理する
- ユーザーにこれらの WorkSpaces へのアクセスを許可する

AdSys を使用することで、グループポリシーで Ubuntu WorkSpaces を管理できます。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 WorkSpaces で DCV の動作を制御する

DCV 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**
>
> 誤った変更またはサポートされていない変更を加えた場合、WorkSpace に新たに確立された接続に wsp.conf ポリシーが適用されない場合があります。

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。

## Ubuntu WorkSpaces のクリップボードのリダイレクトの有効化または無効化

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Ubuntu WorkSpaces のクリップボードのリダイレクトを有効化または無効化するには

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 WorkSpaces のオーディオインリダイレクトの有効化または無効化

デフォルトでは、WorkSpaces はオーディオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Ubuntu WorkSpaces のオーディオインリダイレクトを有効または無効にするには

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 WorkSpaces のビデオインリダイレクトの有効化または無効化

デフォルトでは、WorkSpaces はビデオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Ubuntu WorkSpaces のビデオインリダイレクトを有効化または無効化するには

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 WorkSpaces のタイムゾーンのリダイレクトの有効化または無効化

デフォルトでは、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

必要に応じて、DCV 設定ファイルを使用してこの機能を設定します。

Ubuntu WorkSpaces のタイムゾーンのリダイレクトを有効または無効にするには

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 WorkSpaces のプリンターリダイレクトの有効化または無効化

デフォルトでは、WorkSpaces はプリンターリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Ubuntu WorkSpaces のプリンターリダイレクトを有効化または無効化するには

1. 次のコマンドを使用して、昇格された権限を持つ工ディタで 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

## DCV の画面ロック時におけるセッションの切断を有効または無効にする

画面ロック時におけるセッションの切断を有効にすると、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ます。WorkSpaces クライアントから再接続するには、WorkSpaces で有効になっている認証の種類に応じて、ユーザーはパスワードまたはスマートカードを使用して自分自身を認証できます。

デフォルトでは、WorkSpaces は画面ロックによる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、DCV 設定ファイルを使用してこの機能を有効にします。

Ubuntu WorkSpaces の画面ロック時におけるセッションの切断を有効または無効にするには

1. 次のコマンドを使用して、昇格された権限を持つ工ディタで 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、割り当て済みユーザーおよびドメイン管理者グループのアカウントのみが SSH を使用して Ubuntu WorkSpaces に接続できます。SSH を使用して他のユーザーやアカウントが Ubuntu WorkSpaces に接続できるようにするには、Active Directory で Ubuntu 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。

```
[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。

```
[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際にドメイン名を追加する必要はなく、パスワード認証はデフォルトで無効になっています。SSH 経由で接続するには、Ubuntu WorkSpace の `$HOME/.ssh/authorized_keys` に SSH パブリックキーを追加するか、`/etc/ssh/sshd_config` を編集して `yes` に PasswordAuthentication を設定する必要があります。SSH 接続の有効化の詳細については、「Linux WorkSpace で SSH 接続を有効化する」を参照してください。

## Ubuntu WorkSpace のデフォルトシェルを無効にする

Ubuntu WorkSpace のデフォルトシェルを無効にするには、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、WorkSpace を再起動するか (切断だけでなく) WorkSpace からログアウトし、再度ログインして変更を有効に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、デバイスオペレーティングシステム設定で HTTPS (ポート 443) トラフィック用に指定した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の構成」の手順に従って、グループポリシーを通じて Ubuntu WorkSpaces のデバイスプロキシサーバー設定を構成できます。

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構成の詳細については、「Amazon WorkSpaces 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 macOS クライアントアプリケーションでのプロキシ設定の構成の詳細については、「Amazon WorkSpaces 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 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構成の詳細については、「Amazon WorkSpaces 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。

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) に対するプロキシサーバーの使用も、TLS の復号と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。

DCV WorkSpaces の場合、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 トラフィックに対する 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。

DCV 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 トラフィックに対する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 Web Access 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のプロキシサーバーの使用はお勧めしません。

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、プロキシを使用してもセキュリティは向上しません。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は設計されていないため、ストリーミングの品質と安定性に影響す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の増大を避けるため、プロキシサーバーを WorkSpace クライアントのできるだけ近く、できれば同じネットワーク内に配置してください。

## Rocky Linux WorkSpaces を管理する

Ansible などの設定および管理ソリューションを使用して、Rocky Linux WorkSpaces を管理できます。 https://www.ansible.com/

> **Note**
>
> Rocky Linux ソフトウェアに含まれる著作権、商標、またはその他の所有権または機密性の通知を削除、変更、または隠すことはできません。

### Rocky Linux WorkSpaces で DCV の動作を制御する

DCV 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。ポリシーをデプロイして変更を適用するには、Rocky 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**
>
> 誤った変更またはサポートされていない変更を加えた場合、WorkSpace に新たに確立された接続に `wsp.conf` ポリシーが適用されない場合があります。

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。

## Rocky Linux WorkSpaces 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

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Rocky Linux WorkSpaces 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

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。

## Rocky Linux WorkSpaces 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

デフォルトでは、WorkSpaces はオーディオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Rocky Linux WorkSpaces 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

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

## Rocky Linux WorkSpaces のビデオ入力リダイレクトを有効または無効にする

デフォルトでは、WorkSpaces はビデオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Rocky Linux WorkSpaces 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

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

## Rocky Linux WorkSpaces のタイムゾーンリダイレクトを有効または無効にする

デフォルトでは、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

必要に応じて、DCV 設定ファイルを使用してこの機能を設定します。

Rocky Linux WorkSpaces 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

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

## Rocky Linux WorkSpaces のプリンターリダイレクトを有効または無効にする

デフォルトでは、WorkSpaces はプリンターリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Rocky Linux WorkSpaces 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

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

## DCV の画面ロック時におけるセッションの切断を有効または無効にする

画面ロック時におけるセッションの切断を有効にすると、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ます。WorkSpaces クライアントから再接続するには、WorkSpaces で有効になっている認証の種類に応じて、ユーザーはパスワードまたはスマートカードを使用して自分自身を認証できます。

デフォルトでは、WorkSpaces は画面ロックによる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、DCV 設定ファイルを使用してこの機能を有効にします。

Rocky Linux WorkSpaces 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

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)

## Rocky 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 を使用して Rocky Linux WorkSpaces に接続できます。他のユーザーやアカウントが SSH を使用して Rocky Linux WorkSpaces に接続できるようにするには、Active Directory で Rocky 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。

```
[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
```

Rocky Linux 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、デフォルトでパスワード認証は無効になっています。SSH 経由で接続するには、SSH パブリックキーを Rocky Linux WorkSpace `$HOME/.ssh/authorized_keys`の に追加するか、 を編集`/etc/ssh/sshd_config`して PasswordAuthentication を に設定する必要がありま`yes`す。SSH 接続の有効化の詳細については、「Linux WorkSpace で SSH 接続を有効化する」を参照してください。

### Rocky Linux WorkSpaces のデフォルトシェルを上書きする

Rocky Linux WorkSpaces のデフォルトシェルを上書きするには、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、WorkSpace を再起動するか (切断だけでなく) WorkSpace からログアウトし、再度ログインして変更を有効にする必要があります。

## Red Hat Enterprise Linux WorkSpaces の管理

Windows および Amazon Linux WorkSpaces と同様に、Red Hat Enterprise Linux WorkSpaces はドメイン結合されているため、Active Directory ユーザーとグループを使用して以下を実行できます。

- Red Hat Enterprise Linux WorkSpaces を管理する
- ユーザーにこれらの WorkSpaces へのアクセスを許可する

ADsys を使用することで、グループポリシーで Red Hat Enterprise Linux WorkSpaces を管理できます。詳細については、「Red Hat Enterprise Linux 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。

## Red Hat Enterprise Linux WorkSpaces で DCV の動作を制御する

DCV 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、Red Hat Enterprise 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**
>
> 誤った変更またはサポートされていない変更を加えた場合、WorkSpace に新たに確立された接続に `wsp.conf` ポリシーが適用されない場合があります。

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。

## Red Hat Enterprise Linux WorkSpaces の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

デフォルトでは、WorkSpaces はクリップボードのリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Red Hat Enterprise Linux WorkSpaces の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. 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。

## Red Hat Enterprise Linux WorkSpaces 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

デフォルトでは、WorkSpaces はオーディオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Red Hat Enterprise Linux WorkSpaces 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

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

## Red Hat Enterprise Linux WorkSpaces のビデオ入力リダイレクトを有効または無効にする

デフォルトでは、WorkSpaces はビデオインリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Red Hat Enterprise Linux WorkSpaces 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

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

## Red Hat Enterprise Linux WorkSpaces のタイムゾーンのリダイレクトを有効または無効にする

デフォルトでは、WorkSpaces 内の時間は、WorkSpaces 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反映するように設定されます。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)。
- WorkSpaces で、特定のタイムゾーン内の特定の時刻に実行するタスクをスケジュールした。
- よく出張するユーザーが、一貫性と個人設定のため WorkSpaces を 1 つのタイムゾーンにまとめておきたいと考えている。

必要に応じて、DCV 設定ファイルを使用してこの機能を設定します。

Red Hat Enterprise Linux WorkSpaces のタイムゾーンのリダイレクトを有効または無効にするには

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

## Red Hat Enterprise Linux WorkSpaces のプリンターリダイレクトを有効または無効にする

デフォルトでは、WorkSpaces はプリンターリダイレクトをサポートしています。必要に応じて、DCV 設定ファイルを使用してこの機能を無効にします。

Red Hat Enterprise Linux WorkSpaces 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

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

## DCV の画面ロック時におけるセッションの切断を有効または無効にする

画面ロック時におけるセッションの切断を有効にすると、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ます。WorkSpaces クライアントから再接続するに

は、WorkSpaces で有効になっている認証の種類に応じて、ユーザーはパスワードまたはスマートカードを使用して自分自身を認証できます。

デフォルトでは、WorkSpaces は画面ロックによる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、DCV 設定ファイルを使用してこの機能を有効にします。

Red Hat Enterprise Linux WorkSpaces の画面ロック時におけるセッションの切断を有効または無効にするには

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)

## Red Hat Enterprise Linux WorkSpaces 管理者に SSH アクセスを付与する

デフォルトでは、割り当て済みユーザーおよびドメイン管理者グループのアカウントのみが SSH を使用して Red Hat Enterprise Linux WorkSpaces に接続できます。SSH を使用して他のユーザーやアカウントが Red Hat Enterprise Linux WorkSpaces に接続できるようにするには、Active Directory で Red Hat Enterprise 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。

```
[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 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。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 次の行を追加します。

```
+:(Linux_WorkSpaces_Admins):ALL
```

Red Hat Enterprise Linux WorkSpaces では、SSH 接続のユーザー名を指定する際にドメイン名を追加する必要はなく、パスワード認証はデフォルトで無効になっています。SSH 経由で接続するには、Red Hat Enterprise Linux WorkSpace の `$HOME/.ssh/authorized_keys` に SSH パブリックキーを追加するか、`/etc/ssh/sshd_config` を編集して PasswordAuthentication を `yes` に設定する必要があります。SSH 接続の有効化の詳細については、「Linux WorkSpace で SSH 接続を有効化する」を参照してください。

## Red Hat Enterprise Linux WorkSpaces のデフォルトシェルを上書きする

Red Hat Enterprise Linux WorkSpaces のデフォルトシェルを上書きするには、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、WorkSpace を再起動するか (切断だけでなく) WorkSpace からログアウトし、再度ログインして変更を有効にする必要があります。

## WorkSpaces Personal でリアルタイム通信用に WorkSpaces を最適化する

Amazon WorkSpaces には、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デプロイを円滑化するさまざまな手法が用意されています。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が不要で、WorkSpaces で標準機能としてシームレスに使用できます。ただし、リアルタイムのコミュニケーション要素、特に 1 対 1 の通話と集合的なグループ会議は、この規則の例外となるため注意してください。このような機能を適切に組み込むには、しばしば、WorkSpaces のデプロイプロセス中に目的達成に特化した重点的な取り組みと計画が求められます。

Amazon WorkSpaces での 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、3 つの異なるリアルタイム通信 (RTC) 設定モードを選択できます。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 WorkSpaces 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 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 アプリケーションがリモート WorkSpace で実行され、直接通信のためにメディアフレームワークはサポートされるクライアントにオフロードされます。以下の UC アプリケーションは、Amazon WorkSpaces でこのアプローチを使用しています。

- Zoom Meetings
- Cisco Webex Meetings

メディア最適化 RTC モードが機能するには、UC アプリケーションベンダーは、DCV 拡張機能 SDK などの入手可能な Software Development Kits (SDK) のいずれかを使用して、WorkSpaces との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、未変更の UC アプリケーションが WorkSpace 上で実行され、オーディオとビデオのトラフィックが DCV を経由してクライアントデバイスに送られます。マイクからのローカルオーディオとウェブカメラからのビデオストリームは、WorkSpace にリダイレクトされ、UC アプリケーションで使用されます。このモードは幅広いアプリケーション互換性を備えており、UC アプリケーションをリモート WorkSpace 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、ユーザー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。

- Amazon WorkSpaces 向けの Amazon Connect の最適化
- 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。この構成により、ユーザーがデスクトップクライアントから WorkSpace に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 |
| 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 | | |

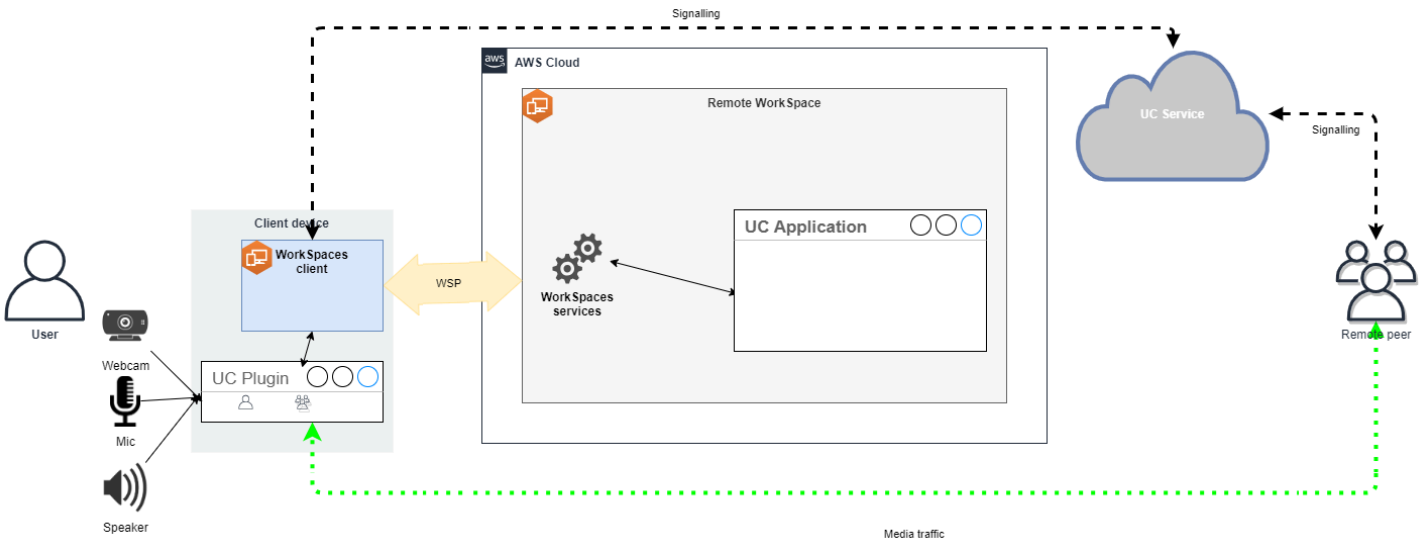
| 機能 | 直接 RTC | メディア最適化 RTC | セッション中最適化 RTC |
| --- | --- | --- | --- |
| オーディオ/ビデオクリップ/メッセージング | 該当しない | 良好 | = ベスト |
| ファイル共有 | 該当しない | UC アプリケーションによって異なる | = ベスト |
| 画面の共有と制御 | 該当しない | UC アプリケーションによって異なる | = ベスト |
| ウェビナー/イベントのブロードキャスト | 該当しない | 良好 | = ベスト |

## 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 やカスタマイズされたプライベートバージョンなどの公開オプションが含まれています。SDK によって、WorkSpace 内で動作する UC 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間で制御チャネルが確立されます。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 モードでは以下のアプリケーションをサポートしています。

- Zoom Meetings (PCoIP および DCV WorkSpaces)
- Cisco Webex Meetings (DCV WorkSpaces のみ)

リストに含まれていないアプリケーションを使用する場合は、アプリケーションベンダーに連絡し、WorkSpaces メディア最適化 RTC のサポートをリクエストすることをお勧めします。このプロセスをより迅速に行うには、aws-av-offloading@amazon.com にお問い合わせください。

メディア最適化 RTC モードにすると通話パフォーマンスが向上し、WorkSpace リソースの使用率が最小限に抑えられますが、一定の制限があります。

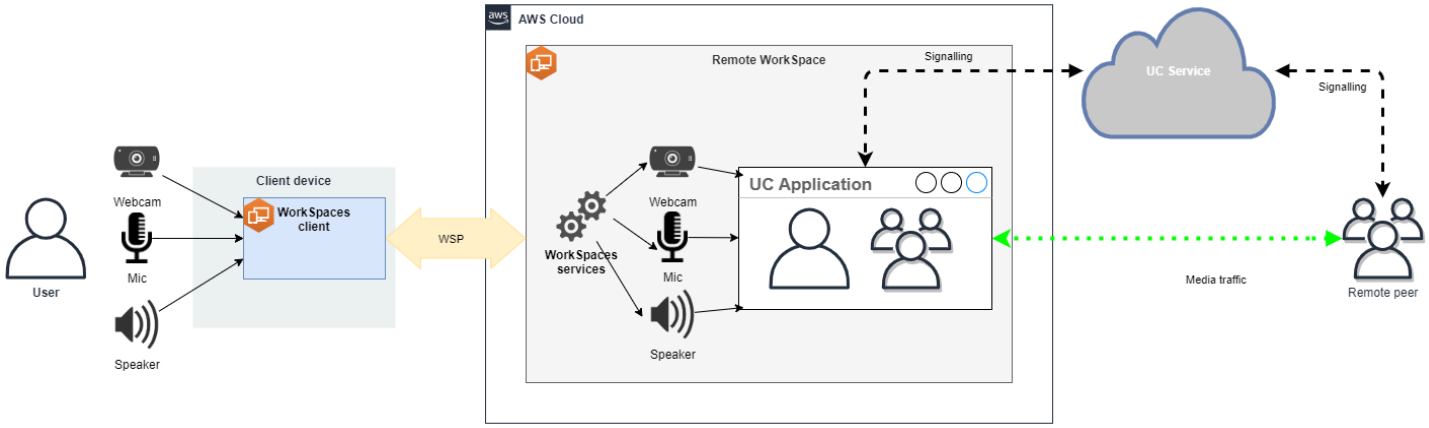
- UC クライアント拡張機能をクライアントデバイスにインストールする必要があります。
- UC クライアント拡張機能は、独立した管理と更新が必要です。
- UC クライアント拡張機能は、モバイルプラットフォームやウェブクライアントなど、特定のクライアントプラットフォームでは使用できない場合があります。
- このモードでは、画面共有の動作が異なる場合があるなど、UC アプリケーションの機能の一部が制限されることがあります。
- クライアント側拡張機能の使用は、Bring-Your-Own-Device (BYOD) や共有キオスクなどのシナリオには適さない場合があります。

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

セッション中最適化 RTC モードでは、何も変更を行わなくとも UC アプリケーションが WorkSpace 上で動作し、ローカルのようなエクスペリエンスを提供します。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、DCV 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 (DCV と PCoIP WorkSpaces の両方) とウェブカメラ (DCV WorkSpaces のみ) の信号がキャプチャされ、WorkSpace にリダイレクトされて、シームレスに UC アプリケーションに渡されます。

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。




DCV は、リモート RTC モードのパフォーマンスを高め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 WorkSpaces のサイズを適切に設定することが重要です。リモート WorkSpace 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すか、それを上回る必要があります。次の表は、一般的な UC アプリケーションをビデオ通話や音声通話に使用する場合の WorkSpaces の最小サポート設定と推奨設定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 | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 参照資料 |
| 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、3 GB メモリ)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 GB メモリ) | Performance (2 vCPU、8 GB メモリ) | • PowerPro (8 vCPU、3 GB メモリ)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 GB メモリ) | Microsoft Teams のハードウェア要件 |

| | | | 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 | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 参照資料 |
| 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、3 GB メモリ)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 GB メモリ) | Performance (2 vCPU、8 GB メモリ) | • PowerPro (8 vCPU、3 GB メモリ)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 GB メモリ) | Zoom システム要件: Windows、macOS、Linux |

| | | | 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 | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 最低限のサポート対象 WorkSpace | 推奨 WorkSpace | 参照資料 |
| 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)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 GB メモリ) | Performance (2 vCPU、8 GB メモリ) | • PowerPro (8 vCPU、32 GB メモリ)<br>• GeneralPurpose.4xlarge (16vCPU 4 GB メモリ)<br>• GeneralPurpose.8xlarge (32vCPU 28 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。GPU 以外の WorkSpaces では、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同時に CPU 上で実行されます。したがって、ビデオストリーミングやビデオ通話に定期的に参加しているユーザーには、PowerPro 以上の設定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。その結果、GPU 以外の WorkSpaces で、画面共有はより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 DCV に活用する

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 DCV に活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。

### WorkSpaces 用の UC アプリケーションの設定

背景ぼかし、仮想背景、リアクション、ライブイベントのホスティングなど、強化されたビデオ処理機能を使用する場合は、最適なパフォーマンスを実現するために GPU 対応の WorkSpace 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 WorkSpaces の CPU 使用率を低減させるために、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。

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 は本質的に、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 WorkSpaces 管理ガイド」の「DCV のビデオ入力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。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「ウェブカメラおよび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

ビデオ会議に Power、PowerPro、GeneralPurpose.4xlarge,または GeneralPurpose.8xlarge WorkSpaces を使用するユーザーには、リダイレクトされた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。PowerPro、GeneralPurpose.4xlarge,または GeneralPurpose.8xlarge,推奨される最大解像度は幅 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

WorkSpaces は 7.1 の高音質オーディオを WorkSpaces からクライアントに配信するようにデフォルトで設定されており、優れた音楽再生品質が保証されています。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
```

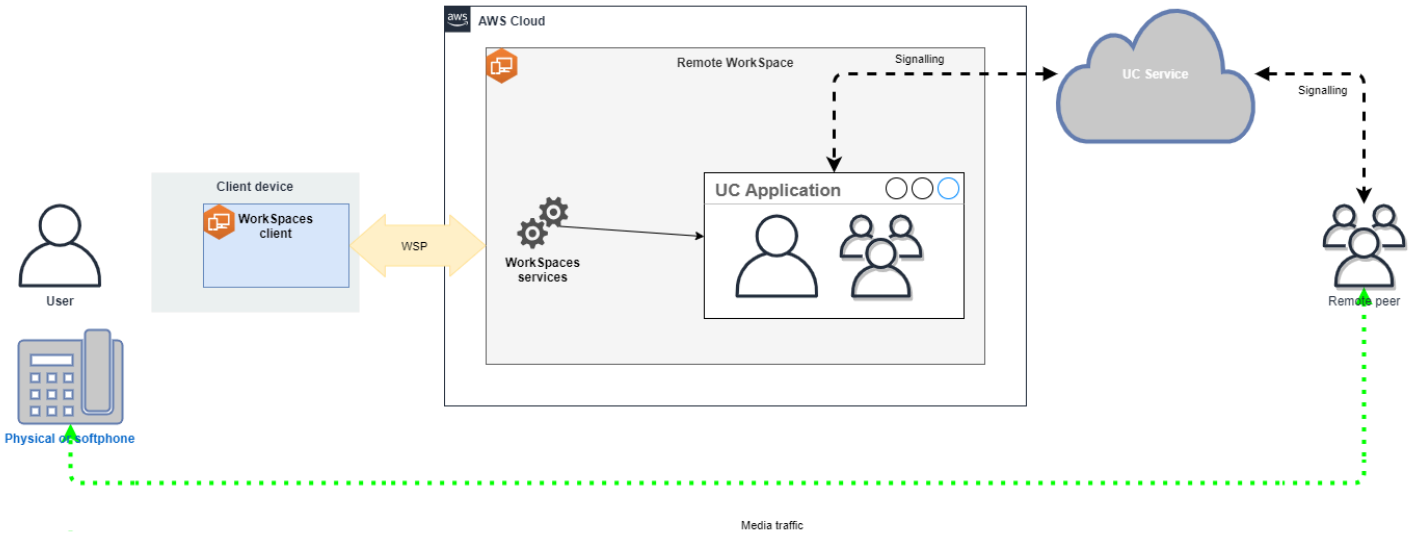
3. `default-profile` と言う名前の文字列値の名前を作成し、`voice` に設定します。

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

直接 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り、WorkSpaces の設定を変更する必要はありません。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:
  - Amazon WorkSpaces 向けの Amazon Connect の最適化
- Google Meet:
  - Use a phone for audio in a video meeting

# WorkSpaces Personal 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。

WorkSpaces が休止をサポートしている場合、デスクトップの状態は WorkSpace のルートボリュームに保存されます。WorkSpace は、ユーザーがログインすると再開されます。開いているすべてのドキュメントと実行中のプログラムは、休止をサポートするすべての WorkSpaces オペレーティングシステムで保存状態に戻ります。

AutoStop Graphics.g4dn、GraphicsPro.g4dn,Graphics、GraphicsPro、および GeneralPurpose.4xlarge または GeneralPurpose.8xlarge は休止をサポートしていないため、停止時にデータとプログラムの状態を保持できません。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/v2/home「https://www.com」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。

を使用して WorkSpace の実行モードを変更するには AWS CLI

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/v2/home://www.com」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。

AutoStop WorkSpace を開始するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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、「WorkSpaces Personal で WorkSpace を削除する」を参照してください。

を使用して AutoStop WorkSpace を停止および開始するには AWS CLI

stop-workspaces コマンドと start-workspaces コマンドを使用します。

## WorkSpaces Personal でアプリケーションを管理する

WorkSpace 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 コンソールに表示されます。

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を表示するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. 左のナビゲーションペインの [WorkSpaces] を選択します。
3. WorkSpace を選択したら、[詳細の表示] を選択します。
4. [アプリケーション] の下に、この WorkSpace に関連付けられているアプリケーションの一覧が、インストールのステータスと共に表示されます。

WorkSpace のアプリケーションバンドルは、次の方法で更新できます。

- WorkSpace 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 にアプリケーションバンドルをインストールし、別のアプリケーションバンドルセットをアンインストールする

Note

- アプリケーションバンドルを更新するには、WorkSpace のステータスが AVAILABLE または STOPPED である必要があります。
- [アプリケーションの管理] は Windows WorkSpaces でのみ使用できます。
- [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

[アプリケーションの管理] では、WorkSpaces で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。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
- Microsoft Visual Studio Professional 2022
- Microsoft Visual Studio Enterprise 2022

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) | Microsoft Visual Studio Professional / Enterprise 2022 |
|---|---|---|---|---|---|---|
| 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 | 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 | サポートされていません |
| 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 | 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 | 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 | インストール/アンインストール |

**Important**

- Microsoft Office/Visio/Project は、同じエディションとする必要があります。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。
- Microsoft Office/Visio/Project は同じバージョンとする必要があります。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、および GraphicsPro WorkSpaces バンドルではサポートされていません。
- Value、Standard、Graphics、および GraphicsPro WorkSpaces バンドルは、Visual Studio 2022 Enterprise/Professional ではサポートされていません。Performance バンドルは、リソースの消費量が少ない Visual Studio ワークロードに使用できます。ただし、最善の結果を得るには、クアッドコア以上のバンドルタイプで Visual Studio を使用することをお勧めします。バンドルタイプ Power、PowerPro、汎用.4xlarge、汎用.8xlarge、Graphics.g4dn、GraphicsPro.g4dn はこの要件を満たしています。詳細については、「Visual Studio 2022 製品ファミリのシステム要件」を参照してください。
- WorkSpaces から Microsoft Office 2016 用の Plus アプリケーションバンドルをアンインストールすると、その Amazon WorkSpaces バンドルの一部として含まれていた Trend Micro のソリューションを利用できなくなります。Amazon WorkSpaces で Trend Micro のソリューションを引き続き使用したい場合は、AWS Marketplace 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。
- アプリケーションの管理を通じてインストール/アンインストールされたアプリケーションを含む、WorkSpaces のカスタムイメージを作成できます。
- 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、WorkSpaces インターネット接続をディレクトリレベルで有効にする必要があります。

## WorkSpace のアプリケーションバンドルを更新する

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces] を選択します。

3. WorkSpace を選択し、[アクション]、[アプリケーションの管理] の順に選択します。
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 WorkSpace 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。
5. この WorkSpace でアプリケーションバンドルをインストールするには:

   a. この WorkSpace 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、[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 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には:

   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、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 WorkSpaces に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/v2/home で WorkSpaces コンソールを開きます。

b. ナビゲーションペインで [WorkSpaces] を選択します。[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。
   - 使用可能/停止中 – アプリケーションバンドルの更新が完了し、WorkSpace は元の状態に戻っています。

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、[詳細を表示] 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**
>
> [アプリケーションの管理] を通じて新しくインストールしたアプリケーションバンドルがライセンス認証されていないことにユーザーが気付いた場合は、WorkSpace を手動で再起動できます。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。

## WorkSpace で Microsoft Visual Studio 2022 ワークロードを更新する

デフォルトでは、Microsoft Visual Studio 2022 は次のワークロードとともにインストールされ、18 GB のハードディスク容量が必要となります。

- Visual Studio コアエディタ
- Azure 開発
- データストレージと処理
- .NET デスクトップ開発
- NET マルチプラットフォームアプリケーション UI 開発
- ASP.NET およびウェブ開発
- Node.js 開発

ユーザーはワークロードや個々のコンポーネントを柔軟に追加または削除できるため、特定の要件に合わせてアプリケーションを調整できます。追加のワークロードをインストールするには、より多くのディスク領域が必要になることに注意してください。ワークロード設定の詳細については、「Visual Studio のワークロード、コンポーネント、および言語パックを変更する」を参照してください。

## [アプリケーションの管理] を使用して変更された WorkSpaces の管理

WorkSpaces 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した後、次のアクションは既存の設定に影響を与える可能性があります。

- 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 の完全な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、「WorkSpaces の復元」を参照してください。[アプリケーションの管理] を使用して変更した WorkSpaces を復元する前に、少なくとも 12 時間待機してください。[アプリケーションの管理] を使用して変更された WorkSpaces を、次の完全なスナップショットの前に復元すると、次の結果になります。
  - [アプリケーションの管理] ワークフローを使用して WorkSpaces にインストールされたアプリケーションバンドルは WorkSpaces から削除されますが、ライセンスは引き続きアクティブ化され、それらのアプリケーションに対して WorkSpaces の料金が発生します。これらのアプリケーションバンドルを WorkSpaces に戻すには、[アプリケーションの管理] 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最初からやり直した後で、もう一度インストールする必要があります。
  - [アプリケーションの管理] ワークフローを使用して WorkSpaces から削除されたアプリケーションバンドルは、WorkSpaces に戻ります。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、それらのアプリケーションバンドルを WorkSpaces から手動でアンインストールします。
- WorkSpace の再構築 – WorkSpace を再構築すると、ルートボリュームが再作成されます。詳細については、「WorkSpaces の再構築」を参照してください。[アプリケーションの管理] を使用して変更した WorkSpaces を再構築すると、次の結果になります。
  - [アプリケーションの管理] ワークフローを使用して WorkSpaces にインストールされたアプリケーションバンドルは WorkSpaces から削除され、非アクティブになります。これらのアプリケーションを WorkSpaces に戻すには、[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。

  - [アプリケーションの管理] ワークフローを使用して WorkSpaces から削除されたアプリケーションバンドルは WorkSpaces にインストールされ、アクティブになります。これらのアプリケーションバンドルを WorkSpaces から削除するには、[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。
- WorkSpace の移行 – 移行プロセスでは、ターゲットバンドルイメージからの新しいルートボリュームと、元の WorkSpace の最後に利用可能なスナップショットからのユーザーボリュームを使用して WorkSpace を再作成します。新しい WorkSpace ID を持つ新しい WorkSpace が作成されます。詳細については、「WorkSpace の移行」を参照してください。[アプリケーションの管理] を使用して変更した WorkSpaces を移行すると、次の結果になります。
  - 移行元 WorkSpaces のすべてのアプリケーションバンドルが削除され、非アクティブになります。新しい移行先 WorkSpaces は、移行先の WorkSpaces バンドルからアプリケーションを継承します。移行元の WorkSpaces アプリケーションバンドルは 1 か月分の請求になりますが、移行先バンドルのアプリケーションバンドルには日割り計算が適用されます。

## WorkSpaces Personal で WorkSpace を変更する

WorkSpace の起動後に、以下の 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。
- WorkSpace が PCoIP AWS バンドルで作成された場合は、CLI または Amazon WorkSpace 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。 Amazon WorkSpaces

WorkSpace の現在の変更状態を表示するには、矢印を選択して WorkSpace の詳細を表示します。[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。

WorkSpace を修正する場合は、ステータスが `AVAILABLE` または `STOPPED` である必要があります。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。

WorkSpace 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、WorkSpace の請求レートが変更されます。

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、WorkSpaces Personal でユーザーを対象とした WorkSpaces の自己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

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、それぞれ 2000 GB まで増やすことができます。セットグループに付属の WorkSpace ルートボリュームおよびユーザーボリュームは変更できません。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**
>
> WorkSpace のボリュームを拡張すると、WorkSpaces により Windows または Linux 内でボリュームのパーティションが自動的に拡張されます。プロセスが終了したら、変更を有効にするために WorkSpace を再起動する必要があります。

データを確実に保持するために、WorkSpace の起動後はルートやユーザーボリュームのサイズを縮小できなくなります。代わりに、WorkSpace を起動するときに、これらのボリュームの最小サイズを指定してください。

- Value、Standard、Performance、Power、PowerPro のいずれかの WorkSpace は、最小 80 GB のルートボリュームおよび 10 GB のユーザーボリュームで起動できます。
- GeneralPurpose.4xlarge または GeneralPurpose.8xlarge WorkSpace を起動できます。ルートボリュームの場合は 175GB、ユーザーボリュームの場合は 100 GB 以上です。
- Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro WorkSpace は、最小 100 GB のルートボリュームおよび 100 GB のユーザーボリュームで起動できます。

WorkSpace のディスクサイズを拡大中の場合でも、ユーザーは自分の WorkSpace でほとんどのタスクを実行できます。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、WorkSpace の再構築、WorkSpace の再起動を行うことはできません。

> **Note**
>
> ディスクサイズの拡大中にユーザーが自身の WorkSpaces を使用できるようにするには、WorkSpaces のボリュームのサイズを変更する前に、WorkSpaces のステータスが `AVAILABLE` ではなく `STOPPED` であることを確認します。WorkSpaces が `STOPPED` となっている場合、ディスクサイズの拡大中にその WorkSpaces を起動することはできません。

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 WorkSpaces でボリュームサイズを変更している場合には、このプロセスが顕著に長くなることもあります。変更する WorkSpaces が多数ある場合は、 に連絡してサポート AWS サポート 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。
- WorkSpace を起動するときは、6 時間待ってからボリュームのサイズを変更する必要があります。
- 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、GraphicsPro でない限り、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、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。

WorkSpace のルートボリュームを変更するには

1. https://console.aws.amazon.com/workspaces/v2/home://www.com」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 root volume] (ルートボリュームの変更) の順に選択します。
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. [Save changes] (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、WorkSpace を再起動して変更を反映する必要があります。データの損失を避けるために、WorkSpace を再起動する前に、開いているファイルを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

1. https://console.aws.amazon.com/workspaces/v2/home://www.com」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 user volume] (ユーザーボリュームの変更) の順に選択します。
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. [Save changes] (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、WorkSpace を再起動して変更を反映する必要があります。データの損失を避けるために、WorkSpace を再起動する前に、開いているファイルを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

`RootVolumeSizeGib` または `UserVolumeSizeGib` プロパティを使用して 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

WorkSpace は、Standard、Power、Performance、PowerPro GeneralPurpose.4xlarge,および GeneralPurpose.8xlarge コンピューティングタイプの間で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**
>
> - ソースオペレーティングシステムが Windows Server 2022 または Windows 11 以外の場合は、コンピューティングタイプを PowerPro からGeneralPurposeに変更することはできません。
> - コンピューティングタイプを non-GPU-enabledバンドルから GeneralPurpose.4xlarge または GeneralPurpose.8xlarge,WorkSpaces は最小ルートボリュームサイズ 175 GB、ユーザーボリュームサイズ 100 GB を満たす必要があります。WorkSpaces のボリュームサイズを増やすには、「」を参照してくださいボリュームサイズの変更。
> - コンピューティングタイプを Graphics.g4dn から GraphicsPro.g4dn に、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は他の値に変更できません。
> - 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。それまでに 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、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
> - GraphicsPro バンドルは 2025 年 10 月 31 日にend-of-lifeとなります。GraphicsPro WorkSpaces は、2025 年 10 月 31 日より前にサポートされている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、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
> - Graphics および GraphicsPro のコンピューティングタイプは他の値に変更できません。

コンピューティングの変更をリクエストすると、WorkSpaces は新しいコンピューティングタイプを使用して WorkSpace を再起動します。WorkSpaces は、WorkSpace のオペレーティングシステム、アプリケーション、データ、およびストレージの設定を保持します。

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。新規の WorkSpace については、より大きなバンドルをリクエストするには 6 時間待機する必要があります。

WorkSpace コンピューティングタイプが変更中の場合、ユーザーは WorkSpace から切断されるため、WorkSpace を使用または変更することはできません。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**
>
> データの損失を避けるため、WorkSpace の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。

WorkSpace のコンピューティングタイプを変更するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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 compute type] (コンピューティングタイプの変更) の順に選択します。
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. [Save changes] (変更の保存) をクリックします。

WorkSpace のコンピューティングタイプを変更するには

`ComputeTypeName` プロパティを使用して 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、WorkSpace 移行機能を使用せずに、既存の WorkSpace を使用してプロトコルを移行できます。また、これにより、移行プロセス中に既存の PCoIP WorkSpaces を再作成しなくても、DCV を使用してルートボリュームを維持できます。

- 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ていて、GPU 対応の WorkSpace でない場合のみです。
- プロトコルを DCV に変更する前に、WorkSpace が DCV WorkSpace の以下の要件を満たしていることを確認してください。
  - WorkSpaces クライアントが DCV をサポートしている。
  - WorkSpace のデプロイ先のリージョンが DCV をサポートしている。
  - DCV 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、「WorkSpaces の IP アドレスとポートの要件」を参照してください。
  - 現在のバンドルが DCV 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、PowerPro、GeneralPurpose.4xlarge,または GeneralPurpose.8xlarge のみを使用することをお勧めします。

> **Note**
>
> - プロトコルの変更を開始する前に、本番環境以外の WorkSpaces 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 DCV に変更した後で PCoIP に戻すと、Web Access 経由で WorkSpaces に接続できなくなります。

WorkSpace のプロトコルを変更するには

1. (オプション) WorkSpace を再起動し、`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 の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`DCV` 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 `DCV` を必ず使用してください。

4. コマンドを実行した後で、WorkSpace が再起動して必要な設定を完了するまでには最大 20 分かかります。
5. `describe-workspaces` コマンドをもう一度使用して WorkSpace のプロパティを一覧表示し、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**
>
> - WorkSpace のプロトコルを変更しても、コンソールのバンドルの表示は更新されません。[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 WorkSpace が `UNHEALTHY` 状態のままである場合は、コンソールで WorkSpace を再起動します。

6. これで WorkSpace に接続できるようになりました。

## WorkSpaces Personal でブランドをカスタマイズする

Amazon WorkSpaces では、API を使用して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など、WorkSpace のログインページをカスタマイズすることで、ユーザーに親しみやすい WorkSpaces エクスペリエンスを作成できます。WorkSpace ログインページには、デフォルトの WorkSpaces ブランドに代わり、お客様のブランドがユーザーに表示されます。

以下のクライアントをサポートしています。

- Windows
- リナックス
- Android
- macOS
- iOS

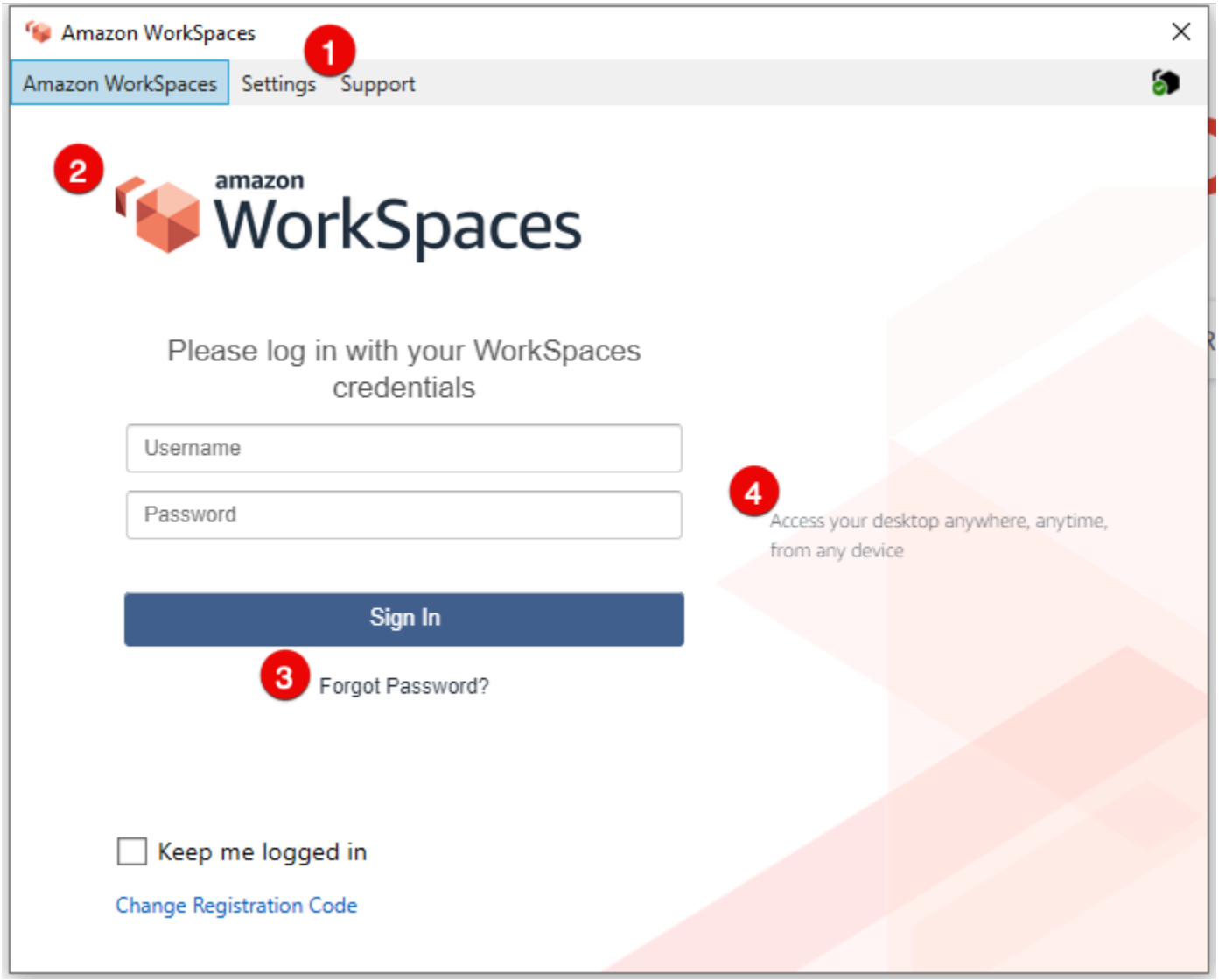
- Web Access

> **Note**
>
> で 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、「API リファレンスの ImportClientBranding」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 WorkSpaces に関するヘルプを問い合わせるためのサポート E メールリンク | • 各プラットフォームタイプでは、`SupportEmail` と `SupportLink` パラメー |

| ブランド要素 | 説明 | 要件と推奨事項 |
| --- | --- | --- |
| | を指定できます。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。 | 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。<br>• デフォルトの E メールは workspaces-feedback@amazon.com です。<br>• 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。<br>• 推奨解像度:<br>  • Android: 978 x 190<br>  • デスクトップ: 319 x 55<br>  • iOS@2x: 110 x 200<br>  • iOS@3x: 1650 x 300 |
| パスワードを忘れた場合のリンク | ForgotPasswordLink 属性を使用してウェブアドレスを追加し、これによりユーザーが WorkSpace のパスワードを忘れた場合に移動できます。 | 長さの制限：最小長 1、最大長は 200 です。 |

| ブランド要素 | 説明 | 要件と推奨事項 |
| --- | --- | --- |
| 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。 | • 長さの制約: 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。<br>• 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、ImportClientBranding を使用するためのサンプルコードスニペットです。

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、DescribeClientBranding を使用するためのサンプルスクリプトです。詳細については、「API リファレンスの DescribeClientBranding」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、DeleteClientBranding を使用するためのサンプルスクリプトです。詳細については、「API リファレンスの DeleteClientBranding」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 Personal で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。タグを使用することは、 AWS リソースを管理し、請求データを含むデータを整理するためのシンプルで強力な方法です。

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。
- タグ名または値に `aws:` または `aws:workspaces:` プレフィックスを使用しないでください。これらは AWS 使用のため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/v2/home「https://www.com」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、[キー] と [ボールト] 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. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
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、[キー] と [ボールト] 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。

## WorkSpaces Personal 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/v2/home「https://www.com」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/v2/home「https://www.com」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. [保存] を選択します。

を使用して WorkSpace の状態を変更するには AWS CLI

modify-workspace-state コマンドを使用します。

# WorkSpaces Personal の暗号化された 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 キーを使用して WorkSpaces のストレージボリュームを暗号化できます。WorkSpace を起動する際に、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) 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**
>
> - WorkSpaces の暗号化に加えて、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、「WorkSpaces Personal で FedRAMP 認証または DoD SRG コンプライアンスを設定する」を参照してください。
> - Amazon WorkSpaces では、BitLocker 暗号化はサポートされていません。

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、AmazonWorkSpaces の AWS 管理 KMS キー（ aws/workspaces ）または対称カスタマー管理の KMS キーのいずれかになります。

- AWS マネージド KMS キー – リージョンの WorkSpace sコンソールから暗号化されていない WorkSpaces を初めて起動すると、Amazon WorkSpaces はアカウントに AWS マネージド KMS キー (aws/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、WorkSpace 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。詳細については、「AWS KMSを使用した WorkSpaces 暗号化の概要」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 WorkSpaces は、この KMS キーを作成および管理します。Amazon WorkSpaces だけがこの KMS を使用でき、WorkSpaces はアカウント内の WorkSpaces リソースの暗号化だけに使用できます。

AWS Amazon WorkSpaces がサポートする マネージド KMS キーは、毎年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「ローテーション AWS KMS キー」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 を使用して KMS キーを作成する方法の詳細については、「 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場合は、元の KMS キーと新しい KMS キーの両方を有効にして、 AWS KMS が元の KMS キーが暗号化した WorkSpaces を復号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、WorkSpaces を再作成し、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 WorkSpaces を暗号化するには、次の要件を満たす必要があります。

- KMS キーは対称である必要があります。Amazon WorkSpaces では、非対称 KMS キーがサポートされていません。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 管理者に追加の許可を付与する」を参照してください。

## 制限

- 既存の WorkSpace は暗号化できません。WorkSpace を起動するときは、暗号化する必要があります。
- 暗号化された WorkSpace からのカスタムイメージの作成は、サポートされていません。
- 暗号化された WorkSpace の暗号化を無効にすることは、現在サポートされていません。
- ルートボリュームの暗号化を有効にした状態で起動された WorkSpaces では、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 WorkSpace を再起動または再構築するには、 AWS KMS キーが有効であることを最初に確認します。有効ではない場合、WorkSpace は使用できません。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。

## AWS KMSを使用した WorkSpaces 暗号化の概要

暗号化されたボリュームで WorkSpaces を作成すると、WorkSpaces は Amazon Elastic Block Store (Amazon EBS) を使用してこ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 WorkSpaces の両方が KMS キーを使用して暗号化されたボリュームを操作します。EBS ボリューム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。

暗号化されたボリュームを使用するWorkSpaces を起動すると、エンドツーエンドの処理が次のように行われます。

1. 暗号化に使用する KMS キーと、WorkSpace のユーザーとディレクトリを指定します。このアクションにより、この WorkSpaces (指定されたユーザーとディレクトリに関連付けられた WorkSpace )にのみ KMS キーの使用を許可する権限が作成されます。

2. WorkSpaces は、WorkSpace の暗号化された EBS ボリュームを作成し、使用する KMS キーとボリュームのユーザーおよびディレクトリを指定します。このアクションにより、Amazon EBS が WorkSpace とボリューム (指定されたユーザーとディレクトリに関連付けられた WorkSpace および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権限が作成されます。
3. Amazon EBS は、KMS キーによって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) および AWS Directory Service ディレクトリ ID、ならびに暗号化コンテキストとしての 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 WorkSpace にアタッチします。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 WorkSpace にアタッチされている限り、プレーンテキストデータキーをメモリ内に保持します。
8. Amazon EBS は、暗号化されたデータキー (Step 4 で受け取ったデータキー) とボリュームメタデータを保存し、後で WorkSpace を再起動または再構築した場合に使用できるようにします。
9. を使用して WorkSpace AWS Management Console を削除する (または WorkSpaces API で `TerminateWorkspaces`アクションを使用する) と、WorkSpaces と Amazon EBS は、その WorkSpace の KMS キーの使用を許可した許可を廃止します。

## 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) `Decrypt`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 にリクエストを送信しません。ただし、Amazon EBS が、WorkSpaces の暗号化されたボリュームに対して暗号化されたデータキーをリクエストする場合 (Step 3 の AWS KMSを使用した WorkSpaces 暗号化の概要) と、そのデータキーのプレーンテキストコピーをリクエストする場合 (Step 5) には、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、 がデータの整合性を確保するために AWS KMS 使用する追加の認証済みデータ (AAD) を提供します。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、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。

- WorkSpace 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
- 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 キーを使用する許可を WorkSpaces に付与する

WorkSpace sの AWS マネージド KMS キー (aws/workspaces) またはカスタマーマネージド KMS キーで WorkSpaces データを保護できます。カスタマー管理 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 許可を与える必要があります。WorkSpaces の 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。

WorkSpaces で使用する KNS キーを準備するには、次の手順を実行します。

1. KMS キーのキーポリシーでキーユーザーのリストに WorkSpaces 管理者を追加する
2. IAM ポリシーによって 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、WorkSpaces を使用する許可も必要です。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 の管理者をキーユーザーとして追加する

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://www.com 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ーを使用します。
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、[Add] (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. GetKeyPolicy オペレーションを使用して既存のキーポリシードキュメントを取得し、キー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. PutKeyPolicy オペレーションを使用して、KMS キーにキーポリシーを適用します。

パート 2: IAM ポリシーを使用して WorkSpaces 管理者に追加の許可を付与する

カスタマー管理の KMS キーを選択して暗号化に使用する場合は、アカウントで暗号化された WorkSpaces を起動する IAM ユーザーの代わりに、Amazon WorkSpaces で KMS キーの使用を許可する IAM ポリシーを確立する必要があります。また、そのユーザーにも、Amazon WorkSpaces を使用するための許可が必要です。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 の暗号化では、KMS キーへのアクセスを制限する必要があります。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、 と統合されている AWS サービスが AWS KMS 、指定されたプリンシパルに代わって キーを使用できます。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で WorkSpaces AWS Management Console を作成する場合、管理者はエイリアスとリストキー ( "kms:ListAliases" および のアクセス許可) を一覧表示するアクセス"kms:ListKeys"許可が必要です。WorkSpaces 管理者が (コンソールではなく) Amazon WorkSpaces API のみを使用する場合は、"kms:ListAliases" および "kms:ListKeys" のアクセス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"}}
    }
  ]
}
```

WorkSpace を暗号化しているロールまたはユーザーに適用する IAM ポリシーには、カスタマー管理の KMS キーを使用するためのアクセス許可と WorkSpaces へのアクセス権が必要です。IAM ユーザーまたはロールに WorkSpaces のアクセス許可を付与するには、以下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": "*"
    }
  ]
}
```

## WorkSpace を暗号化します。

WorkSpace を暗号化するには

1. https://console.aws.amazon.com/workspaces/v2/home://www.com」で WorkSpaces コンソールを開きます。
2. [Launch WorkSpaces] を選択し、最初の 3 つの手順を完了します。
3. [WorkSpaces Configuration] のステップで、以下を行います。
   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 WorkSpaces によって作成された AWS マネージド KMS キーまたは作成した 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 では、非対称 KMS キーがサポートされていません。
   c. [Next Step] を選択します。
4. [Launch WorkSpaces] を選択します。

## 暗号化された WorkSpaces を表示する

どの WorkSpaces とボリュームが WorkSpaces コンソールから暗号化されたのかを表示するには、左のナビゲーションバーから [WorkSpaces] を選択します。[Volume Encryption] 列に、各 WorkSpace で暗号化が有効になっているか無効になっているかが表示されます。特定のボリュームが暗号化されているかどうかを表示するには、WorkSpace エントリを展開して [Encrypted Volumes] フィールドを確認します。

## WorkSpaces Personal の WorkSpace を再起動する

場合によっては、WorkSpace を手動で再起動する必要があります。WorkSpace を再起動すると、ユーザーが切断され、WorkSpace のシャットダウンと再起動が実行されます。データの損失を避けるため、WorkSpace 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。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 WorkSpace を再起動するには、まず AWS KMS キーが有効になっていることを確認します。有効になっていない場合、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。

WorkSpace を再起動するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 再起動する WorkSpaces を選択したら、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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、[Reboot WorkSpaces] を選択します。

を使用して WorkSpace を再起動するには AWS CLI

reboot-workspaces コマンドを使用します。

WorkSpaces を一括再起動するには

amazon-workspaces-admin-module を使用します。

## WorkSpaces Personal の WorkSpace を再構築する

WorkSpace を再構築すると、WorkSpace の起動元のバンドルの最新イメージのルートボリューム、ユーザーボリューム、およびプライマリ Elastic Network Interface が再作成されます。WorkSpace を再構築すると、WorkSpace を復元するよりも多くのデータが削除されますが、必要なのは

ユーザーボリュームのスナップショットだけです。WorkSpace を復元するには、「WorkSpaces Personal の WorkSpace を復元する」を参照してください。

WorkSpace を再構築すると、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 /) は、WorkSpace の作成元のバンドルの最新のイメージで更新されます。WorkSpace の作成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。

  WorkSpace を再構築するとき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。ユーザーボリュームのこれらのスナップショットは、WorkSpace の正常性に関係なく取得されます。[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 を再構築すると、再構築が完了した直後に (多くの場合 30 分以内に) 新しいスナップショットも作成されます。
- プライマリ Elastic Network Interface が再作成されます。WorkSpace は新しいプライベート IP アドレスを受け取ります。

> **Important**
>
> 2020 年 1 月 14 日以降、パブリック Windows 7 バンドルから作成された WorkSpaces を再構築することはできません。Windows 7 の WorkSpaces については、Windows 10 への移行を検討することをお勧めします。詳細については、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。

WorkSpace を再構築できるのは、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`、`STOPPED`、または `REBOOTING` である必要があります。`REBOOTING` 状態で WorkSpace 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。

WorkSpace を再構築するには

> **Warning**
>
> 暗号化された WorkSpace を再構築するには、まず AWS KMS キーが有効になっていることを確認します。有効になっていない場合、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/v2/home「https://www.com 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. 再ビルドする 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. [Rebuild] を選択します。

を使用して WorkSpace 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した後に WorkSpace 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、ユーザー命名属性を元に戻してから再ビルドをするか、そのユーザー用に新しい WorkSpace を作成します。

Microsoft Entra ID に参加済みの WorkSpaces を再構築する

ユーザーが再構築後に初めて WorkSpace にログインするときは、新しい WorkSpace が割り当てられたときと同様に、Out of Box Experience (OOBE) を再度実行する必要があります。その結果、WorkSpace に新しいユーザープロファイルフォルダが作成され、元のユーザープロファイル

フォルダが上書きされます。したがって、Entra に参加している WorkSpace の再構築中、元のユーザープロファイルフォルダのコンテンツは再構築された WorkSpace の D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated> に保存されます。デスクトップアイコン、ショートカット、データファイルを含むすべてのユーザープロファイルデータを復元するには、ユーザーが元のプロファイルコンテンツを D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated> からユーザーのプロファイルフォルダ D:\Users\<USERNAME> にコピーする必要があります。

> **Note**
>
> Microsoft Entra ID に参加している WorkSpaces では、可能な場合は常に、WorkSpaces の再構築ではなく WorkSpaces の復元を使用することをお勧めします。

## WorkSpaces Personal の WorkSpace を復元する

WorkSpace を復元すると、WorkSpace が正常であったときに取得された各ボリュームのスナップショットを使用して、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、ルートボリュームとユーザーボリュームの両方のデータが、スナップショットが作成された時点までロールバックされます。WorkSpace を再構築すると、ユーザーボリュームのデータのみがロールバックされます。つまり、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、復元には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、「WorkSpaces Personal の WorkSpace を再構築する」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 /) は、スナップショットを使用して、指定された日時で復元されます。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) は、スナップショットを使用して、指定された日時で再作成されます。ユーザーボリュームの現在の内容は上書きされます。

### 復元ポイント

[アクション]、[WorkSpace のリビルドとリストア] の順に選択すると、操作に使用されるスナップショットの日付と時刻が表示されます。操作に使用されるスナップショットの日付と時刻を AWS CLIで確認するには、describe-workspace-snapshots コマンドを使用します。

### 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。

- 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。一部のリージョンでは AWS 、WorkSpace の作成後に最初のスナップショットを取得するまでに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。一部のリージョンでは AWS 、WorkSpace が復元されてからこれらのスナップショットを取得するまでに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/v2/home「https://www.com」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。

を使用して WorkSpace を復元するには AWS CLI

restore-workspace コマンドを使用します。

## WorkSpaces Personal での 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れば、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を搭載した WorkSpaces に 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することができます。

- Windows 10 (Bring Your Own License)
- Windows 11 (Bring Your Own License)
- Windows Server 2016
- [Windows Server 2019]
- Windows Server 2022

WorkSpaces で Microsoft 365 Apps for enterprise を使用するには、Microsoft 365 E3/E5、Microsoft 365 A3/A5、Microsoft 365 G3/G5、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 をインストールおよび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 365 に含まれていない Microsoft アプリケーション (Microsoft Project、Microsoft Visio、Microsoft Power Automate など) を WorkSpaces にインストールすることもできますが、自分の追加ライセンスを用意する必要があります。

プライマリ WorkSpaces とフェイルオーバー WorkSpaces にはマルチリージョンレジリエンスを使用して、Microsoft 365 やその他の 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 でワークスペースを作成
- 既存の WorkSpaces を移行して、Microsoft 365 Apps for enterprise を使用する
- WorkSpaces で Microsoft 365 Apps for enterprise を更新する

## Microsoft 365 Apps for enterprise でワークスペースを作成

Microsoft 365 Apps for enterprise で WorkSpaces を作成するには、アプリケーションをインストールし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。この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た新しい WorkSpaces を起動できます。WorkSpaces では、Microsoft 365 Apps for enterprise のパブリックバンドルは提供していません。

Microsoft 365 Apps for enterprise で WorkSpace を作成するには:

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
2. 他の Microsoft アプリケーション WorkSpaces のイメージとして使用する WorkSpace を起動します。ここに Microsoft アプリケーションをインストールします。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. WorkSpace から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、「カスタムの WorkSpaces イメージとバンドルの作成」を参照してください。

7. 作成したカスタムバンドルを使用して WorkSpaces を起動します。これらの WorkSpaces には、Microsoft 365 Apps for enterprise がインストールされています。

## 既存の WorkSpaces を移行して、Microsoft 365 Apps for enterprise を使用する

WorkSpaces に を通じて Microsoft Office ライセンスがない場合は AWS、WorkSpaces 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 ライセンスがある場合は AWS、エンタープライズ用 Microsoft 365 Apps をインストールする前に、まず Microsoft Office ライセンスの登録を解除する必要があります。

**Important**

WorkSpaces 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されません。Microsoft Office ライセンスの料金が発生しないようにするには、次のいずれか AWS を実行して、 を使用して Microsoft Office アプリケーションから WorkSpaces を登録解除します。

- アプリケーションの管理 (推奨) – Microsoft Office 2016 と 2019 をWorkSpaces からアンインストールできます。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。アンインストール後は、WorkSpaces に Microsoft 365 Apps for enterprise をインストールできます。
- WorkSpace の移行 – ユーザーボリューム上のデータを保持しながら、1 つのバンドルから別のバンドルに WorkSpace 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。移行が完了すると、WorkSpaces に Microsoft 365 Apps for enterprise をインストールできます。
  - または、イメージに既に Microsoft 365 Apps for enterprise がインストールされているカスタム WorkSpaces イメージとバンドルを作成してから、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。
  - WorkSpaces の移行方法の詳細については、「WorkSpace の移行」を参照してください。

### WorkSpaces で Microsoft 365 Apps for enterprise を更新する

デフォルトでは、Microsoft Windows オペレーティングシステムで実行されている 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。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頻度を設定するには、更新チャネルを指定し、Microsoft 365 on WorkSpaces のライセンスポリシーに準拠するように、[現在のチャネル] または [月次エンタープライズチャネル] に設定します。

## WorkSpaces Personal で Windows BYOL WorkSpaces をアップグレードする

Windows Bring-Your-Own-License (BYOL) WorkSpaces では、インプレース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 および 11 の BYOL WorkSpaces にのみ適用されます。

> **Important**
>
> アップグレード済みの WorkSpace で Sysprep を実行しないでください。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 を実行する予定の場合は、アップグレードされていない WorkSpace のみで使用してください。

> **Note**
>
> このプロセスを使用して Windows 10 および 11 の 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。

内容

## 前提条件

- グループポリシーや System Center Configuration Manager (SCCM) を使用して Windows 10 および 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 および 11 の WorkSpaces に対して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。
- WorkSpace が自動停止 WorkSpace である場合は、AlwaysOn WorkSpace に変更してからインプレースアップグレードプロセスを開始し、更新の適用中に自動停止しないようにします。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 を AutoStop に設定したままにする場合は、アップグレードの実行中に自動停止時間を 3 時間以上に変更します。
- 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` および `update-pvdrivers.ps1`) を使用して、Windows Update プロセスの実行に必要な変更を WorkSpaces に加えます。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 は D:\Users\%USERNAME% にユーザープロファイルを作成します。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 にプロファイルが保存されている WorkSpaces は、再構築または移行すると、自分でデータをバックアップして復元しない限り、ユーザープロファイルのすべてのデータは失われます。ドライブ C にプロファイルを残す場合は、このトピックで後述するように、UserShellFoldersRedirection レジストリキーを使用して、ユーザーシェルフォルダをドライブ D にリダイレクトできます。

WorkSpaces を確実に再構築または移行できるようにしたり、ユーザーシェルフォルダのリダイレクトに関する起こり得る問題を回避したりするには、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 に復元することをお勧めします。そのためには、このトピックで後述するように、PostUpgradeRestoreProfileOnD レジストリキーを使用します。

## 既知の制限事項

- ドライブ D からドライブ C へのユーザープロファイルの場所の変更は、WorkSpace の再構築または移行中には行われません。Windows 10 および 11 の BYOL WorkSpace でインプレースアップグレードを実行してから、その WorkSpace を再構築または移行すると、新しい WorkSpace のドライブ D にユーザープロファイルが作成されます。

  > **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。

- また、デフォルトの BYOL バンドル内のイメージが旧リリースの Windows 10 および 11 に基づいている場合は、WorkSpace の再構築または移行後に再度インプレースアップグレードを実行する必要があります。

## 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: HKLM:\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<br><br>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<br><br>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) を復元する |
| 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<br><br>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 – ユーザープロファイルのレジストリを変更した後、スクリプトが WorkSpace を再起動することを許可しない |

レジストリパス: HKLM:\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 AWS ドライバーの更新を無効にします<br><br>1 – PV AWS 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 WorkSpaces でインプレース Windows アップグレードを有効にするには、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。複数の WorkSpaces を更新する場合は、グループポリシーまたは SCCM を使用して PowerShell スクリプトをプッシュできます。サンプルの PowerShell スクリプトについては、PowerShell スクリプトを使用して WorkSpace レジストリを更新する を参照してください。

Windows 10 および 11 のインプレースアップグレードを実行するには

1. 更新する Windows 10 および 11 の BYOL WorkSpaces で現在実行されている Windows のバージョンを確認し、システムを再起動します。
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変更により、WorkSpace のインプレースアップグレードが有効になります。

- HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1
- HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\update-pvdrivers.ps1

> **Note**
>
> これらのキーが存在しない場合は、WorkSpace を再起動します。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\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\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\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

     キー名: PostUpgradeRestoreProfileOnD

     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\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

     キー名: PostUpgradeRestoreProfileOnD

キー値: 1

キー名: UserShellFoldersRedirection

キー値: 0

4. レジストリに変更を保存したら、再び WorkSpace を再起動して変更を適用します。

> **Note**
>
> - 再起動後に 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約 10 分かかります。

(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。この設定で、WorkSpace がブロック解除され、更新可能になります。

HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\profileImagePathDeleted

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。元の Windows 10 および 11 バージョンとインストール済みのアプリ数に応じて、このプロセスの所要時間は 40 ～ 120 分です。

> **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 インスタンスの状態は、アップグレード中に UNHEALTHY として表示されることがあります。

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**
>
> インプレースアップグレードが失敗すると、Windows は自動的にロールバックし、アップグレードを開始する前に存在していた Windows 10 および 11 バージョンを使用しま

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\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\scriptExecutionComplete

7. AlwaysOn に設定するか、自動停止時間を変更することで WorkSpace の実行モードを変更し、インプレースアップグレードプロセスを中断することなく実行できるようにした場合は、実行モードを元の設定に戻します。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、インプレースアップグレード後に C:\Users\%USERNAME% に配置されるため、今後の 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再度実行する必要はありません。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 WorkSpaces の他の場所にリダイレクトする場合は、インプレースアップグレード後に WorkSpaces で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。

  Windows ログ > Application > Source: Amazon WorkSpaces

> **Tip**
>
> インプレースアップグレード中にデスクトップの一部のアイコンのショートカットが正常に動作しなくなった場合、アップグレードの準備のために WorkSpaces によってドライブ D のユーザープロファイルがドライブ C に移動されたことが原因です。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。

## PowerShell スクリプトを使用して WorkSpace レジストリを更新する

次のサンプルの PowerShell スクリプトを使用して WorkSpaces 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することができます。インプレースアップグレードの実行 に従いますが、このスクリプトを使用して各 WorkSpace のレジストリを更新します。

```
# 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
    }
}
```

# WorkSpaces Personal で WorkSpace を移行する

> **Note**
>
> AWS を通じてWorkSpace から Microsoft Office バージョンのライセンスをサブスクリプション解除またはアンインストールする場合は、[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ながら、1 つのバンドルから別のバンドルに WorkSpace 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から Windows 10 デスクトップエクスペリエンスに WorkSpaces を移行できます。
- WorkSpaces を PCoIP プロトコルから DCV に移行できます。
- Windows Server 2016 搭載の WorkSpaces に 32 ビットの Microsoft Office が付属したバンドルから、Windows Server 2019 および Windows Server 2022 搭載の WorkSpaces に 64 ビットの Microsoft Office が付属したバンドルに、WorkSpaces 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 WorkSpaces を移行することもできます。例えば、GPU 対応 (Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro) バンドルから非 GPU 対応のバンドルへの移行、またはその逆に移行できます。
- WorkSpaces を Windows 10 BYOL 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 のバリューバンドル WorkSpaces を Windows 11 に移行するには、まずバリュー WorkSpaces を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。
- WorkSpaces を Windows 7 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、Windows 10 WorkSpace に少なくとも 1 回ログインしてください。Windows 7 WorkSpaces から Windows 11 への直接の移行はサポートされていません。
- Microsoft Office を使用する Windows WorkSpaces AWS を、Microsoft 365 アプリケーションを使用するカスタム 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 を使用する Windows WorkSpaces AWS を、Office 2016/2019 サブスクリプションなしで 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。
- BYOL BYOP WorkSpaces を Windows 10 から Windows 11 に移行し、ライセンス込みの BYOP WorkSpaces を Windows Server 2019 から Windows Server 2022 に移行できます。

Amazon WorkSpaces バンドルの詳細については、WorkSpaces Personal のバンドルとイメージ を参照してください。

移行プロセスでは、ターゲットバンドルイメージからの新しいルートボリュームと、元の WorkSpace の最後に利用可能なスナップショットからのユーザーボリュームを使用して WorkSpace を再作成します。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、WorkSpace ごとに最大 1 時間かかります。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 が終了します。

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 WorkSpaces は、他の BYOL バンドルにのみ移行できます。BYOL WorkSpace を PCoIP から DCV に移行するには、最初に DCV プロトコルを使用して 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 DCV 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作成された WorkSpace を BYOL バンドルに移行することはできません。
- Graphics.g4dn、GraphicsPro.g4dn,Graphics、GraphicsPro バンドルは、Windows および Ubuntu の PCoIP プロトコルで使用できます。Graphics.g4dn および GraphicsPro.g4dn は、Windows および Ubuntu の DCV プロトコルで使用できます。Graphics と GraphicsPro WorkSpaces をまだ DCV に移行することはできません。
- Linux WorkSpaces の移行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 WorkSpaces を移行できます。
- 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)。同じバンドルを使用して WorkSpace を更新する場合は、代わりに WorkSpace を再構築します。
- リージョン間で WorkSpaces を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。移行の試行後 1 時間経過しても WorkSpace バンドルが同じである場合、移行は失敗します。AWS サポート センターにアクセスしてサポートをお求めください。
- BYOP WorkSpaces を PCoIP または DCV WorkSpaces に移行することはできません。
- Active Directory ドメイン結合 WorkSpaces を Microsoft Entra-joined WorkSpaces に移行することはできません。

## 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 |

| 移行元 OS | 移行先 OS | 使用可能 |
| --- | --- | --- |
| 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 |
| 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 |

| 移行元 OS | 移行先 OS | 使用可能 |
| --- | --- | --- |
| 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 |
| 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 |
| Windows 10 BYOP BYOL | Windows 11 BYOP BYOL | はい |
| Windows 11 BYOP BYOL | Windows 10 BYOP BYOL | いいえ |
| Windows Server 2019 搭載のパブリック BYOP | Windows Server 2022 搭載のパブリック BYOP | はい |
| Windows Server 2022 搭載のパブリック BYOP | Windows Server 2019 搭載のパブリック BYOP | いいえ |

**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 WorkSpace の初回起動時に、移行プロセスで元の `D:\Users\%USERNAME%` フォルダが `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` という名前のフォルダに移動されます。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 WorkSpace に割り当てられたタグは移行中に引き継がれ、WorkSpace の実行モードは保持されます。ただし、新しい WorkSpace は、新しい WorkSpace ID、コンピュータ名、および IP アドレスを取得します。

## ベストプラクティス

WorkSpace を移行する前に、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たことを確認するために、移行中の WorkSpace の経過時間が 12 時間以上であることを確認します。Amazon WorkSpaces コンソールの [Migrate WorkSpaces] (WorkSpace の移行) 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に、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。WorkSpaces が ADMIN_MAINTENANCE モードになっている場合は移行できないことに注意してください。
- 移行する WorkSpaces のステータスが、AVAILABLE、STOPPED、または ERROR であることを確認します。
- 移行する WorkSpaces 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 WorkSpaces に割り当てられます。
- スクリプトを使用して WorkSpaces を移行する場合、一度に移行できる WorkSpace のバッチの最大数は 25 です。

## 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 WorkSpaces を移行し、移行が成功しなかった場合、API によって返されたターゲット WorkSpace ID は使用されず、WorkSpace で元の WorkSpace ID が保持されます。
- 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。不要になった WorkSpaces は、手動による削除が必要になる場合があります。

## 請求への影響

移行が発生する月に、新しい WorkSpaces と元の WorkSpaces の両方に比例配分された金額が請求されます。たとえば、5 月 10 日に WorkSpace A を WorkSpace B に移行すると、5 月 1 日から 5 月 10 日まで WorkSpace A の料金が請求され、5 月 11 日から 5 月 30 日まで WorkSpace B の料金が請求されます。

> **Note**
>
> WorkSpace を別のバンドルタイプに移行する場合 (たとえば、Performance から Power へ、または Value から Standard へ)、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、移行元の 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。

## WorkSpace の移行

WorkSpaces は、Amazon WorkSpaces コンソール、、 AWS CLI または Amazon WorkSpaces API を使用して移行できます。

WorkSpace を移行するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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 を選択したら、[アクション]、[Migrate WorkSpaces (WorkSpace の移行)] の順に選択します。
4. [Bundle] (バンドル) で、WorkSpace の移行先のバンドルを選択します。

   > **Note**
   >
   > BYOL WorkSpace を PCoIP から DCV に移行するには、最初に DCV プロトコルを使用して 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 DCV BYOL バンドルに移行できます。

5. [Migrate WorkSpaces (WorkSpace の移行)] を選択します。

   Amazon WorkSpaces コンソールに、ステータスが `PENDING` の新しい WorkSpace が表示されます。移行が完了すると、元の WorkSpace が終了し、新しい WorkSpace のステータスが `AVAILABLE` に設定されます。
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 Personal で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。

を介して WorkSpaces を移行するには AWS CLI、migrate-workspace コマンドを使用します。Amazon WorkSpaces API を使用して WorkSpaces を移行するには、Amazon WorkSpaces API リファレンスの MigrateWorkSpace を参照してください。

## WorkSpaces Personal で WorkSpace を削除する

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 Personal でディレクトリを削除する 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/v2/home「https://www.com」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 Personal で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 Personal でディレクトリを削除する」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。

# WorkSpaces Personal の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、およびソフトウェアリソースの組み合わせです。WorkSpace を起動するときに、必要に応じてバンドルを選択します。WorkSpaces で使用できるデフォルトのバンドルはパブリックバンドルと呼ばれます。WorkSpaces で利用可能なさまざまな公開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。

Windows または Linux WorkSpace を起動してカスタマイズした場合は、その WorkSpace からカスタムイメージを作成できます。

カスタムイメージには、WorkSpace の OS、ソフトウェア、設定のみが含まれます。カスタムバンドルは、WorkSpace の起動元になるカスタムイメージとハードウェアの両方を組み合わせたものです。

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 WorkSpaces を起動するときにこのカスタムバンドルを指定して、新しい WorkSpaces が同じ一貫した構成 (ハードウェアとソフトウェア) になるようにします。

WorkSpaces にソフトウェアの更新や追加ソフトウェアのインストールが必要な場合は、カスタムバンドルを更新し、そのバンドルにより WorkSpaces を再構築できます。

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。次の表は、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ています。

| 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/サポート終了日 |
|---|---|---|---|---|
| Windows Server 2016 | 含まれる | DCV、PCo | Value、Standard、Performance、Power、PowerPro、Graphics (廃止)、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn | 2027 年 1 月 12 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/サポート終了日 |
|---|---|---|---|---|
| [Windows Server 2019] | 含まれる | DCV、PCo | Value、Standard、Performance、Power、PowerPro、Graphics (廃止)、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn | 2029 年 1 月 9 日 |
| Windows Server 2022 | 含まれる | DCV、PCo | Standard、Performance、Power、PowerPro、GeneralPurpose.4xlarge,GeneralPurpose.8xlarge,Graphics (廃止)、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn | 2031 年 10 月 14 日 |
| Windows 10 | Bring-Your-Own-License (BYOL) | DCV、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) | DCV | Standard、Performance、Power、PowerPro、GeneralPurpose.4xlarge,GeneralPurpose.8xlarge | サポート中 |
| Amazon Linux 2 | 含まれる | DCV、PCo | Value、Standard、Performance、Power、PowerPro | サポート中 |
| Ubuntu 22.04 LTS | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro、Graphics.g4dn、GraphicsPro.g4dn | 2032 年 6 月 |

| 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/サポート終了日 |
|---|---|---|---|---|
| Rocky Linux 8 | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro | 2029 年 5 月 31 日 |
| Red Hat Enterprise Linux 8 | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro | 2029 年 5 月 31 日 |

> **Note**
>
> - ベンダーでサポートされ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 サポートでもサポートされません。
> - Windows オペレーティングシステムで実行されている WorkSpaces の場合、Graphics 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



## WorkSpaces Personal の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。DCV 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。
> - BYOP (Bring Your Own Protocol) バンドルは WorkSpaces Core 用です。Amazon WorkSpaces が提供する BYOP バンドルには、WorkSpaces が提供するストリーミングプロトコルがインストールされていません。WorkSpaces クライアントまたはゲートウェイを使用して接続することはできません。Amazon WorkSpaces Core の責任共有モデルを理解するには、Amazon WorkSpaces Core のテクノロジーパートナー統合ガイド」を参照してください。詳細については、Amazon WorkSpaces Core」を参照してください。

> **Important**
>
> - GraphicsPro バンドルは 2025 年 10 月 31 日にend-of-lifeになります。2025 年 10 月 31 日より前に、GraphicsPro WorkSpaces をサポートされている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、「WorkSpaces Personal で WorkSpace を移行する」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。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
- E メール

このバンドルは、音声およびビデオ会議、画面共有、ワードプロセッシング、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、グラフィックス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
- E 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、グラフィックス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
- E 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
- E 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やグラフィックアプリケーションにはお勧めしません。

汎用バンドル

これらのバンドルは、GeneralPurpose.4xlarge およびGeneralPurpose.8xlarge,以下に適しています。

- ウェブブラウジング
- 言語処理
- E 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
- Batch 処理
- CPU ベースの ML (機械学習) モデルトレーニング

このバンドルは、複雑なモデルの 3D レンダリング、写真のようにリアルな設計、ゲームストリーミング、ML モデルトレーニング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
- E 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、写真のようにリアルな設計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
- E 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、音声およびビデオ会議、3D レンダリング、写真のようなリアルな設計、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 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
- E 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。

## WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する

Windows または Linux WorkSpace を起動してカスタマイズした場合は、その WorkSpace 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。

カスタムイメージには、WorkSpace の OS、ソフトウェア、設定のみが含まれます。カスタムバンドルは、WorkSpace の起動元になるカスタムイメージとハードウェアの両方を組み合わせたものです。

> **Note**
>
> バンドルを削除した後で同じ名前の新しいバンドルを作成する場合は、削除してから少なくとも 2 時間待ってください。

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 WorkSpaces を起動するときにこのカスタムバンドルを指定して、新しい WorkSpaces が同じ一貫した構成 (ハードウェアとソフトウェア) になるようにします。

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 WorkSpace からイメージを作成する場合、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、イメージの作成はサポートされないことに注意してください。ただし、Windows の累積的な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 のイメージ作成プロセスでサポートされます。
> - 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 の WorkSpaces については、Windows 10 への移行を検討することをお勧めします。詳細については、「WorkSpaces Personal で WorkSpace を移行する」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。それまでに 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、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。
> - GraphicsPro バンドルは 2025 年 10 月 31 日にend-of-lifeとなります。GraphicsPro WorkSpaces は、2025 年 10 月 31 日より前にサポートされている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、「the section called “WorkSpace の移行”」を参照してください。
> - 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。

- カスタムバンドルの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。

目次



## 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。お客様が WorkSpace のイメージを作成するには、C ドライブに 12,884,901,888 バイト (または 12 GiB) を超える空き容量があり、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 のステータスが [利用可能] で、変更の状態が [なし] であることが必要です。
- WorkSpaces イメージ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 WorkSpaces では、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 WorkSpaces では、C ドライブには 12 GB 以上の空き容量が必要です。

- WorkSpace 上で実行されるすべてのアプリケーションサービスは、ドメインユーザー資格情報の代わりにローカルシステムアカウント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。
- WorkSpace は暗号化しないでください。暗号化された WorkSpace からのイメージの作成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、イメージから起動する WorkSpaces は正しく機能しません。詳細については、「the section called “必須の設定とサービスコンポーネント”」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

- WorkSpace のステータスが [利用可能] で、変更の状態が [なし] であることが必要です。
- 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。
- WorkSpace は暗号化しないでください。暗号化された WorkSpace からのイメージの作成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、イメージから起動する WorkSpaces は正しく機能しません。
  - Cloud-init
  - Teradici PCoIP または DCV 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

WorkSpace からイメージを作成する前に、以下を実行します。

- 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。
- WorkSpace をプライベートサブネットにデプロイし、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 WorkSpace の最小ボリュームサイズを使用し、カスタムバンドルの作成時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プログラム (Windows の機能/バージョンの更新プログラムを除く) とすべてのアプリケーション更新プログラムを WorkSpace にインストールします。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ない WorkSpace からキャッシュされたデータを削除します (たとえば、ブラウザの履歴、キャッシュされたファイル、ブラウザの Cookie など)。
- バンドルに含めるべきではない WorkSpace から構成設定を削除します (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ます。デフォルトでは、リージョンごとに 40 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 制限のフォームを使用します。
- 暗号化された WorkSpace 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。暗号化された WorkSpace からのイメージの作成は現在サポートされていません。
- WorkSpace でウイルス対策ソフトウェアを実行している場合は、イメージの作成時に無効にします。
- WorkSpace でファイアウォールを有効にしている場合は、ファイアウォールによって必要なポートがブロックされていないことを確認します。詳細については、「WorkSpaces Personal の IP アドレスとポートの要件」を参照してください。
- Windows WorkSpaces の場合、イメージを作成する前にグループポリシーオブジェクト (GPO) を設定しないでください。
- Windows WorkSpaces の場合、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 WorkSpaces については、ホワイトペーパー「Linux イメージ用に Amazon WorkSpaces を準備するためのベストプラクティス」も参照してください。
- DCV を有効にした状態で Linux WorkSpace でスマートカードを使用する場合、イメージを作成する前に Linux WorkSpace に対して行う必要があるカスタマイズについては、「WorkSpaces Personal での認証にスマートカードを使用する」を参照してください。
- ENA、NVMe、PV ドライバーなど、WorkSpaces のネットワーク依存関係ドライバーを必ず更新してください。この作業は、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)、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に関する説明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。この作業は、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 および 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ライセンス持ち込み (BYOL) イメージから起動した WorkSpaces の場合、デフォルトのコンピュータ名の形式を使用する代わりに、コンピュータ名の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 WorkSpaces のコンピュータ名の形式は `DESKTOP-XXXXX` であり、Windows 11 WorkSpaces のコンピュータ名の形式は `WORKSPA-XXXXX` です。

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で `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` 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**
>
> WorkSpace の Windows エクスプローラーから C: ドライブにアクセスするには、アドレスバーに **C:** 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 のドキュメントの「ComputerName」をご参照ください。
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、<RegisteredOrganization> に **Amazon.com** を指定し、<RegisteredOwner> に **EC2** を指定したとします。Windows 10 ベースのイメージの場合、カスタムバンドルを使用する WorkSpaces のコンピュータ名は EC2AMAZ-*xxxxxxx* で始まります。Windows 11 ベースのイメージの場合、カスタムバンドルを使用する WorkSpaces のコンピュータ名は WORKSPA-*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。
   > - <RegisteredOrganization> と <RegisteredOwner> はいずれも必須の値です。

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. Windows 10 を使用している場合は、<settings pass="specialize"> セクションで <ComputerName>*</ComputerName> のコメントを解除します。Windows 11 を使用している

場合は、このセクションのコメントを解除する必要はありません。<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 のドキュメントの「ComputerName」をご参照ください。

3. <settings pass="specialize"> セクションには、Windows 10 の場合も Windows 11 の場合も <RegisteredOrganization> フィールドが表示されます。<RegisteredOwner> タグは、デフォルトでは Windows 10 にのみ表示されます。Windows 11 を使用している場合は、このタグを追加する必要があります。<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>、**EC2** に <RegisteredOwner> を指定した場合、カスタムバンドルから作成された WorkSpaces 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。
   > - <RegisteredOrganization> と <RegisteredOwner> はいずれも必須の値です。

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 WorkSpaces でのみ使用できます。Linux WorkSpace からイメージを作成する場合は、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 に進みます。

Windows WorkSpace がイメージ作成の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。

> **Important**
>
> - WorkSpace は、Image Checker によって実行されるすべてのテストに合格した後に、イメージの作成に使用できます。
> - Image Checker を実行する前に、WorkSpace に最新の Windows セキュリティと累積更新プログラムがインストールされていることを確認します。

Image Checker を入手するには、以下のいずれかを実行します。

- WorkSpace を再起動します。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 から Amazon WorkSpaces Image Checker をダウンロードし、`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、[Run (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、テストの失敗と警告の原因となる問題を解決し、WorkSpace がすべてのテストに合格するまで Image Checker の実行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. WorkSpace 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。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ことが必要

最新バージョンの Microsoft Windows PowerShell をインストールします。

> **Important**
>
> WorkSpace の PowerShell 実行ポリシーは、RemoteSigned スクリプトを許可するように設定する必要があります。実行ポリシーを確認するには、Get-ExecutionPolicy PowerShell コマンドを実行します。実行ポリシーが Unrestricted または RemoteSigned に設定されていない場合は、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 設定では、イメージの作成に必要な Amazon WorkSpaces でスクリプトを実行できます。

### C および D ドライブのみが存在できる

イメージの作成に使用される WorkSpace には、C および D ドライブのみが存在できます。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 の累積的な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 のイメージ作成プロセスでサポートされます。

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 サポート 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 WorkSpaces では、ユーザープロファイル (`D:\Users\`*`username`*) は合計で 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 WorkSpaces では、ドライブ C には 12 GB 以上の空き容量が必要です。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 WorkSpaces では、FAILED メッセージが表示され、ディスク容量が 2 GB を超えている場合は、無視できます。

ドメインアカウントで実行できるサービスがない

イメージ作成プロセスを実行するために、WorkSpace にドメインアカウントで実行できるサービスがありません。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] を選択してください。

### DHCP を使用するように WorkSpace を設定することが必要

静的 IP アドレスの代わりに DHCP を使用するように、WorkSpace のすべてのネットワークアダプター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] を選択してください。
9. WorkSpace 上のすべてのネットワークアダプターに対してこのプロセスを繰り返します。

### 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] を選択してください。

### ユーザープロファイルが存在することが必要

イメージの作成に使用する WorkSpace には、ユーザープロファイル (`D:\Users\`*`username`*) が必要です。このテストに失敗した場合は、AWS サポート 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のパスに、System32 と Windows PowerShell のエントリがありません。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] を選択してください。
7. WorkSpace を再起動します。

> **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ために、WorkSpace の環境変数のパスを、新しく作成された WorkSpace または新しい Windows インスタンスのパスと比較できます。

### 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] を選択してください。

### 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] を選択してください。

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。

WorkSpace に存在できるユーザープロファイルは 1 つのみ

イメージの作成に使用している WorkSpace に存在できる WorkSpaces ユーザープロファイル (`D:\Users\username`) は 1 つのみです。WorkSpace の対象ユーザーに属していないユーザープロファイルを削除します。

イメージの作成用に、WorkSpace に 3 つのユーザープロファイルのみを含めることができます。

- WorkSpace の対象ユーザーのユーザープロファイル (`D:\Users\username`)
- 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、および対象の WorkSpaces ユーザー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、その追加の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、WorkSpace に属していない他のプロファイルを削除します。

6. [OK] を 2 回選択し、コントロールパネルを閉じます。
7. WorkSpace を再起動します。

### 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、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を行っていない WorkSpace 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

Image Checker で実行されるすべてのテストに WorkSpace が合格したにもかかわらず、WorkSpace からイメージを作成できない場合は、以下の点を確認します。

- WorkSpace が Domain Guests 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、以下の 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をコピーしているときに問題が発生した場合は、以下の点を確認します。
  - 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。イメージを作成しようとする前に、継承がブロックされて GPO が適用されていない新しい組織単位 (OU) に、WorkSpace 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] を選択してください。

## 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. 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。

2. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
3. ナビゲーションペインで [WorkSpaces] を選択します。
4. WorkSpace を選択して詳細ページを開き、[Create image] (イメージ) の作成を選択します。WorkSpace の状態が [Stopped] (停止) の場合、[Actions] (アクション)、[Start WorkSpaces] (WorkSpaces の起動) の順に選択してから、[Actions] (アクション)、[Create Image] (イメージの作成) を選択する必要があります。

   > **Note**
   >
   > プログラムによって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」の「CreateWorkspaceImage」を参照してください。

5. 続行する前に WorkSpace を再起動するように求めるメッセージが表示されます。WorkSpace を再起動すると、Amazon WorkSpaces ソフトウェアが最新バージョンに更新されます。

   メッセージを閉じて、WorkSpaces Personal の WorkSpace を再起動する のステップに従って WorkSpace を再起動します。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、WorkSpace のステータスが [利用可能]で、変更の状態が [なし] 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。イメージが作成されている間、WorkSpace のステータスは [Suspended (停止)] となり、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「-」を使用しないでください。使用する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。WorkSpace のステータスが [Available] (使用可能) に変わると、イメージは完成です (これには最長 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 リファレンスの CreateWorkspaceBundle 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。

   - [Bundle hardware type] (バンドルハードウェアタイプ) で、このカスタムバンドルから WorkSpaces を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、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、WorkSpace の起動後はルートやユーザーボリュームのサイズを縮小できなくなります。代わりに、WorkSpace を起動するときに、これらのボリュームの最小サイズを指定してください。
     >
     > - Value、Standard、Performance、Power、PowerPro のいずれかの WorkSpace は、最小 80 GB のルートボリュームおよび 10 GB のユーザーボリュームで起動できます。
     > - GeneralPurpose.4xlarge または GeneralPurpose.8xlarge WorkSpace を起動できます。ルートボリュームの場合は 175GB、ユーザーボリュームの場合は 100 GB 以上です。

- Graphics.g4dn、GraphicsPro.g4dn、Graphics、GraphicsPro WorkSpace は、最小 100 GB のルートボリュームおよび 100 GB のユーザーボリュームで起動できます。

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アイテム

Windows 7、Windows 10、または Windows 11 の WorkSpace からイメージを作成すると、C ドライブの内容全体が含まれます。

Windows 10 または 11 の WorkSpaces の場合、`D:\Users\`*`username`* のユーザープロファイルはカスタムイメージに含まれません。

Windows 7 WorkSpaces の場合、以下のものを除いて、`D:\Users\`*`username`* のユーザープロファイルの内容全体が含まれます。

- 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 WorkSpace からイメージを作成すると、ユーザーボリューム (/home) の内容はすべて削除されます。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/lib/AccountsService/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

## WorkSpaces Personal のカスタムバンドルを更新する

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/v2/home「https://www.com」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、WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する を参照してください。
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、「WorkSpaces Personal の WorkSpace を再構築する」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 Personal でカスタムイメージをコピーする

リージョン内または AWS 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、イメージを他のリージョンにコピーするには、 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 Personal でカスタムイメージを共有または共有解除する 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 のクォータ 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 () の copy-workspace-image コマンドを使用しますAWS CLI。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、そのイメージが正しい 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/v2/home://www.com」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 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 Personal で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 Personal でカスタムイメージを共有または共有解除する

同じ AWS リージョン内の AWS アカウント間でカスタム WorkSpaces イメージを共有できます。イメージが共有されると、受信者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 Personal でカスタムイメージをコピーする 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 リージョン内のイメージ数のクォータが適用されます。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 のクォータ 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 アカウントでのみ共有できます。BYOL イメージを共有する AWS アカウントは、 (同じ支払者アカウントで) 組織の一部である必要があります。

> **Note**
>
> AWS アカウント間での BYOL イメージの共有は、現時点では AWS GovCloud (米国西部) および AWS GovCloud (米国東部) リージョンではサポートされていません。 AWS GovCloud (米国西部) リージョンと 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には、 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、AWS コマンドラインインターフェイス (CLI) で DescribeWorkSpaceImages および DescribeWorkspaceImagePermissions API オペレーションを使用するか、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/v2/home「https://www.com」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/v2/home「https://www.com」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で、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、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

プログラムでイメージを共有または共有解除するには、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 Personal で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、最初にバンドルに基づくすべての WorkSpaces を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/v2/home「https://www.com」で WorkSpaces 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 リファレンスの DeleteWorkspaceBundle を参照してください。

> **Note**
>
> バンドルを削除した後で同じ名前の新しいバンドルを作成する場合は、削除してから少なくとも 2 時間待ってください。

## 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/v2/home「https://www.com」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、[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 リファレンスの DeleteWorkspaceImage を参照してください。

# WorkSpaces Personal のモニタリング

WorkSpaces をモニタリングするには、次の機能を使用することができます。

CloudWatch メトリクス

Amazon WorkSpaces は、WorkSpaces に関するデータポイントを Amazon CloudWatch に発行します。CloudWatch では、それらのデータポイントについての統計を、(メトリクスと呼ばれる) 順序付けられた時系列データの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 が正常に実行されていることを確認できます。詳細については、「」を参照してくださいCloudWatch メトリクスを使用した WorkSpaces のモニタリング

CloudWatch Events

ユーザーが WorkSpaces にログインするときに Amazon WorkSpaces から Amazon CloudWatch Events にイベントを送信できます。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、「」を参照してくださいAmazon EventBridge を使用して WorkSpace をモニタリングする

CloudTrail ログ

AWS CloudTrail は、WorkSpaces でユーザー、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記録を提供します。CloudTrail で収集された情報を使用して、WorkSpaces に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、CloudTrail.logs を使用した WorkSpaces API コールのログ記

録」を参照してください。スマートカードユーザーのサインインイベントの成功と失敗。 AWS CloudTrail 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について」を参照してください。

CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor は、インターネットの問題が、 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の間のパフォーマンス 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 は、次の目的にも使用できます。

- 1 つ以上の WorkSpace ディレクトリのモニターを作成する。
- 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 (ロケーションと ASN (通常はインターネットサービスプロバイダー (ISP)) と WorkSpace リージョン間の問題に関するアラームを取得する。

Internet Monitor は、グローバルネットワークフットプリントから AWS キャプチャされた接続データを使用して、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のベースラインを計算します。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。

Amazon S3 アクセスログ

ユーザーがアプリケーション設定データまたはホームフォルダのデータを Amazon S3 バケットに保存している場合は、Amazon S3 サーバーアクセスログを表示してアクセスをモニタリングすることを検討してください。これらのログでは、バケットに対して行われたリクエストの詳細なレコードが提供されます。サーバーアクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 Server Access Logging」を参照してください。

## CloudWatch 自動ダッシュボードを使用して WorkSpaces の状態をモニタリングする

CloudWatch 自動ダッシュボードを使って WorkSpaces 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て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、特定のしきい値を監視するアラームを設定し、これらの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 CloudWatch ユーザーガイド」を参照してください。

AWS アカウントを使用して WorkSpaces 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。ダッシュボードを使用すると、状態やパフォーマンスなどの WorkSpaces のメトリクスを、リージョンをまたいでモニタリングできます。ダッシュボードは、次の目的でも使用できます。

- 異常な WorkSpace インスタンスを特定する。
- WorkSpace インスタンスに異常がある実行モード、プロトコル、オペレーティングシステムを特定する。
- 時間の経過に伴う重要なリソースの使用率を表示する。
- トラブルシューティングに役立つ異常を特定する。

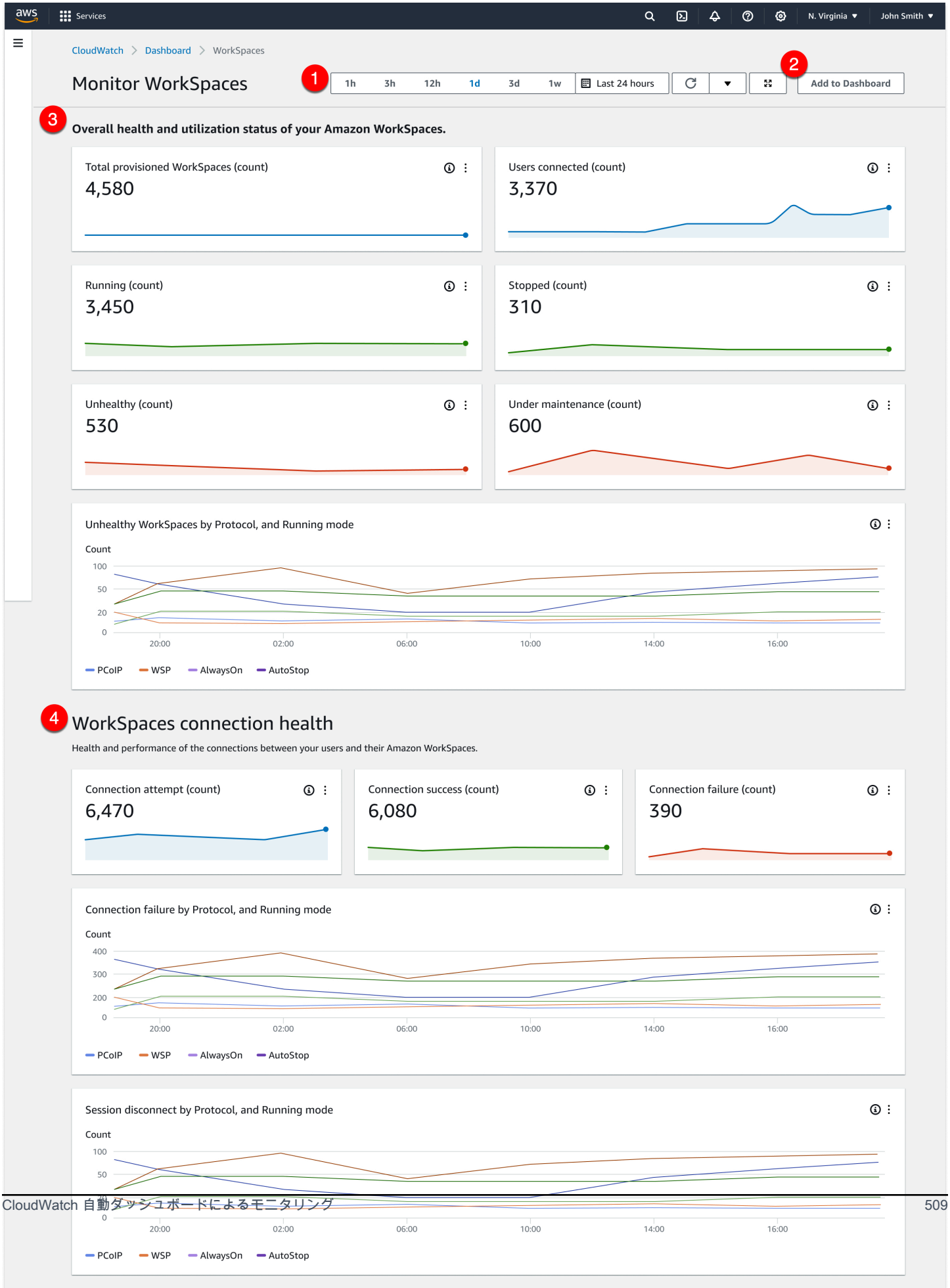
WorkSpaces CloudWatch 自動ダッシュボードは、すべての AWS 商用リージョンで利用できます。

WorkSpaces の CloudWatch 自動ダッシュボードを使用するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) 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. [WorkSpaces] を選択します。

## WorkSpaces の CloudWatch 自動ダッシュボードについて

CloudWatch 自動ダッシュボードでは、WorkSpaces の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、次の機能で構成されます。

1. 時間および日付範囲コントロールを使用して履歴データを表示する。
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する。
3. 以下を実行して、WorkSpaces の全体的な状態と使用率のステータスをモニタリングする。
    a. プロビジョニングされた WorkSpaces の合計数、接続されたユーザー数、異常および正常な WorkSpace インスタンスの数を表示する。
    b. 異常な WorkSpaces と、そのさまざまな変数 (プロトコルやコンピューティングモードなど) を表示する。
    c. 折れ線グラフにカーソルを合わせて、特定のプロトコルと実行モードでの一定期間における正常/異常な WorkSpace インスタンスの数を表示する。
    d. 省略記号メニューを選択し、[メトリクスで表示] を選択して、タイムスケールチャートでメトリクスを表示する。
4. 指定した時点での WorkSpaces 環境の接続メトリクスとそのさまざまな変数 (接続試行回数、成功した接続の回数、失敗した接続の回数など) を表示する。
5. ラウンドトリップタイム (RTT) など、ユーザーのエクスペリエンスに影響を与えるセッション内レイテンシーを表示して、接続の正常性とパケット損失を特定し、ネットワークの状態をモニタリングする。
6. ホストのパフォーマンスとリソース使用率を表示して、潜在的なパフォーマンスの問題を特定し、トラブルシューティングを行う。

## CloudWatch メトリクスを使用した WorkSpaces のモニタリング

WorkSpaces と Amazon CloudWatch が統合され、パフォーマンスメトリクスを収集して分析できるようになりました。これらのメトリクスは、CloudWatch コンソールまたは CloudWatch コマンドラインインターフェイスを使用して、あるいはプログラムによって CloudWatch API を使用してモニタリングできます。CloudWatch では、メトリックスの指定したしきい値に到達したときのアラームを設定することもできます。

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

前提条件

CloudWatch メトリクスを取得するには、us-east-1 リージョン にある AMAZON サブセットの ポート 443 へのアクセスを有効にします。詳細については、「」を参照してくださいWorkSpaces Personal の IP アドレスとポートの要件

目次



## 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] | 正常な状態を返した WorkSpaces の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | カウント |
| Unhealthy [1] | 正常でない状態を返した WorkSpaces の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>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<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | カウント |
| ConnectionSuccess [2] | 成功した接続の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>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<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | カウント |
| SessionLaunchTime [2、6] | WorkSpaces セッションを開始するためにかかる時間。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | 秒 (時間) |
| InSessionLatency [2、6] | WorkSpaces クライアントと WorkSpaces 間のラウンドトリップ時間。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>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<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | カウント |
| UserConnected [3] | ユーザーが接続されている WorkSpaces の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Sum、Maximum、Minimum、Data Samples | カウント |
| Stopped | 停止中の WorkSpaces の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>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] | メンテナンス中の WorkSpaces の数。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>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 | 使用された CPU リソースの割合。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum | 割合 (%) |
| MemoryUsage | マシンのメモリの使用率。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum | 割合 (%) |
| RootVolumeDiskUsage | ルートディスクボリュームの使用率。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum | 割合 (%) |

| メトリクス | 説明 | ディメンション | 統計 | 単位 |
| --- | --- | --- | --- | --- |
| UserVolumeDiskUsage | ユーザーディスクボリュームの使用率。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum | 割合 (%) |
| UDPPacketLossRate [7] | クライアントとゲートウェイの間でドロップしたパケットの割合。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum、Data Samples | 割合 (%) |
| UpTime | WorkSpace の最後の再起動からの時間。 | DirectoryId<br>WorkspaceId<br>RunningMode<br>Protocol<br>ComputeType<br>BundleId<br>UserName | Average、Maximum、Minimum、Data Samples | [秒] |

[1] WorkSpacesは定期的にステータスリクエストを WorkSpaces に送信します。WorkSpaces は、これらのリクエストに応答すると `Available` とマークされ、リクエストに応答できないと `Unhealthy` とマークされます。これらのメトリクスは WorkSpaces レベルの粒度で利用でき、組織のすべての WorkSpaces で集計されます。

[2] WorkSpaces は、各 WorkSpaces に対して行われた接続のメトリクスを記録します。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で出力されます。メトリクスは WorkSpaces レベルの粒度で利用でき、ディレクトリのすべての WorkSpaces で集計されます。

[3] WorkSpaces は定期的に接続ステータスのリクエストを WorkSpaces に送信します。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 WorkSpaces レベルの粒度で利用でき、組織のすべての WorkSpaces で集計されます。

[4] このメトリクスは、AutoStop 実行モードで設定された WorkSpaces に適用されます。WorkSpaces のメンテナンスを有効にしている場合、このメトリクスは、現在メンテナンス中の WorkSpaces の数を記録します。このメトリクスは、WorkSpaces レベルの粒度で利用でき、WorkSpaces がメンテナンスに入った時期と削除された時期を示します。

[5] ディレクトリに対して信頼されたデバイスの機能が有効になっている場合、Amazon WorkSpaces は証明書ベースの認証を使用して、デバイスが信頼されているかどうかを判断します。ユーザーが自分の WorkSpaces にアクセスしようとすると、これらのメトリクスが出力され、信頼されたデバイスの認証が成功したか失敗したかが示されます。これらのメトリクスは、Amazon WorkSpaces の Windows と MacOS クライアントアプリケーションでのみ、ディレクトリレベルの粒度で使用できます。

[6] WorkSpaces Web Access ではご利用いただけません。

[7] このメトリクスは、パケットの平均損失を測定します。

- PCoIP: クライアントからゲートウェイへの UDP パケットの平均損失を測定します。

  > **Note**
  >
  > これはゲートウェイで測定されます。

- DCV: ゲートウェイからクライアントへの UDP パケットの損失を測定します。

> **Note**
>
> これはゲートウェイで測定されます。

## WorkSpaces メトリッ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` | 指定したディレクトリの WorkSpaces に、メトリクスデータをフィルタリングします。ディレクトリ ID の形式は `d-XXXXXXXXXX` です。 |
| `WorkspaceId` | 指定した WorkSpaces に対してメトリクスデータをフィルタリングします。WorkSpaces ID の形式は `ws-XXXXXXXXXX` です。 |
| `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 WorkSpaces の実行モード別にフィルタリングします。実行モードの形式は AutoStop または AlwaysOn です。 |
| `BundleId` | メトリクスデータを WorkSpaces のプロトコル別にフィルタリングします。バンドルの形式は `wsb-XXXXXXXXXX` です。 |
| `ComputeType` | メトリクスデータを WorkSpaces のコンピューティングタイプ別にフィルタリングします。 |
| `Protocol` | メトリクスデータを WorkSpaces のプロトコルタイプ別にフィルタリングします。 |

| ディメンション | 説明 |
| --- | --- |
| UserName | メトリクスデータを WorkSpaces のユーザー名別にフィルタリングします。<br><br>**Note**<br>UserName に次のような非 ASCII 文字を使うことはできません。<br>• アクセント文字: é、à、ö、ñ など。<br>• 非ラテン文字<br>• 記号: ©#、®#、€、£、µ、¥ など。 |

## 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、ディレクトリ内のどの WorkSpaces 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、指定したディレクトリの WorkSpaces 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、ディレクトリ内の各 WorkSpaces の CloudWatch メトリクスを取得します。

```
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 EventBridge を使用して WorkSpace をモニタリングする

Amazon WorkSpaces のイベントを使用することで、WorkSpaces への正常なログインを表示、検索、ダウンロード、アーカイブ、分析し、これに対して応答することができます。たとえば、次の目的でイベントを使用できます。

- 後に参照できるよう WorkSpaces の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て、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のログイン元を特定し、ポリシーを使用して、`WorkSpaces Access` のイベントタイプで見つかったアクセス基準を満たす WorkSpaces のファイルまたはデータにのみアクセスすることを許可します。
- 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 への接続に使用される WorkSpaces クライアントのバージョンを確認します。

Amazon WorkSpaces は、ベストエフォートベースでこれらのイベントを発行します。EventBridge からのイベントは、ほぼリアルタイムに EventBridge に提供されます。EventBridge では、イベントに応答し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

ユーザーが正常に WorkSpace にログインすると、WorkSpaces クライアントアプリケーションが `WorkSpaces Access` イベントを送信します。これらのイベントは、すべての WorkSpaces クライアントより送信されます。

DCV を使用して WorkSpaces に対して発行されるイベントには、バージョン 4.0.1 以降の WorkSpaces クライアントアプリケーションが必要です。

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`

ユーザーが WorkSpaces にログインした時間。

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

WorkSpaces のディレクトリの識別子。`domain/` にはディレクトリ識別子を前置する必要があります。例えば、`"domain/d-123456789"` と指定します。

`clientVersion`

WorkSpaces への接続に使用される WorkSpaces クライアントのバージョン。

`workspaceId`

WorkSpaces の識別子。

## WorkSpaces イベントを処理するルールを作成する

WorkSpaces イベントを処理する ルールを作成するには、次の手順を使用します。

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] を選択してください。
3. [トピックの作成] を選択してください。
4. [Type (タイプ)] で、[Standard (標準)] を選択してください。
5. [Name] (名前) で、トピックの名前を入力してください。
6. [トピックの作成] を選択してください。
7. [Create subscription] を選択してください。
8. [Protocol (プロトコル)] として [Email (E メール)] を選択してください。
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てください。
10. [Create subscription] を選択してください。
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. Amazon EventBridge コンソールの https://console.aws.amazon.com/events/ を開いてください。
2. [Create rule] を選択してください。
3. [Name] (名前) に、ルールの名前を入力してください。
4. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
5. [Next] を選択してください。
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 を選択してください。
   b. [AWS のサービス] で、[WorkSpaces] を選択します。

c. [イベントタイプ] で、[WorkSpaces Access] (WorkSpaces のアクセス) 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. [Next (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] を選択してください。

b. [Select a target] (ターゲットの選択) には[SNS topic] (SNS トピック) を選択してください。

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. [Next (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. [Next] を選択してください。

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について

AWS CloudTrail は、スマートカードユーザーのサインインイベントの成功と失敗を記録します。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` | ユーザーが特定の認証情報のチャレンジを解決するよう AWS リクエストしたことを に通知し、`CredentialType` 必要な を指定します (例: ""CARD)。 |
| `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 |

| イベント名 | イベントの目的 |
| --- | --- |
| | 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) |
| 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 | UserAuthentication | "LoginTo": "https://skylight.local“ |

| 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 |
| --- | --- | --- | --- |
| | は口グに記録されません。 | | |

## 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。

内容

- スマートカードを使用した認証での正常なサインイン
- 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

### 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"
    }
}
```

# AWS CloudFormation テンプレートを使用してカスタム CloudWatch ダッシュボードを作成する

AWS には、WorkSpaces のカスタム CloudWatch ダッシュボードを作成するために使用できる AWS CloudFormation テンプレートが用意されています。コンソールで WorkSpaces のカスタムダッシュボードを作成するには、次の AWS CloudFormation テンプレートオプションから選択します AWS CloudFormation 。

## 開始する前に考慮すべき点

カスタム CloudWatch ダッシュボードの作成を開始する前に、次の点を考慮してください。

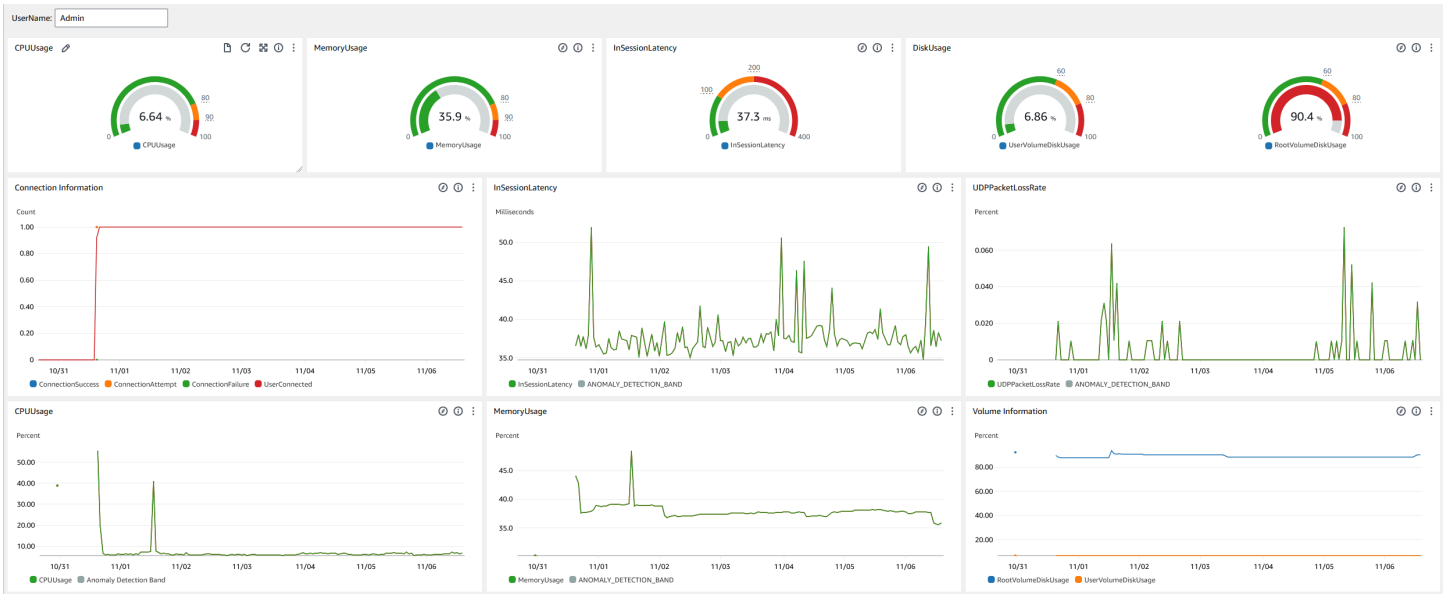
- モニタリングするデプロイされた WorkSpaces AWS リージョン と同じ にダッシュボードを作成します。
- CloudWatch コンソールを使用してカスタムダッシュボードを作成することもできます。
- コストは、カスタム CloudWatch ダッシュボードに関連付けられる場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

## ヘルプデスク用ダッシュボード

ヘルプデスク用ダッシュボードには、特定の WorkSpace の次のメトリクスが表示されます。

- CPU の使用
- メモリ使用量
- セッション内レイテンシー
- ルートボリューム
- ユーザーボリューム
- パケットロス
- ディスク使用量

以下は、ヘルプデスク用ダッシュボードの例です。




AWS CloudFormationを使用して CloudWatch でカスタムダッシュボードを作成するには、次の手順を実行します。

1. AWS CloudFormation コンソールでスタックの作成ページを開きます。このリンクをクリックすると、ヘルプデスク用カスタム CloudWatch ダッシュボードテンプレートの Amazon S3 バケットの場所があらかじめ入力された状態で、ページが開きます。
2. [スタックの作成] ページでデフォルトの選択を確認します。Amazon S3 URL フィールドには、AWS CloudFormation テンプレートの Amazon S3 バケットの場所が事前に入力されていることに注意してください。
3. [Next (次へ)] を選択します。
4. [スタック名] ボックスに、スタックの名前を入力します。

   スタック名は、スタックのリストから特定のスタックを見つけるために役立つ識別子です。スタック名には、英数字 (大文字と小文字が区別されます) とハイフンのみを使用できます。先頭の文字はアルファベット文字である必要があります。また、128 文字より長くすることはできません。
5. [ダッシュボード名] テキストボックスに、ダッシュボードに付ける名前を入力します。

   ダッシュボード名には、英数字、ダッシュ (-)、アンダースコア (_) のみを使用できます。
6. [Next (次へ)] を選択します。
7. [スタックオプションの設定] ページでデフォルトの選択内容を確認し、[次へ] を選択します。

8. [変換では、アクセス機能が必要になる場合があります] まで下にスクロールし、確認のチェックボックスをオンにします。次に、[送信] を選択してスタックとカスタム CloudWatch ダッシュボードを作成します。

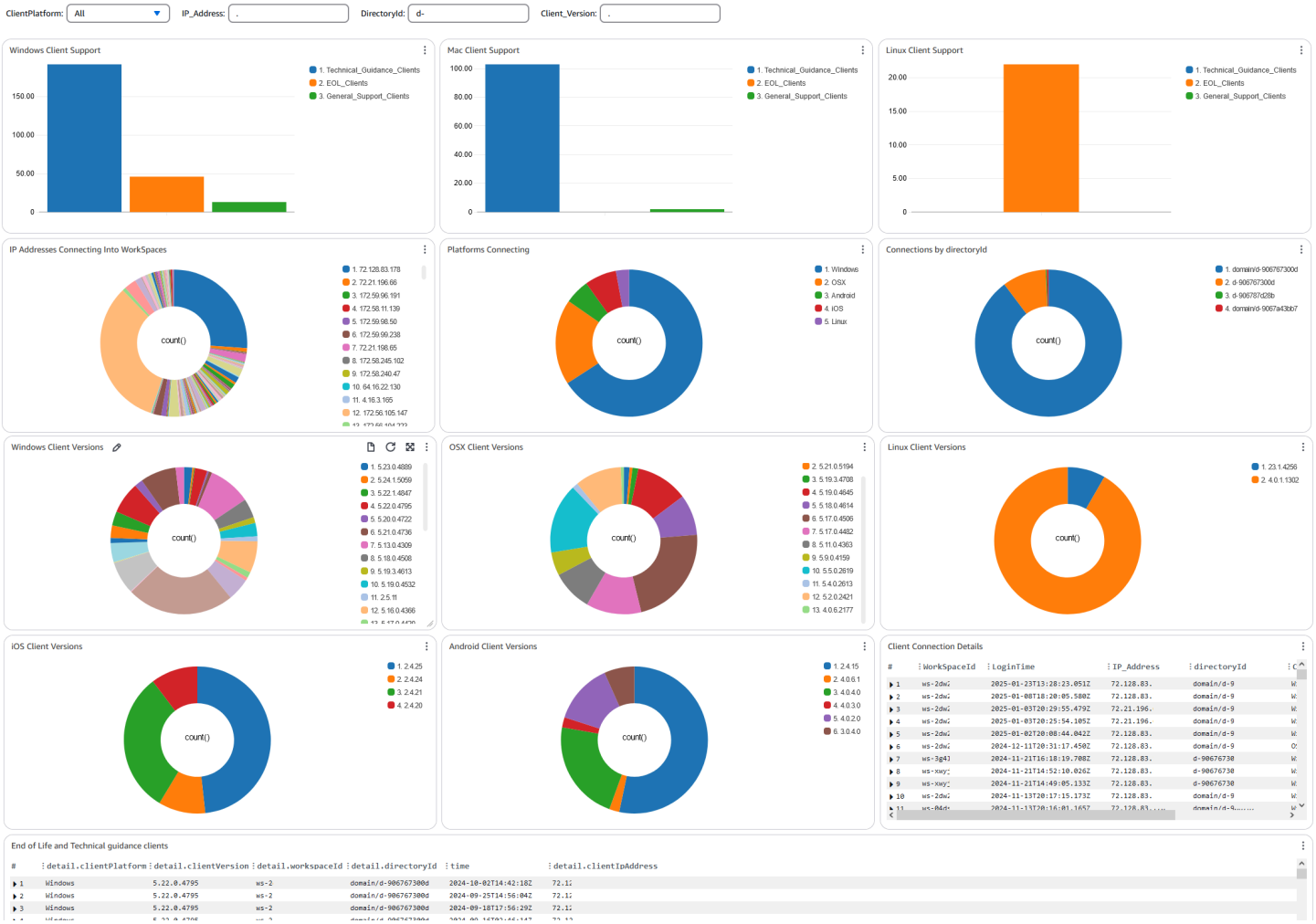
> **Important**
>
> コストは、カスタム CloudWatch ダッシュボードに関連付けられる場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

9. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
10. 左のナビゲーションバーの [ダッシュボード] を選択します。
11. [カスタムダッシュボード] で、この手順の前半で入力したダッシュボード名を持つダッシュボードを選択します。
12. ヘルプデスクのサンプルテンプレートを使用して、WorkSpace の UserName を入力してデータをモニタリングします。

## 接続インサイト用ダッシュボード

接続インサイト用ダッシュボードには、WorkSpaces に接続されているクライアントバージョン、プラットフォーム、IP アドレスが表示されます。このダッシュボードを使用すると、ユーザーがどのように接続しているかをよく理解できるため、古いクライアントを使用しているユーザーに対して事前に通知できます。動的変数を使用することで、IP アドレスまたは特定のディレクトリの詳細を監視できます。

以下は、接続インサイト用ダッシュボードの例です。




AWS CloudFormationを使用して CloudWatch でカスタムダッシュボードを作成するには、次の手順を実行します。

1. AWS CloudFormation コンソールでスタックの作成ページを開きます。このリンクをクリックすると、接続インサイト用カスタム CloudWatch ダッシュボードテンプレートの Amazon S3 バケットの場所があらかじめ入力された状態で、ページが開きます。
2. [スタックの作成] ページでデフォルトの選択を確認します。Amazon S3 URL フィールドには、AWS CloudFormation テンプレートの Amazon S3 バケットの場所が事前に入力されていることに注意してください。
3. [Next (次へ)] を選択します。
4. [スタック名] ボックスに、スタックの名前を入力します。

   スタック名は、スタックのリストから特定のスタックを見つけるために役立つ識別子です。スタック名には、英数字 (大文字と小文字が区別されます) とハイフンのみを使用できます。先頭

の文字はアルファベット文字である必要があります。また、128 文字より長くすることはできません。

5. [ダッシュボード名] テキストボックスに、ダッシュボードに付ける名前を入力します。関連する他の CloudWatch アクセスグループの設定情報を入力します。

   ダッシュボード名には、英数字、ダッシュ (-)、アンダースコア (_) のみを使用できます。

6. [ログの保持期間] で、LogGroup を保持する日数を入力します。
7. [EventBridge の設定] で、WorkSpaces のアクセスログを取得するために EventBridge ルールをデプロイするかどうかを選択します。
8. [WorkSpace アクセスログ名] に、WorkSpace アクセスログを持つ CloudWatch LogGroup の名前を入力します。
9. [Next (次へ)] を選択します。
10. [スタックオプションの設定] ページでデフォルトの選択内容を確認し、[次へ] を選択します。
11. [変換では、アクセス機能が必要になる場合があります] まで下にスクロールし、確認のチェックボックスをオンにします。次に、[送信] を選択してスタックとカスタム CloudWatch ダッシュボードを作成します。

> **Important**
>
> コストは、カスタム CloudWatch ダッシュボードに関連付けられる場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

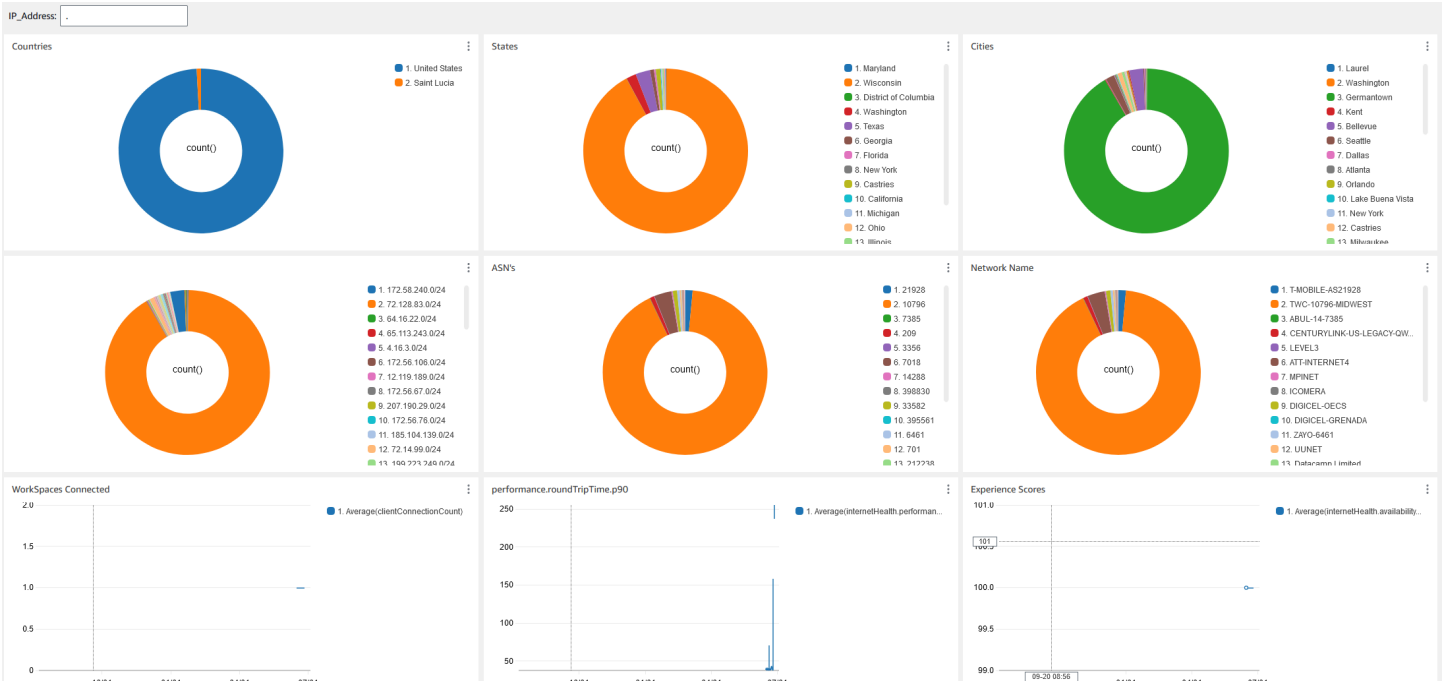
12. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
13. 左のナビゲーションバーの [ダッシュボード] を選択します。
14. [カスタムダッシュボード] で、この手順の前半で入力したダッシュボード名を持つダッシュボードを選択します。
15. これで、接続インサイト用ダッシュボードを使用して WorkSpaces のデータをモニタリングできるようになりました。

## インターネットモニタリング用ダッシュボード

インターネットモニタリング用ダッシュボードには、ユーザーが WorkSpaces インスタンスに接続するときに使用するインターネットサービスプロバイダー (ISP) の詳細が表示されます。都市、州、ASN、ネットワーク名、接続された WorkSpaces の数、パフォーマンス、エクスペリエンスス

コアに関する詳細を提供します。特定の IP アドレスを使用して、特定の場所から接続しているユーザーの詳細を取得することもできます。CloudWatch Internet Monitor をデプロイして ISP データ情報を取得します。詳細については、「Amazon CloudWatch Internet Monitor の使用」を参照してください。

以下は、インターネットモニタリング用ダッシュボードの例です。




を使用して CloudWatch でカスタムダッシュボードを作成するには AWS CloudFormation

> **Note**
>
> カスタムダッシュボードを作成する前に、CloudWatch Internet Monitor でインターネットモニターを作成してください。詳細については、「コンソールを使用して Amazon CloudWatch Internet Monitor でモニターを作成する」を参照してください。

1. AWS CloudFormation コンソールでスタックの作成ページを開きます。このリンクをクリックすると、インターネットモニタリング用カスタム CloudWatch ダッシュボードテンプレートの Amazon S3 バケットの場所があらかじめ入力された状態で、ページが開きます。
2. [スタックの作成] ページでデフォルトの選択を確認します。Amazon S3 URL フィールドには、AWS CloudFormation テンプレートの Amazon S3 バケットの場所が事前に入力されていることに注意してください。
3. [Next (次へ)] を選択します。

4. [スタック名] ボックスに、スタックの名前を入力します。

   スタック名は、スタックのリストから特定のスタックを見つけるために役立つ識別子です。スタック名には、英数字 (大文字と小文字が区別されます) とハイフンのみを使用できます。先頭の文字はアルファベット文字である必要があります。また、128 文字より長くすることはできません。

5. [ダッシュボード名] テキストボックスに、ダッシュボードに付ける名前を入力します。関連する他の CloudWatch アクセスグループの設定情報を入力します。

   ダッシュボード名には、英数字、ダッシュ (-)、アンダースコア (_) のみを使用できます。

6. [監視するリソース] で、インターネットモニタリングを有効にしたディレクトリのディレクトリ ID を入力します。
7. [モニター名] で、使用するインターネットモニターの名前を入力します。
8. [Next (次へ)] を選択します。
9. [スタックオプションの設定] ページでデフォルトの選択内容を確認し、[次へ] を選択します。
10. [変換では、アクセス機能が必要になる場合があります] まで下にスクロールし、確認のチェックボックスをオンにします。次に、[送信] を選択してスタックとカスタム CloudWatch ダッシュボードを作成します。

    > **Important**
    >
    > コストは、カスタム CloudWatch ダッシュボードに関連付けられる場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

11. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
12. 左のナビゲーションバーの [ダッシュボード] を選択します。
13. [カスタムダッシュボード] で、この手順の前半で入力したダッシュボード名を持つダッシュボードを選択します。
14. これで、インターネットモニタリング用ダッシュボードを使用して WorkSpaces のデータをモニタリングできるようになりました。

# WorkSpaces Personal のビジネス継続性

Amazon WorkSpaces は、 AWS リージョンとアベイラビリティーゾーンに編成された 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、「」を参照してくださいAmazon WorkSpaces の耐障害性

Amazon WorkSpaces 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 が利用できない場合に WorkSpaces ユーザーを別の WorkSpaces にリダイレクトする機能であるクロスリージョンリダイレクトも提供します。たとえば、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の WorkSpaces にアクセスできない場合に、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、メンテナンス期間中のトラフィックのディストリビューションや代替の WorkSpaces の提供など、他の目的に使用することもできます。DNS 設定に Amazon Route 53 を使用する場合は、Amazon CloudWatch アラームを監視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 WorkSpaces リージョンに自動化された冗長的な仮想デスクトップインフラストラクチャを提供し、プライマリリージョンが障害でアクセス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処理を合理化します。

WorkSpaces マルチ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すると、セカンダリ WorkSpaces リージョンに冗長的な仮想デスクトップインフラストラクチャをデプロイし、破壊的なイベントに備えた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、トラフィックのディストリビューションや、メンテナンス期間中の代替の WorkSpaces の提供など、他の目的に使用することもできます。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



## WorkSpaces Personal のクロスリージョンリダイレクト

Amazon WorkSpaces 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。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 が利用できない場合に WorkSpaces ユーザーを別の WorkSpaces にリダイレクトします。たとえば、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 リージョンの WorkSpaces にア

クセスできない場合に、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、トラフィックのディストリビューションや、メンテナンス期間中の代替の WorkSpaces の提供など、他の目的に使用することもできます。DNS 設定に Amazon Route 53 を使用する場合は、Amazon CloudWatch アラームを監視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 つの (またはそれ以上) AWS リージョンでユーザーの WorkSpaces 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、こ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により、WorkSpaces ユーザーはフェイルオーバーリージョンで設定した WorkSpaces にリダイレクトされます。

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

- ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する
- クロスリージョンリダイレクトアーキテクチャ図
- クロスリージョンリダイレクトを開始する
- クロスリージョンリダイレクト時の動作
- 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
- 接続エイリアスの共有を解除する
- 接続エイリアスを削除する
- 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
- 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

## 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 WorkSpaces とともに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。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、WorkSpaces 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 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連携して動作し、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各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、ユーザー用の WorkSpaces を作成します。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 ユーザーデータの同期を維持するには、AD Connector を使用して、ユーザー用に WorkSpaces を設定した各リージョンで同じ Active Directory をポイントすることをお勧めします。WorkSpaces の作成の詳細については、「WorkSpaces の起動」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と、Amazon WorkSpaces で使用できるようにプライマリリージョンのディレクトリのみを登録できます。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 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内の 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にリージョンベースの登録コード (`WSpdx+ABC12D` など) 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 WorkSpace 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がユーザーに自動的に送信されます。つまり、フェイルオーバーリージョンでユーザー用に WorkSpaces を設定すると、これらのフェイルオーバー WorkSpaces の E メールも自動的に受信されます。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

- クロスリージョンリダイレクトでは、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、WorkSpaces を別のリージョンにフェイルオーバーします。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、プライマリリージョンで 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た Amazon Route 53 フェイルオーバー DNS ルーティングポリシーを使用できます。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によって、WorkSpaces ユーザーがフェイルオーバーリージョンで設定した WorkSpaces にリダイレクトされます。
- クロスリージョンリダイレクトは、バージョン 3.0.9 以降の Linux、macOS、および Windows WorkSpaces クライアントアプリケーションでのみサポートされます。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と中国 (寧夏) リージョンを除く、AWS 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/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、WorkSpaces のプライマリ 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] 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、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. 上記のステップを繰り返しますが、Step 2 では、WorkSpaces のフェイルオーバーリージョンを必ず選択してください。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で接続エイリアスを作成するには、必ず同じ AWS アカウントを使用してください。

## (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 リージョン内の他の 1 つの 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、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アカウント (アカウントまたは共有アカウント) は 1 つだけです。

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/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上で、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」の下に、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複数のリージョンの 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にすることができます。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と、米国西部 (オレゴン) リージョンに配置し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) リージョンで設定した WorkSpaces 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 (たとえば、数千マイル離れている) 場合、WorkSpaces のエクスペリエンスの反応は通常より低くなることがあります。ロケーションからさまざまな AWS リージョンへの往復時間 (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、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アカウント (アカウントまたは共有アカウント) は 1 つだけです。

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、WorkSpaces のプライマリ 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で、ディレクトリへの関連付けで、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、Amazon WorkSpaces で使用できるのはプライマリリージョンのディレクトリのみです。Amazon WorkSpaces 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内の Amazon WorkSpaces での使用はサポートされていません。

6. [Associate] を選択します。

7. 上記のステップを繰り返しますが、Step 2 では、WorkSpaces のフェイルオーバーリージョンを必ず選択してください。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の WorkSpaces 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 WorkSpaces ディレクトリとの間の関連付けの接続識別子が必要になります。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/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、WorkSpaces のプライマリ 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. 上記のステップを繰り返しますが、Step 2 では、WorkSpaces のフェイルオーバーリージョンを必ず選択してください。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監視する CloudWatch アラームも設定する必要があります。CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドの Amazon CloudWatch とは を参照してください。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状態を決定する方法および CloudWatch アラームをモニタリングする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. [監視対象] 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] のいずれかを選択します。
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、WorkSpaces でのみ使用するようにドメインを設定していない限り、`desktop` または `workspaces` などのサブドメインを使用することをお勧めします。

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によって WorkSpaces ユーザーがフェイルオーバーリージョンにリダイレクトされます。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の WorkSpaces 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 を必要に応じてリダイレクトするには、接続文字列 (FQDN) をユーザーに送信する必要があります。既に WorkSpaces ユーザーにリージョンベースの登録コード (`WSpdx+ABC12D` など) を発行している場合、これらのコードは有効なままです。ただし、クロスリージョンリダイレクトが機能するためには、WorkSpaces ユーザーが WorkSpaces クライアント

アプリケーションに WorkSpaces を登録するときに、登録コードとして接続文字列を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、新しい WorkSpace を起動するたびに、リージョンベースの登録コード (`WSpdx+ABC12D` など) が記載された招待 E メールがユーザーに自動的に送信されます。クロスリージョンリダイレクトをすでに設定している場合でも、新しい WorkSpaces 用に自動的に送信される招待 E メールには、接続文字列ではなく、このリージョンベースの登録コードが含まれています。
>
> WorkSpaces ユーザーがリージョンベースの登録コードの代わりに接続文字列を使用していることを確認するには、以下の手順に従って、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/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上隅で、WorkSpaces のプライマリ AWS リージョンを選択します。
3. ナビゲーションペインで [WorkSpaces] を選択します。
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。
5. [アクション]、[Invite User (ユーザーを招待)] の順に選択します。
6. [WorkSpaces にユーザーを招待する] 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が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では、クロスリージョンのフェイルオーバーとフォールバックのみが円滑化されます。セカンダリリージョンで WorkSpaces を容易に作成、維持できるわけではなく、クロスリージョンのデータレプリケーションも許可されません。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 WorkSpaces 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、DNS レコードを手動で更新するか、ヘルスチェックに基づく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。「Creating Disaster Recovery Mechanisms Using Amazon Route 53」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の WorkSpaces 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によって、フェイルオーバーリージョンで設定した WorkSpaces 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。この現象が発生した場合は、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、再度ログインを試みる必要があります。

## 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/v2/home 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]、[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/v2/home 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、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**
>
> WorkSpaces ユーザーの登録コードとして FQDN を使用しなくなった場合は、セキュリティ上の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/v2/home 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 を使用しなくなった場合は、潜在的なセキュリティ上の問題を防ぐために、次の予防措置を講じる必要があります。

- WorkSpaces ユーザーに WorkSpaces ディレクトリのリージョン固有の登録コード (WSpdx+ABC12D など) を発行し、登録コードとして FQDN の使用を停止するように指示してください。
- 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 ユーザーが登録コードとして FQDN を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。

# WorkSpaces Personal のマルチリージョンレジリエンス

Amazon WorkSpaces マルチリージョンレジリエンス (MRR) を使用すると、破壊的なイベントが原因でプライマリ WorkSpaces リージョンにアクセスできなくなった場合に、ユーザーをセカンダリ WorkSpaces にリダイレクトできます。ユーザーは登録コードを切り替えることなく、スタンバイ WorkSpaces にログインできます。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にユーザーディレクトリを設定したら、スタンバイ WorkSpace を作成する対象であるプライマリリージョン内の WorkSpace を選択します。システムは、プライマリ WorkSpace の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。次に、セカンダリリージョンで新しいスタンバイ WorkSpace 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 ヘルスチェック機能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。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 WorkSpaces にログインすると、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 リージョン間でユーザーをリダイレクトできます。Amazon Route 53 を使用する場合は、WorkSpaces のクロスリージョンリダイレクト戦略を確立するときに、ヘルスチェックを使用して Amazon CloudWatch アラームをモニタリングすることをお勧めします。詳細については、「Amazon Route 53 デベロッパーガイド」で 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に関する説明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の一方向にデータをレプリケートするスタンバイ WorkSpaces 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によって新しいスナップショットが定期的にチェックされ、スナップショットが見つかると、セカンダリリージョンに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、そのコピーでセカンダリ WorkSpace が更新されます。

内容

- スタンバイ WorkSpaces の一方向データレプリケーション
- 復旧用に Amazon EC2 のキャパシティー予約を計画する

## 前提条件

- スタンバイ WorkSpaces を作成する前に、プライマリリージョンにユーザー用の WorkSpaces を作成する必要があります。WorkSpaces 作成の詳細については、「WorkSpaces Personal のディレクトリを作成する」を参照してください。
- スタンバイ WorkSpaces でデータレプリケーションを有効にするには、スタンバイリージョンにレプリケートするようにセルフマネージド Active Directory または AWS Managed Microsoft AD を設定する必要があります。詳細については、AWS 「 Managed Microsoft AD ディレクトリの作成」および「レプリケートされたリージョンの追加」を参照してください。
- ENA、NVMe、PV ドライバーなど、プライマリ WorkSpaces のネットワーク依存関係ドライバーを必ず更新してください。この作業は、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)、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に関する説明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。この作業は、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 および 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ために、プライマリリージョンとセカンダリリージョンの Active Directory で FQDN、OU、ユーザー SID が同期していることを確認します。
- スタンバイ WorkSpaces のデフォルトのクォータ (制限) は 0 です。スタンバイ WorkSpace 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。詳細については、「Amazon WorkSpaces のクォータ」を参照してください。
- プライマリ WorkSpaces とスタンバイ WorkSpaces の両方の暗号化に、カスタマーマネージドキーを使用していることを確認します。単一リージョンキーとマルチリージョンキーのいずれかを使用して、プライマリおよびスタンバイ WorkSpaces を暗号化できます。

## 制限

- スタンバイ WorkSpaces は、プライマリ WorkSpaces のバンドルイメージのみをコピーし、プライマリ WorkSpaces のシステムボリューム (ドライブ C) やユーザーボリューム (ドライブ D) はコピーしません。システムボリューム (ドライブ C) やユーザーボリューム (ドライブ D) をプライマ

リ WorkSpaces からスタンバイ WorkSpaces にコピーするには、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 WorkSpace 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。
- 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、プライマリリージョンで 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た Amazon Route 53 フェイルオーバー DNS ルーティングポリシーを使用できます。プライマリリージョンで 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により、WorkSpaces ユーザーは、フェイルオーバーリージョンでユーザー用に設定した WorkSpaces にリダイレクトされます。
- 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への 1 方向のみでデータをコピーします。スタンバイ WorkSpaces のフェイルオーバー中は、12 ~ 24 時間前のデータとアプリケーションにアクセスできます。障害の発生後は、セカンダリ WorkSpace で作成したデータを手動でバックアップし、ログアウトします。プライマリ WorkSpace からデータにアクセスできるよう、作業内容はネットワークドライブなどの外付けドライブに保存することをお勧めします。
- データレプリケーションは AWS Simple AD をサポートしていません。
- スタンバイ WorkSpaces でデータレプリケーションを有効にすると、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 時間ごとに作成されます。特定のデータボリュームの初回スナップショットはフルコピーで、それ以降のスナップショットは増分コピーです。そのため、特定の WorkSpace の初回レプリケーションは、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 WorkSpaces 内部のスケジュールで開始され、ユーザーがタイミングを制御することはできません。
- プライマリ WorkSpace とスタンバイ WorkSpace が同じドメインを使用して参加している場合は、ドメインコントローラーとの接続が失われないように、特定の時点でプライマリ WorkSpace とスタンバイ WorkSpace 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、WorkSpaces で使用できるように登録できるのは、プライマリリージョンのディレクトリのみです。レプリケート先のリージョンのディレクトリを登録して WorkSpaces で使用しようとすると失敗します。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内の WorkSpaces での使用ではサポートされていません。
- 既にクロスリージョンリダイレクトを設定し、スタンバイ WorkSpaces を使用せずにプライマリージョンとセカンダリリージョンの両方に WorkSpaces を作成している場合は、セカンダリリージョンの既存の WorkSpace 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の WorkSpace をシャットダウンし、スタンバイ WorkSpace を作

成する対象である、プライマリリージョンの WorkSpace を選択して、スタンバイ WorkSpaces を使用してスタンバイ WorkSpace を作成する必要があります。

- 障害の発生後は、セカンダリ WorkSpace で作成したデータを手動でバックアップし、ログアウトします。プライマリ WorkSpace からデータにアクセスできるよう、作業内容はネットワークドライブなどの外付けドライブに保存することをお勧めします。
- WorkSpaces マルチリージョンレジリエンスは、現在以下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、バージョン 3.0.9 以降の Linux、macOS、および Windows WorkSpaces クライアントアプリケーションでのみサポートされます。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 WorkSpaces と Bring-Your-Own-License (BYOL) WorkSpaces をサポートしています。Amazon Linux 2、Ubuntu WorkSpaces、Red Hat Enterprise Linux、GeneralPurpose.4xlarge,GeneralPurpose.8xlarge,または GPU 対応 WorkSpaces (Graphics、GraphicsPro、Graphics.g4dn、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 WorkSpace に接続します。

## マルチリージョンレジリエンスのスタンバイ WorkSpace を設定する

マルチリージョンレジリエンスのスタンバイ WorkSpace を設定するには

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に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 ディレクトリで必ず同じユーザー名を使用します。

   Active Directory ユーザーデータの同期を維持するには、AD Connector を使用して、ユーザー用に WorkSpaces を設定した各リージョンで同じ Active Directory をポイントする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、「WorkSpaces でディレクトリを登録する」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、WorkSpaces で使用できるように登録できるのは、プライマリリー

ジョンのディレクトリのみです。レプリケートしたリージョンのディレクトリを登録して WorkSpaces で使用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、レプリケート先のリージョン内の WorkSpaces では使用できません。

2. プライマリリージョンにユーザー用の WorkSpaces を作成します。WorkSpaces の作成の詳細については、「WorkSpaces の起動」を参照してください。
3. セカンダリリージョンにスタンバイ WorkSpace を作成します。スタンバイ WorkSpace の作成については、「スタンバイ WorkSpace を作成する」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 WorkSpaces 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、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 WorkSpaces のクロスリージョンリダイレクト」のステップ 1 ~ 3 に従ってください。
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連携して動作し、必要に応じて WorkSpaces ユーザーをリダイレクトします。
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でリージョンベースの登録コード (WSpdx+ABC12D など) 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してください。

> **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、新しい WorkSpace 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がユーザーに自動的に送信されます。つまり、セカンダリリージョンでユーザー用に WorkSpaces を設定すると、ユーザーは、これらのセカンダリ WorkSpaces 用の E メールも自動的に受信します。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有効なままです。ただし、クロスリージョンリダイレクトが機能するためには、ユーザーが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。

## スタンバイ WorkSpace の作成

スタンバイ WorkSpace を作成する前に、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のユーザーディレクトリの作成、プライマリリージョンでのユーザー用の WorkSpaces のプロビジョニング、アカウントでのクロスリージョンリダイレクトの設定、Service Quotas によるスタンバイ WorkSpaces の制限の引き上げリクエストなど、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 WorkSpace を作成するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上で、WorkSpaces のプライマリ AWS リージョンを選択します。
3. ナビゲーションペインで [WorkSpaces] を選択します。
4. スタンバイ WorkSpace を作成したい WorkSpace を選択します。
5. [Actions] (アクション) を選択し、[Create standby WorkSpace] (スタンバイ WorkSpace の作成) を選択します。
6. スタンバイ WorkSpace を作成するセカンダリリージョンを選択し、[Next] (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) 暗号化キーを追加し、データ暗号化を有効にして、タグを管理します。

   - 暗号化キーを追加するには、入力暗号化キーにキーを入力します。
   - 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、毎月の追加料金を承認していることを確定します。
   - 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の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 WorkSpace のスナップショットで正常に更新されると、[復旧スナップショット] でスナップショットのタイムスタンプを確認できます。

9. スタンバイ WorkSpaces の設定を確認して、[Create] (作成) を選択します。

> **Note**
>
> - スタンバイ WorkSpaces に関する情報を表示するには、プライマリ WorkSpace の詳細ページに移動します。
> - スタンバイ WorkSpace は、プライマリ WorkSpace のバンドルイメージのみをコピーし、プライマリ WorkSpaces のシステムボリューム (ドライブ C) やユーザーボリューム (ドライブ D) はコピーしません。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) やユーザーボリューム (ドライブ D) をプライマリ WorkSpaces からスタンバイ WorkSpaces にコピーするには、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 WorkSpace の管理

スタンバイ WorkSpace 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。

スタンバイ WorkSpace のデータレプリケーションを有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. プライマリリージョンに移動し、プライマリ WorkSpace の ID を選択します。
3. [スタンバイ状態の WorkSpace] セクションまで下にスクロールし、[スタンバイ状態の WorkSpace を編集] 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、毎月の追加料金を承認していることを確定します。次に、[保存] を選択します。

Note

- スタンバイ WorkSpaces は休止状態にできません。スタンバイ WorkSpace を停止すると、未保存の作業は保持されません。スタンバイ WorkSpaces を終了する前に、必ず作業内容を保存することをお勧めします。
- スタンバイ WorkSpaces でデータレプリケーションを有効にするには、スタンバイリージョンにレプリケートするようにセルフマネージド Active Directory または AWS Managed Microsoft AD を設定する必要があります。ディレクトリを設定するには、Amazon WorkSpaces と AWS Directory Services と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 に従うか、Amazon WorkSpaces でのマルチリージョン AWS マネージド Active Directory 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がサポートされているのは、 AWS Managed Microsoft AD の Enterprise Edition のみです。
- データレプリケーションの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 WorkSpace のスナップショットで正常に更新されると、[復旧スナップショット] でスナップショットのタイムスタンプを確認できます。

## スタンバイ WorkSpace の削除

スタンバイ WorkSpace は、通常の WorkSpace を終了するのと同じ方法で終了できます。

スタンバイ WorkSpace を削除するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. コンソールの右上で、WorkSpaces のプライマリ AWS リージョンを選択します。
3. ナビゲーションペインで [WorkSpaces] を選択します。
4. スタンバイ WorkSpace を選択し、[Delete] (削除) を選択します。スタンバイ WorkSpace が削除されるまで約 5 分かかります。削除中のスタンバイ WorkSpace のステータスは [Terminating] (終了中) に設定されます。削除が完了すると、スタンバイ WorkSpace がコンソールから消えます。

> **Note**
>
> スタンバイ 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。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 WorkSpaces の一方向データレプリケーション

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。安定した状態では、マルチリージョンレジリエンスによって 12 時間ごとにプライマリ WorkSpaces 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が作成されます。これらのスナップショットがセカンダリリージョンに転送され、スタンバイ WorkSpaces の更新に使用されます。デフォルトでは、スタンバイ WorkSpaces のデータレプリケーションは無効になっています。

スタンバイ WorkSpaces でデータレプリケーションを有効にすると、特定のデータボリュームの初回スナップショットは完全コピーとなり、それ以降のスナップショットは増分コピーとなります。そのため、特定の WorkSpace の初回レプリケーションは、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 WorkSpaces 内部の所定の間隔でトリガーされ、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に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、スタンバイ WorkSpaces で 12 ~ 24 時間前のデータとアプリケーションにアクセスできます。ユーザーがスタンバイ WorkSpaces を使用している間は、マルチリージョンレジリエンスによってユーザーがスタンバイ WorkSpaces からのログアウトを強制されたり、プライマリリージョンのスナップショットでスタンバイ WorkSpaces が更新されたりすることはありません。

障害の発生後は、ユーザーがスタンバイ WorkSpaces からログアウトする前に、セカンダリ WorkSpaces 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。再度ログインすると、ユーザーはプライマリリージョンのプライマリ WorkSpaces に誘導されます。

## 復旧用に Amazon EC2 のキャパシティー予約を計画する

Amazon マルチリージョンレジリエンス (MRR) では、デフォルトで、Amazon EC2 オンデマンドプールが使用されます。特定の Amazon EC2 インスタンスタイプで復旧に対応できない場合、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繰り返し試行しますが、極端な状況では、インスタンスが常に使用できるとは限りません。最も重要な

WorkSpaces に必要なインスタンスタイプの可用性を高めるには、 AWS サポートにお問い合わせください。キャパシティープランニングを支援します。

# WorkSpaces Personal に関する問題のトラブルシューティング

以下の情報は、WorkSpaces の問題のトラブルシューティングに役立ちます。

## 高度なログ記録の有効化

任意の Amazon WorkSpaces クライアントに対して高度なログ記録を有効にして、ユーザーが直面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てることができます。

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 を確認し、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 サポート。詳細については、AWS サポート 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` フラグを指定して 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 人のユーザーに対して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てください。

   ```
   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てください。

   ```
   /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` フラグを指定して 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 人のユーザーに対して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てください。

   ```
   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. 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ロ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 (高度なロ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 クライアントのログは、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、WorkSpaces に固有の問題のトラブルシューティングに役立ちます。

問題点

- ユーザー名に無効な文字があるため Amazon Linux WorkSpace を作成できません
- Amazon Linux WorkSpace のシェルを変更しましたが、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
- 接続したディレクトリの WorkSpaces の起動にたびたび失敗する
- 内部エラーにより WorkSpaces の起動に失敗する
- 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で Windows WorkSpace に接続できない
- ユーザーが Windows WorkSpace に接続できない
- ユーザーが WorkSpaces Web Access から WorkSpaces にログオンしようとすると問題が発生する
- Amazon WorkSpaces クライアントで、グレーの「ロード中...」画面がしばらく表示されてからログイン画面に戻る。他のエラーメッセージは表示されない。
- ユーザーに「WorkSpace Status: Unhealthy。We were unable to connect you to your 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「This device is not authorized to access the 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 DCV 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。」というメッセージが表示される。
- WorkSpaces クライアントがネットワークエラーを返しますが、デバイス上の他のネットワーク対応アプリケーションは使用できます
- 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 WorkSpace にアプリケーションをインストールしようとすると、「システム管理者がポリシーを設定してこのインストールを禁止しています」というメッセージが表示される
- ディレクトリのいずれの WorkSpaces もインターネットに接続できない
- WorkSpace がインターネットにアクセスできなくなった
- 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 をアイドル状態のままにすると、スリープ状態になる
- WorkSpace の一部のステータスに UNHEALTHY と表示されます
- WorkSpace が予期せずクラッシュまたは再起動する
- 同じユーザー名に対応する複数の WorkSpace があるが、そのユーザーはいずれかの WorkSpaces にしかログインできない
- Amazon WorkSpaces で Docker の使用がうまくいかない
- 一部の API コールで ThrottlingException エラーが表示される
- WorkSpace をバックグラウンドで実行させておくと、接続が何度も切断される
- SAML 2.0 フェデレーションが動作していません。ユーザーには、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。
- ユーザーが 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) 主導のフローを使用してフェデレートすると、ユーザーにリダイレクト URI エラーが発生します。または、IdP にフェデレートした後、クライアントからサインインを試みるたびに、WorkSpaces クライアントアプリケーションの追加インスタンスが開始されます。
- ユーザーが IdP にフェデレートした後に WorkSpace Spaces 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、「Something went wrong: An error occurred while launching your

WorkSpace」(問題が発生しました: WorkSpace の起動中にエラーが発生しました) というメッセージが表示されます。

- ユーザーが IdP にフェデレートした後に 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、「Unable to validate tags」(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 WorkSpaces で動作しません。
- 私の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きに 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処理を実行しようとしていますが、WorkSpaces がメディアを提供しません。
- 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 を使用して WorkSpaces 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 WorkSpaces クライアントを使用してパスワードをリセットでき、設定されているきめ細かなパスワードポリシー (FFGP) 設定は無視されます AWS Managed Microsoft AD。
- ユーザーが Web Access を使用して Windows/Linux WorkSpace にアクセスしようとすると、「この OS/プラットフォームは WorkSpace へのアクセスを許可されていません」という内容のエラーメッセージが表示されます。
- 停止状態の AutoStop WorkSpace に接続した後、ユーザーの WorkSpace が異常と表示されている
- ログイン後に WorkSpaces Ubuntu バンドルで Gnome がクラッシュする

## ユーザー名に無効な文字があるため Amazon Linux WorkSpace を作成できません

Amazon Linux WorkSpaces の場合、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 WorkSpaces には適用されません。Windows WorkSpaces では、ユーザー名のすべての文字で @ および - 記号をサポートしています。

## Amazon Linux WorkSpace のシェルを変更しましたが、PCoIP セッションをプロビジョニングできません

Linux WorkSpaces のデフォルトシェルを上書きするには、「Amazon Linux WorkSpaces のデフォルトシェルを上書きする」を参照してください。

## 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する予定です。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 WorkSpaces のセッションプロビジョニングが失敗し、エンドユーザーは WorkSpaces に接続できなくなります。

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/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces] を選択します。
3. Linux WorkSpace を選択し、[アクション]、[WorkSpaces の再起動] の順に選択して再起動します。WorkSpace ステータスが `STOPPED` の場合は、[アクション]、[WorkSpaces を起動] の順に選択し、ステータスが `AVAILABLE` になるまで待ってから再起動する必要があります。
4. WorkSpace が再起動され、ステータスが `AVAILABLE` になったら、このアップグレードの実行中に WorkSpace のステータスを `ADMIN_MAINTENANCE` 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` に変更します。`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。

   WorkSpace のステータスを `ADMIN_MAINTENANCE` に変更するには、次の操作を行います。

   a. WorkSpace を選択して、[Actions]、[Modify WorkSpace] の順に選択します。

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 経由で Linux WorkSpace に接続します。詳細については、「WorkSpaces Personal で Linux WorkSpaces の SSH 接続を有効にする」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. WorkSpace から切断し、再度再起動します。

9. WorkSpace のステータスを Step 4 の ADMIN_MAINTENANCE に設定した場合は、Step 4 を繰り返し、意図した状態を AVAILABLE に設定します。

PCoIP エージェントをアップグレードしても Linux WorkSpace が起動しない場合は、 AWS サポートにお問い合わせください。

## 接続したディレクトリの WorkSpaces の起動にたびたび失敗する

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。

## 内部エラーにより WorkSpaces の起動に失敗する

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。この設定を有効にすると、Performance バンドルまたは Graphics バンドルを使用して WorkSpace 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 WorkSpaces で使用するために正常に登録できますが、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内の Amazon WorkSpaces 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で Windows WorkSpace に接続できない

ログオンバナーを表示するためにインタラクティブなログオンメッセージが実装されると、これによりユーザーは自分の Windows WorkSpaces にアクセスできなくなります。現在、インタラクティブなログオンメッセージのグループポリシー設定は PCoIP WorkSpaces でサポートされていません。Interactive logon: Message text for users attempting to log on グループポリシーが適用されていない組織単位 (OU) に WorkSpaces を移動します。ログオンメッセージは DCV WorkSpaces でサポートされており、ユーザーはログオンバナーを承諾した後に再度ログインする必要があります。

## ユーザーが Windows WorkSpace に接続できない

ユーザーが Windows WorkSpace に接続しようとすると、次のエラーが表示されます。

```
"An error occurred while launching your WorkSpace. Please try again."
```

このエラーは、WorkSpace が PCoIP を使用して Windows デスクトップを読み込めない場合によく発生します。以下を確認してください。

- 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 エージェントがアンインストールされた場合は、Amazon WorkSpaces コンソールから WorkSpace を再起動して、自動的に再インストールします。

- 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も、長時間の遅延後にこのエラーが Amazon WorkSpaces クライアントで発生する可能性があります。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で WorkSpaces 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通信でき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、ユーザーは自分の Windows WorkSpace にアクセスできなくなります。

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 から WorkSpaces にログオンしようとすると問題が発生する

Amazon WorkSpaces では、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、専用のログオン画面設定を使用しています。

Web Access ユーザーが WorkSpaces にログオンできるようにするには、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構成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と、ログオン時間が長くなったり、WorkSpaces にログオンする際にブラックスクリーンがユーザーに表示されたりする場合があります。これらの設定を構成するには、「WorkSpaces Personal で WorkSpaces Web Access を有効にして設定する」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 自分のライセンス使用 (BYOL) WorkSpaces に接続できなくなります。

## Amazon WorkSpaces クライアントで、グレーの「ロード中...」画面がしばらく表示されてからログイン画面に戻る。他のエラーメッセージは表示されない。

通常、この動作が発生する場合、WorkSpaces クライアントはポート 443 経由で認証できますが、ポート 4172 (PCoIP) または 4195 (DCV) 経由でストリーミング接続を確立できないことを示しています。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した場合は、WorkSpace のネットワーク設定に問題がある可能性があります。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) クライアントを使用して WorkSpace 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 Status: Unhealthy。We were unable to connect you to your 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。

WorkSpace を再起動または起動したばかりの場合は、数分待ってからもう一度お試しください。

WorkSpace がしばらくの間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 サービスについて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「This device is not authorized to access the 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、次のいずれかが発生している可能性があることを示しています。

- WorkSpace ディレクトリで IP アクセスコントロールグループは設定されているが、クライアント IP アドレスが許可リストに登録されていない。

  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 アドレスで WorkSpace へのアクセスが許可されていることを確認します。

- [信頼されたデバイス] オプションを使用する際、アクセスコントロールでデバイスのオペレーティングシステムが信頼されたデバイスとして許可されていないか、適切な証明書がデバイスにインストールされていない。以下を実行して、使用しているデバイスのタイプを信頼されたデバイスとして追加します。

  1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
  2. ナビゲーションペインで [ディレクトリ] を選択します。
  3. 使用している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] まで下にスクロールし、[編集]を選択します。
  5. [信頼されたデバイス] で、アクセスを許可するデバイスタイプについて、ドロップダウンから [すべて許可] を選択します。クライアント証明書がインストールされているデバイスに制限する場合は、[信頼されたデバイス] を選択します。
  6. 前の手順で [信頼されたデバイス] を選択した場合は、少なくとも 1 つのルート証明書をインポートしてあること、さらに、ルート証明機関 (CA) によって発行されたクライアント証明書がクライアントにインストールされていることを確認します。ルート証明書の作成、デプロイ、インポートの詳細については、「WorkSpaces Personal で信頼されたデバイスへのアクセスを制限する」を参照してください。
  7. [保存] を選択します。

- 使用しているデバイスのタイプに WorkSpaces へのアクセス許可が付与されていない。以下を実行して、デバイスのタイプにアクセス許可を付与します。

  1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
  2. ナビゲーションペインで [ディレクトリ] を選択します。
  3. 使用しているディレクトリを選択します。
  4. [他のプラットフォーム] まで下にスクロールし、[編集] を選択します。
  5. WorkSpaces へのアクセスを許可するデバイスタイプを次から 1 つ選んで、チェックボックスをオンにします。
     - ChromeOS

- iOS
- リナックス
- Web Access
- ゼロクライアント

6. [保存] を選択します。

## ユーザーが DCV 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。」というメッセージが表示される。

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。DCV を使用する WorkSpaces の場合、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 に変更されています。

## WorkSpaces クライアントがネットワークエラーを返しますが、デバイス上の他のネットワーク対応アプリケーションは使用できます

WorkSpaces の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いるため、最低 1 Mbps のダウンロード帯域幅を提供する接続が必要です。デバイスがネットワークに断続的に接続している場合、WorkSpaces クライアントアプリケーションがネットワークに関する問題を報告することがあります。

WorkSpaces は、2018 年 5 月の時点で Amazon Trust Services により発行されたデジタル証明書の使用を適用します。Amazon Trust Services は、WorkSpaces でサポートされているオペレーティングシステムですでに信頼されたルート CA になっています。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 WorkSpaces に接続できず、クライアントからネットワークエラーが返されます。

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をダウンロードしてインストールします。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] を選択してください。[OK] を選択してください。
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、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 以降を使用して WorkSpace に直接接続するには、Amazon Trust Services が発行し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。

登録サービスでエラーが発生すると、[Connection Health Check] ページに次のメッセージが WorkSpace ユーザーに表示されます: 「ご使用のデバイスは WorkSpaces 登録サービスに接続できません。このデバイスを WorkSpaces に登録することはできません。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アクセス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場合に発生します。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 Personal で PCoIP ゼロクライアントを設定する」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 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。

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は、USB リダイレクトを有効にしない限り、USB 周辺デバイスは PCoIP ゼロクライアントデバイスで動作しません。

> **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

グループポリシーを介してこれらのレジストリの変更をWorkSpacesにプッシュ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\ ソフトウェア\ ポリシー\ 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\ SOWARE\ ソフトウェア\ ポリシー\ Teradici\ PCoIP\ pcoIP\ pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1

3. まだ行っていない場合は、WorkSpace からログアウトしてから、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、SkipThisVersion レジストリキーが設定されます。そのため、新しいバージョンのクライアント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 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。以下の 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 設定が定義されます。そのため、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」の説明に従って、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 アプリ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はこれ以上更新されず、その使用はサポートされません。

Android アプリケーションのインストールに対応している Chromebook では、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、「WorkSpaces Personal で Chromebook 用の Android を設定する」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 または信頼できるドメインを使用して作成された WorkSpaces のウェルカム E メール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は届きません。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 Personal で 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。([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 Personal で Active Directory 管理ツールを設定する を参照してください。

## Windows WorkSpace にアプリケーションをインストールしようとすると、「システム管理者がポリシーを設定してこのインストールを禁止しています」というメッセージが表示される

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。ディレクトリ内の複数の WorkSpaces にこのポリシーをデプロイするには、ドメイン結合された 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. ドメインに WorkSpaces グループポリシー管理用テンプレート がインストールされていることを確認します。
2. Windows WorkSpace クライアントでグループポリシーの管理ツールを開き、WorkSpaces コンピュータアカウントの 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] を選択してください。
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。
   - WorkSpace を再起動します (WorkSpaces コンソールで、WorkSpace を選択し、[Actions] (アクション)、[Reboot WorkSpaces] (WorkSpaces の再起動) 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。

## ディレクトリのいずれの WorkSpaces もインターネットに接続できない

WorkSpaces はデフォルトではインターネットと通信することができません。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、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

## WorkSpace がインターネットにアクセスできなくなった

WorkSpace がインターネットにアクセスできなくなり、RDP を使用して WorkSpace に接続できない場合は、おそらく WorkSpace 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。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、(Amazon が提供するプールからの) Elastic IP アドレスは、起動時に 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 WorkSpace に関連付けた後、その Elastic IP アドレスと WorkSpace 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 WorkSpace に関連付けるには、WorkSpace を再構築する必要があります。WorkSpace を再構築しない場合は、所有する別の Elastic IP アドレスを WorkSpace に関連付ける必要があります。

WorkSpace の起動後は、WorkSpace の Elastic Network Interface を変更しないことをお勧めします。Elastic IP アドレスが WorkSpace に割り当てられると、WorkSpace は同じパブリック IP アドレスを保持します (WorkSpace が再構築された場合を除く。その場合は新しいパブリック 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 TechNet の「SRV リソースレコード」を参照してください。

## Windows WorkSpace をアイドル状態のままにすると、スリープ状態になる

この問題を解決するには、WorkSpace に接続し、次の手順を使用して電源プランを [High performance (高パフォーマンス)] に変更します。

1. WorkSpace から [コントロールパネル] を開き、[ハードウェア] もしくは [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は、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. WorkSpace から [コントロールパネル] を開き、[ハードウェア] もしくは [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は、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。

## WorkSpace の一部のステータスに UNHEALTHY と表示されます

WorkSpaces サービスは定期的にステータスリクエストを WorkSpace に送信します。このリクエストに応答しない WorkSpace は、"UNHEALTHY" と表示されます。この問題に対する一般的な原因は次のとおりです。

- WorkSpace のアプリケーションがネットワークポートをブロックして、WorkSpace によるステータスリクエストへの応答を妨げています。
- 高 CPU 使用率は、WorkSpace によるステータスリクエストへの応答を一時的に防ぐことがあります。
- WorkSpace のコンピュータ名が変更された場合。これにより、 WorkSpaces と WorkSpace の間に確立されるべき安全な交信が妨げられます。

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 コンソールから WorkSpace を再起動します。
- トラブルシューティングの目的でのみ使用する必要がある次の手順を使用して、不具合のある WorkSpace に接続します。

  1. 不具合のある WorkSpace と同じディレクトリ内の動作している WorkSpace に接続します。
  2. 動作している WorkSpace から、Remote Desktop Protocol ( RDP ) を使って、不具合のある WorkSpace の IP アドレスから不具合のある WorkSpace に接続します。問題の規模により、不具合のある WorkSpace に接続できない場合もあります。
  3. 不具合のある WorkSpace で最低限の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 Status: Unhealthy。We were unable to connect you to your 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 コンソールから WorkSpace を再構築します。WorkSpace の再構築ではデータ損失が発生する可能性があるため、その他のすべての問題対処方法が失敗した場合にのみ、このオプションを実行してください。

## WorkSpace が予期せずクラッシュまたは再起動する

PCoIP に対応した WorkSpace が繰り返しクラッシュまたは再起動し、エラーログやクラッシュダンプで `spacedeskHookKmode.sys` または `spacedeskHookUmode.dll` の問題が示されている場

合、あるいは次のエラーメッセージが表示される場合は、WorkSpace へのウェブアクセスの無効化が必要になる場合があります。

```
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ステップは、DCV 用に設定された WorkSpaces には適用されません。これらは、PCoIP に対応した WorkSpaces にのみ適用されます。
> - 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。

WorkSpace に対して Web Access を無効にするには、WorkSpaces ディレクトリで Web Access を無効にし、WorkSpace を再起動する必要があります。

## 同じユーザー名に対応する複数の WorkSpace があるが、そのユーザーはいずれかの WorkSpaces にしかログインできない

最初に WorkSpace を削除せずに Active Directory (AD) でユーザーを削除してから、そのユーザーを Active Directory に再度追加し、そのユーザーの新しい WorkSpace を作成すると、同じユーザー名に対応する 2 つの WorkSpaces が同じディレクトリに作成されます。ただし、そのユーザーが元の WorkSpace に接続しようとすると、以下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 コンソールでそのユーザー名を検索すると、両方の WorkSpaces がまだ存在していても、新しい WorkSpace のみが返されます (ユーザー名の代わりに WorkSpace ID を検索すると、元の WorkSpace を見つけることができます)。

この動作は、最初に WorkSpace 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見られることがあります。その場合、ユーザー名を元のユーザー名に戻し、そのユーザーの新しい WorkSpace を作成すると、同じユーザー名に対応する 2 つの WorkSpaces が同じディレクトリに作成されます。

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に、Amazon WorkSpaces コンソールは SID を使用して Active Directory で一致する名前を見つけます。Amazon WorkSpaces クライアントも SID を使用して、WorkSpaces に接続しようとするユーザーを識別します。

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、そのユーザーが元の WorkSpace に接続できることを確認してください。確認できれば、ユーザーデータを手動でバックアップして新しい WorkSpace から元の WorkSpace に転送した後、新しい WorkSpace を削除できます (必要に応じて)。
- 元のユーザーオブジェクトを復元できない場合は、そのユーザーの元の WorkSpace を削除します。そのユーザーは、代わりに新しい WorkSpace に接続し、その WorkSpace を使用できるようになります。必ずユーザーデータを手動でバックアップし、元の WorkSpace から新しい WorkSpace に転送してください。

> **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。

## Amazon WorkSpaces で Docker の使用がうまくいかない

### Windows WorkSpaces

ネストされた仮想化 (Docker の使用を含む) は、Windows WorkSpaces ではサポートされていません。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 WorkSpaces で Docker を使用するには、Docker によって使用される CIDR ブロックが、WorkSpace に関連付けられている 2 つの Elastic Network Interface (ENI) 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。Linux WorkSpaces で Docker を使用する際に問題が発生した場合、Docker にお問い合わせください。

## 一部の API コールで 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、許可される最大「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。 |
| 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。 |

| 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 |
|---|---|---|---|
| 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。 |

## WorkSpace をバックグラウンドで実行させておくと、接続が何度も切断される

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。ユーザーには、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。この IAM ロールは、WorkSpaces ディレクトリにアクセスしているフェデレーション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に WorkSpace を持っていることを確認します。詳細については、「SAML 2.0 Authentication and Troubleshooting SAML 2.0 Federation with AWS」を参照してください。

## ユーザーが 60 分ごとに WorkSpaces セッションから切断されます。

WorkSpaces に SAML 2.0 認証を設定している場合、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) 主導のフローを使用してフェデレートすると、ユーザーにリダイレクト URI エラーが発生します。または、IdP にフェデレートした後、クライアントからサインインを試みるたびに、WorkSpaces クライアントアプリケーションの追加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 フェデレーションのセットアップで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で、ユーザーアクセス URL とリレーステートパラメータ名が IdP フェデレーションに対して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 IdP にフェデレートした後に WorkSpace Spaces 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、「Something went wrong: An error occurred while launching your WorkSpace」(問題が発生しました: WorkSpace の起動中にエラーが発生しました) というメッセージが表示されます。

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 Subject NameID] (SAML サブジェクト名 ID) 値は WorkSpaces ユーザー名と一致する必要があります。通常は、Active Directory ユーザーの sAMAccountName 属性と同じです。さらに、PrincipalTag:Email 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email に設定された [Attribute] (属性) 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 にフェデレートした後に 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、「Unable to validate tags」(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 WorkSpaces で動作しません。

[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、必要に応じてグループポリシーオブジェクト (GPO) を作成して、マイクやウェブカメラを有効にできます。

## 私の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きに 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がサポートされていません。証明書ベースの認証は、最新の WorkSpaces Windows クライアントアプリケーションを使用している Windows WorkSpaces DCV バンドルでサポートされます。

- WorkSpaces ディレクトリで証明書ベースの認証を有効にしたら、WorkSpaces を再起動する必要があります。
- WorkSpaces は証明書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で `certutil -viewstore -enterprise NTAuth` 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前 (24 時間) にキャッシュをクリア サポート するには、 にお問い合わせください。詳細については、サポート 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ていません。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がオンラインになっていないか、WorkSpaces からも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 CA があるかどうかを確認するには、CA で PKIVIEW.msc を実行します。古い CA がある場合は、PKIVIEW.msc mmc を使用して手動で削除します。
- 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、repadmin /replsum を実行します。

トラブルシューティングのその他のステップには、WorkSpaces インスタンスの Windows イベントログを確認することが含まれます。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 サポート。詳細については、サポート 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処理を実行しようとしていますが、WorkSpaces がメディアを提供しません。

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て Amazon EC2 にアタッチし、ファイルを必要とする WorkSpace にファイルを転送します。WorkSpaces の BYOL で Windows 10 を使用していて、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用意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 ボリュームは WorkSpace に直接アタッチできないため、Amazon EC2 インスタンスにアタッチしてから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 を使用して WorkSpaces を起動したい。

WorkSpaces で現在サポートされていないリージョンのディレクトリを使用して Amazon WorkSpaces を起動するには、以下の手順に従ってください。

> **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、Amazon WorkSpaces を登録する

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、このディレクトリの WorkSpaces へのアクセスを有効にします。
5. WorkSpaces でディレクトリを登録する 詳細については、「WorkSpaces でディレクトリを登録する」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、WorkSpace でコマンド `systemctl status *os-update-mgmt.timer | grep enabled` を実行します。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

通常、Firefox は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と共に Amazon Linux 2 WorkSpaces で自動更新されます。ただし、これはお使いの WorkSpaces のタイプによって異なります。

- AlwaysOn WorkSpaces の場合、毎週のメンテナンスウィンドウは、ワークスペースのタイムゾーンの日曜日 0:00 ~ 4:00 です。
- AutoStop WorkSpaces の場合。毎月第 3 月曜日から最大 2 週間、メンテナンスウィンドウは WorkSpace の AWS リージョンのタイムゾーンで毎日約 00:00 から 05:00 まで開かれます。

メンテナンスウィンドウの詳細については、「WorkSpace のメンテナンス」を参照してください。

WorkSpace を再起動して 15 分後に再接続することで、すぐに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WorkSpaces にサイドロードします。WorkSpaces では、`sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm` のような標準 YUM コマンドでインストールできます。

> **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 WorkSpaces 向けの Firefox アップデートを自動的に提供します。2023 年 7 月 31 日以降に作成された Amazon Linux 2 WorkSpaces では、Firefox Extra リポ

ジトリが既にアクティブ化されています。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 リポジトリ経由で Amazon Linux 2 WorkSpaces 向けの Firefox アップデートを継続的に受け取るには、WorkSpaces が Amazon Linux 2 リポジトリにアクセス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 WorkSpaces クライアントを使用してパスワードをリセットでき、設定されているきめ細かなパスワードポリシー (FFGP) 設定は無視されます 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の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、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(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

パスワードには、空白、キャリッジリターン、タブ、改行、null 文字など、印刷不可能な Unicode 文字が含まれていないことを確認してください。

WorkSpaces に FFGP を適用することを組織から求められている場合は、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。

### ユーザーが Web Access を使用して Windows/Linux WorkSpace にアクセスしようとすると、「この OS/プラットフォームは WorkSpace へのアクセスを許可されていません」という内容のエラーメッセージが表示されます。

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に、WorkSpaces の Web Access との互換性がありません。WorkSpace ディレクトリの [他のプラットフォーム] 設定で Web Access を有効にしてください。WorkSpaces の Web Access を有効にする方法の詳細については、「WorkSpaces Personal で WorkSpaces Web Access を有効にして設定する」を参照してください。

### 停止状態の AutoStop WorkSpace に接続した後、ユーザーの WorkSpace が異常と表示されている

ユーザーは、休止状態から再開するときにネットワークインターフェイスに問題を引き起こすことがわかっているソフトウェアを使用している可能性があります。例えば、WorkSpace に NPCAP 1.1 アプリケーションがインストールされている場合は、バージョン 1.2 以降に更新してこの問題を解決します。

### ログイン後に WorkSpaces Ubuntu バンドルで Gnome がクラッシュする

ubuntu ユーザー名を使用して WorkSpace を起動すると、デフォルトで存在するubuntuユーザーとの競合が発生します。これにより、Gnome でクラッシュし、他のパフォーマンスが低下する可能性があります。この問題を回避するには、Ubuntu WorkSpaces をプロビジョニングするときにubuntuユーザー名を指定しないでください。

## WorkSpaces Personal の DCV ホストエージェントのバージョン

DCV ホストエージェントは、WorkSpace 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にストリーミングし、双方向の音声とビデオ、印刷などのセッション内の機能を備えています。DCV 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。

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。WorkSpaces を手動で再起動して DCV ホストエージェントを更新できます。DCV ホストエージェントは、通常の WorkSpaces のデフォルト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、「WorkSpace のメンテナンス」を参照してください。これらの機能の中には、最新の WorkSpaces クライアントバージョンを必要とするものがあります。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、WorkSpaces Personal の DCV 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 |
| --- | --- | --- |
| • Ubuntu WorkSpaces - 2.1.0.1923 | 2025 年 5 月 1 日 | • パフォーマンス向上とバグ修正が行われています。 |
| • Rocky Linux WorkSpaces - 2.1.0.1843<br>• Red Hat Enterprise Linux WorkSpaces - 2.1.0.1843 | 2025 年 4 月 10 日 | • パフォーマンス向上とバグ修正が行われています。 |
| • Windows WorkSpaces - 2.1.0.1840 | 2025 年 3 月 19 日 | • プリンターリダイレクト GPO が無効になっていてもプリンターのリストが表示される問題を修正しました。<br>• パフォーマンス向上とバグ修正が行われています。 |
| • Windows WorkSpaces - 2.1.0.1792 | 2024 年 11 月 19 日 | パフォーマンス向上とバグ修正が行われています。 |
| • Windows WorkSpaces - 2.1.0.1786 | 2024 年 10 月 31 日 | • WorkSpaces Streaming Protocol (WSP) の名前を Amazon DCV に変更しました。<br>• 「」アプリケーションを使用しているお客様の DCV エージェントでのオーディオダックの問題を修正しました。<br>• PIN プロンプトページでユーザーがアイドル状態のときに発生する |

| リリース | 日付 | 変更 |
| --- | --- | --- |
| | | SmartCard ログインの問題を修正しました。<br>• Chrome ブラウザでの初回ログイン試行時の WebAuthn リダイレクトの問題を修正しました。<br>• パフォーマンス向上とバグ修正が行われています。 |
| • Windows WorkSpaces - 2.1.0.1757 | 2024 年 8 月 19 日 | • IAM アイデンティティセンター (IdC) との統合についてサポートが追加されました。<br>• パフォーマンス向上とバグ修正が行われています。 |
| • Windows WorkSpaces - 2.1.0.1696 | 2024 年 7 月 29 日 | • Windows Graphics ホストのサポートが追加されました。<br>• Amazon Connect で WebRTC リダイレクトのサポートが追加されました。<br>• システム起動時にサービスを実行できない問題を修正しました。<br>• 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 |
| --- | --- | --- |
| • 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。<br>• 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。<br>• ユーザーが表示設定を変更したときに WorkSpaces が切断され、白い画面が表示される問題を修正しました。<br>• 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 | • 優先するウェブカメラの解像度を 480x360 から 640x480 に変更しました。<br>• 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 |
| --- | --- | --- |
| • Windows WorkSpaces - 2.0.0.1425 | 2024 年 2 月 22 日 | • リモートの 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、セッション中の WebAuthn リクエストのリダイレクトについてサポートが開始されました。この機能により、DCV WebAuthn リダイレクト拡張機能の有効化をユーザーに求める 1 回限りのブラウザプロンプトが表示されます。この機能は、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ます。<br>• ログイン時に白い画面や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。<br>• 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に関連するバグを修正しました。<br>• ログ記録に関連する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 以降で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。<br>• 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。<br>• クリップボードイメージの透過性に関連するバグを修正しました。<br>• Windows のスケールファクターが保持されるバグを修正しました。<br>• 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。<br>• 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。<br>• 再接続と信頼性の問題を改善しました。<br>• 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<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• アップグレードの問題を修正しました。<br>• 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。<br>• 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。<br>• DCV 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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。<br>• 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、「DCV 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、「既に DCV WorkSpace を持っている場合、どのように更新すればよいですか?」を参照してください。
- DCV 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、「WorkSpaces ユーザーガイド」で、WorkSpaces macOS クライアントアプリケーションのセクションの「リリースノート」を参照してください。
- DCV 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、「WorkSpaces ユーザーガイド」で、WorkSpaces Windows クライアントアプリケーションのセクションの「リリースノート」を参照してください。

# WorkSpaces Pools の使用と管理

WorkSpaces Pools では、一時的なインフラストラクチャでホストされている高度に選別されたデスクトップ環境へのアクセスを必要とするユーザーに向けて、カスタマイズされた非永続的な仮想デスクトップを提供します。

トピック



## AWS リージョン WorkSpaces Pools の およびアベイラビリティーゾーン

WorkSpaces Pools は、以下にあります AWS リージョン。

> **Note**
>
> WorkSpaces Personal AWS リージョン に適用される については、 AWS 全般のリファレンス リファレンスガイドのAmazon WorkSpaces エンドポイントとクォータ」を参照してください。

| リージョン名 | リージョン | エンドポイント | プロトコル | アベイラビリティーゾーン | |
|---|---|---|---|---|---|
| 米国東部 (バージニア北部) | us-east-1 | workspaces.us-east-1.amazonaws.com<br>workspaces-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS | use1-az2、use1-az4、use1-az6 | |
| 米国西部 (オレゴン) | us-west-2 | workspaces.us-west-2.amazonaws.com<br>workspaces-fips.us-west-2.amazonaws.com | HTTPS<br>HTTPS | usw2-az1、usw2-az2、usw2-az3 | |
| アジアパシフィック (ムンバイ) | ap-south-1 | workspaces.ap-south-1.amazonaws.com | HTTPS | aps1-az1、aps1-az3 | |
| アジアパシフィック (ソウル) | ap-northeast-2 | workspaces.ap-northeast-2.amazonaws.com | HTTPS | apne2-az1、apne2-az3 | |
| アジアパシフィック (シンガポール) | ap-southeast-1 | workspaces.ap-southeast-1.amazonaws.com | HTTPS | apse1-az1、apse1-az2 | |

| リージョン名 | リージョン | エンドポイント | プロトコル | アベイラビリティーゾーン | |
|---|---|---|---|---|---|
| アジアパシフィック (シドニー) | ap-southeast-2 | workspaces.ap-southeast-2.amazonaws.com | HTTPS | apse2-az1、apse2-az3 | |
| アジアパシフィック (東京) | ap-northeast-1 | workspaces.ap-northeast-1.amazonaws.com | HTTPS | apne1-az1、apne1-az4 | |
| カナダ (中部) | ca-central-1 | workspaces.ca-central-1.amazonaws.com | HTTPS | cac1-az1、cac1-az2 | |
| 欧州 (フランクフルト) | eu-central-1 | workspaces.eu-central-1.amazonaws.com | HTTPS | euc1-az2、euc1-az3 | |
| 欧州 (アイルランド) | eu-west-1 | workspaces.eu-west-1.amazonaws.com | HTTPS | euw1-az1、euw1-az2、euw1-az3 | |
| 欧州 (ロンドン) | eu-west-2 | workspaces.eu-west-2.amazonaws.com | HTTPS | euw2-az2、euw2-az3 | |

| リージョン名 | リージョン | エンドポイント | プロトコル | アベイラビリティーゾーン |
|---|---|---|---|---|
| 欧州 (パリ) | eu-west-3 | workspaces.eu-west-3.amazonaws.com | HTTPS | euw3-az1、euw3-az2、euw3-az3 |
| 南米 (サンパウロ) | sa-east-1 | workspaces.sa-east-1.amazonaws.com | HTTPS | sae1-az1、sae1-az3 |
| AWS GovCloud (米国東部) | us-gov-east-1 | workspaces.us-gov-east-1.amazonaws.com<br><br>workspaces-fips.us-gov-east-1.amazonaws.com | HTTPS<br><br>HTTPS | usgw1-az1、usgw1-az2、usgw1-az3 |
| AWS GovCloud (米国西部) | us-gov-west-1 | workspaces.us-gov-west-1.amazonaws.com<br><br>workspaces-fips.us-gov-west-1.amazonaws.com | HTTPS<br><br>HTTPS | usge1-az1、usge1-az2、usge1-az3 |

# WorkSpaces Pools のディレクトリを管理する

WorkSpaces Pools 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。このセクションでは、WorkSpaces Pools のディレクトリを作成および管理する方法を示します。

内容



# SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する

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、WorkSpaces クライアントアプリケーションの登録と、WorkSpaces Pools の WorkSpaces へのサインインを有効にできます。これを行うには、 AWS Identity and Access Management (IAM) ロールとリレーステート URL を使用して SAML 2.0 ID プロバイダー (IdP) を設定し、 AWSで有効にします。これにより、フェデレーションユーザーに対して WorkSpaces Pools ディレクトリへのアクセス権が付与されます。リレーステートは、 AWSに正常にサインインした後にユーザーが転送される WorkSpaces ディレクトリエンドポイントです。

> **Important**
>
> WorkSpaces Pools は、IP ベースの SAML 2.0 設定をサポートしていません。

トピック

## ステップ 1: 要件を考慮する

WorkSpaces Pools ディレクトリに SAML を設定する場合、以下の要件が適用されます。

- workspaces_DefaultRole IAM ロールは AWS アカウントに存在する必要があります。このロールは、WorkSpaces Quick Setup を使用した場合、または過去に AWS Management Consoleを使用して WorkSpace を起動したことがある場合に、自動的に作成されます。ユーザーに代わって特定の AWS リソースにアクセスするアクセス許可を Amazon WorkSpaces に付与します。このロールが既に存在する場合は、AmazonWorkSpacesPoolServiceAccess マネージドポリシーのアタッチが必要になる場合があります。このポリシーは、Amazon WorkSpaces が WorkSpaces Pools の AWS アカウントで必要なリソースにアクセスするために使用するものです。詳細については、「workspaces_DefaultRole ロールを作成する」および「AWS マネージドポリシー: AmazonWorkSpacesPoolServiceAccess」を参照してください。
- WorkSpaces Pools の SAML 2.0 認証は、この機能をサポートする AWS リージョン で設定できます。詳細については、「AWS リージョン WorkSpaces Pools の およびアベイラビリティーゾーン」を参照してください。
- WorkSpaces で SAML 2.0 認証を使用する場合、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の URL を使用して、未承諾の IdP を起点とする SSO をサポートする必要があります。これをサポートする IdP の例には、ADFS、Azure AD、Duo Single Sign-On、Okta、PingFederate、および PingOne などがあります。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、次の WorkSpaces クライアントでのみサポートされています。最新の WorkSpaces クライアントについては、Amazon WorkSpaces クライアントのダウンロードページを参照してください。
  - Windows クライアントアプリケーション、バージョン 5.20.0 以降
  - macOS クライアント、バージョン 5.20.0 以降
  - Web Access

## ステップ 2: 前提条件を完了させる

WorkSpaces Pools ディレクトリへの SAML 2.0 IdP 接続を設定する前に、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。

- 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 Management Console にアクセスするための IAM との IdP 統合があります。
- 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。
- WorkSpaces コンソールを使用して WorkSpaces Pools ディレクトリを作成します。詳細については、「WorkSpaces Pools での Active Directory の使用」を参照してください。
- 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ユーザー用の WorkSpaces Pools を作成します。詳細については、「WorkSpaces プールを作成する」を参照してください。

## ステップ 3: IAM で SAML ID プロバイダーを作成する

まず、IAM で SAML IdP を作成する必要があります。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、「AWS Identity and Access Management ユーザーガイド」の「SAML ID プロバイダーを作成および管理する」を参照してください。 AWS GovCloud (US) Regionsでの SAML IdP の使用については、「AWS GovCloud (US) ユーザーガイド」の「AWS Identity and Access Management」を参照してください。

## ステップ 4: WorkSpace Pool ディレクトリを作成する

WorkSpaces プールディレクトリを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [Create directory] (ディレクトリの作成) を選択します。
4. [WorkSpace タイプ] で [プール] を選択します。
5. ページの [ユーザー ID ソース] セクションで以下の操作を行います。

    a. [ユーザーアクセス URL] テキストボックスにプレースホルダー値を入力します。例えば、テキストボックスに `placeholder` と入力します。これは、IdP でアプリケーション使用権限を設定した後に編集します。

b. [リレー状態パラメータ名] テキストボックスは空白のままにします。これは、IdP でアプリケーション使用権限を設定した後に編集します。

6. ページの [ディレクトリ情報] セクションで、ディレクトリの名前と説明を入力します。ディレクトリ名と説明は 128 文字未満で、英数字と _ @ # % * + = : ? . / ! \ - の特殊文字を含めることができます。ディレクトリ名と説明を特殊文字で始めることはできません。

7. ページの[ネットワークとセキュリティ] セクションで以下の操作を行います。

   a. アプリケーションが必要とするネットワークリソースへのアクセスが許可されている VPC および 2 つのサブネットを選択します。耐障害性を高めるために、異なるアベイラビリティーゾーンで 2 つのサブネットを選択する必要があります。

   b. WorkSpaces で VPC にネットワークリンクを作成できるように、セキュリティグループを選択します。セキュリティグループは、WorkSpaces から VPC へのフローを許可するネットワークトラフィックを制御します。例えば、セキュリティグループですべてのインバウンド HTTPS 接続が制限されている場合、ウェブポータルにアクセスするユーザーは WorkSpaces から HTTPS ウェブサイトをロードできません。

8. [Active Directory 設定] セクションはオプションです。ただし、WorkSpaces Pools で Active Directory (AD) を使用する場合は、WorkSpaces Pools ディレクトリの作成時に AD の詳細を指定する必要があります。WorkSpaces Pools ディレクトリの作成後に [Active Directory 設定] を編集することはできません。WorkSpaces Pools ディレクトリの AD の詳細を指定する方法の詳細については、「WorkSpaces Pools ディレクトリの Active Directory 情報を指定する」を参照してください。そこで説明されているプロセスが完了したら、このトピックに戻って WorkSpaces Pools ディレクトリの作成を完了する必要があります。

   WorkSpaces Pools で AD を使用する予定がない場合は、[Active Directory 設定] セクションを省略できます。

9. [ストリーミングプロパティ] セクションで以下の操作を行います。

   - クリップボードのアクセス許可の動作を選択し、[ローカル文字数制限にコピー] (オプション) と [リモートセッションへの貼り付けの文字数制限] (オプション) に入力します。
   - ローカルデバイスへの出力を許可するかしないかを選択します。
   - 診断ログを許可するかしないかを選択します。
   - スマートカードサインインを許可するかしないかを選択します。この機能は、この手順の前半で AD 設定を有効にした場合にのみ適用されます。

10. ページの [ストレージ] セクションで、ホームフォルダを有効にするよう選択できます。

11. ページの [IAM ロール] セクションで、すべてのデスクトップストリーミングインスタンスで使用できる IAM ロールを選択します。新しい IAM ロールを作成するには、[新しい IAM ロールを作成] を選択します。

    アカウントから WorkSpace Pool ディレクトリに IAM ロールを適用すると、 AWS 認証情報を手動で管理することなくWorkSpace Pool の WorkSpace から AWS API リクエストを行うことができます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーにアクセス許可を委任するロールを作成する」を参照してください。

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

## ステップ 5: SAML 2.0 フェデレーション IAM ロールを作成する

次の手順を実行して、IAM コンソールで SAML 2.0 フェデレーション IAM ロールを作成します。

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 [ロール] を選択します。
3. [ロールの作成] を選択してください。
4. 信頼されたエンティティタイプとして、[SAML 2.0 フェデレーション] を選択します。
5. SAML 2.0 ベースのプロバイダーとして、IAM で作成した ID プロバイダーを選択します。詳細については、「IAM で SAML ID プロバイダーを作成する」を参照してください。
6. 許可されるアクセスとして [プログラムによるアクセスのみを許可する] を選択します。
7. 属性に SAML:sub_type を選択します。
8. [値] に「`https://signin.aws.amazon.com/saml`」と入力します。この設定値は、値が `persistent` 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。詳細については、「AWS Identity and Access Management ユーザーガイド」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」を参照してください。
9. [次へ] を選択して続行します。
10. [許可を追加] ページでは変更や選択を行いません。[次へ] を選択して続行します。
11. ロールの名前と説明を入力します。
12. [ロールの作成] を選択してください。
13. [ロール] ページで、作成したロールを選択します。

14. [信頼関係] タブを選択します。
15. [Edit trust policy] (信頼ポリシーを編集) を選択します。
16. [信頼ポリシーを編集] JSON テキストボックスで、sts:TagSession アクションを信頼ポリシーに追加します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS STSでセッションタグを渡す」を参照してください。

    結果は次の例のようになります。


17. [ポリシーの更新] を選択してください。
18. [アクセス許可] タブを選択します。
19. ページの [許可ポリシー] セクションで、[許可を追加] を選択し、[インラインポリシーを作成] を選択します。
20. ページの [ポリシーエディタ] セクションで、[JSON] を選択します。
21. [ポリシーエディタ] JSON テキストボックスに、次のポリシーを入力します。必ず以下を置き換えてください。

    - *<region-code>* を、WorkSpace Pool ディレクトリを作成した AWS リージョンのコードに。
    - AWS アカウント ID の *<account-id>*。
    - *<directory-id>* を、作成したディレクトリの ID に。これは WorkSpaces コンソールで取得できます。

    のリソースでは AWS GovCloud (US) Regions、ARN に次の形式を使用します: `arn:aws-us-gov:workspaces:<region-code>:<account-id>:directory/<directory-id>`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:<region-code>:<account-
id>:directory/<directory-id>",
            "Condition": {
                "StringEquals": {"workspaces:userId": "${saml:sub}"}
            }
        }
    ]
}
```

22. [次へ] を選択します。
23. ポリシーの名前を入力し、[Create policy] (ポリシーの作成) を選択します。

## ステップ 6: SAML 2.0 ID プロバイダーを設定する

使用する SAML 2.0 IdP によっては、 AWS をサービスプロバイダーとして信頼するように IdP を手動で更新する必要があります。これを行うには、https://signin.aws.amazon.com/static/saml-metadata.xml にある `saml-metadata.xml` ファイルをダウンロードし、IdP にアップロードします。これによって、IdP のメタデータが更新されます。

一部の IdP では、すでに更新が設定されています。すでに設定されている場合は、この手順を省略できます。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、XML ファイルの URL をダッシュボードに入力するオプションが提供され、IdP がファイルを取得してインストールします。また、URL からファイルをダウンロードし、ダッシュボードにアップロードする必要があるプロバイダーもあります。

> **Important**
>
> このとき、IdP のユーザーに、IdP で設定した WorkSpaces アプリケーションへのアクセスを許可することもできます。ディレクトリの WorkSpaces アプリケーションにアクセスする権限を与えられているユーザーに対して、自動的に WorkSpace が作成されるわけではありません。同様に、WorkSpace が作成されるユーザーに対して、自動的に WorkSpaces アプリケーションへのアクセス権が与えられるわけではありません。SAML 2.0 認証を使用して

WorkSpace に正常に接続するには、ユーザーが IdP によって承認され、WorkSpace が作成されている必要があります。

## ステップ 7: SAML 認証レスポンスのアサーションを作成する

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 よっては、これはすでに設定されている場合があります。すでに設定されている場合は、この手順を省略できます。まだ設定されていない場合は、以下を指定します

- SAML サブジェクト名 ID – 署名するユーザーの一意の識別子。このフィールドの形式/値は変更しないでください。変更すると、ユーザーが別のユーザーとして扱われ、ホームフォルダが正常に機能しません。

  > **Note**
  >
  > ドメインに参加している WorkSpaces Pools の場合、ユーザーの `NameID` 値は、`sAMAccountName` を使用した `domain\username` 形式、`userPrincipalName` を使用した `username@domain.com` 形式、または `userName` のみで指定する必要があります。`sAMAccountName` 形式を使用している場合、NetBIOS 名または完全修飾ドメイン名 (FQDN) を使用してドメインを指定できます。Active Directory の一方向の信頼には、`sAMAccountName` 形式が必要です。詳細については、「WorkSpaces Pools での Active Directory の使用」を参照してください。`userName` だけを指定すると、ユーザーはプライマリドメインにログインすることになります。

- 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、IdP は特定のユーザーからのすべての SAML リクエストで `NameID` 要素に同じ一意の値を送信します。「ステップ 5: SAML 2.0 フェデレーション IAM ロールを作成する」のセクション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::<account-id>:role/<role-name>,arn:aws:iam::<account-id>:saml-provider/<provider-name>` です。
- **`Attribute Name`** 属性が https://aws.amazon.com/SAML/Attributes/RoleSessionName://www./www.jp に設定された 要素 — 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 1 つのAttributeValue要素が含まれています。AttributeValue 要素の値は 2 ~ 64 文字とし、英数字と _ . : / = + - @ の特殊文字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** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email に設定) — この要素には、ユーザーのメールアドレスを指定する AttributeValue 要素が 1 つ含まれます。この値は、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、「AWS Identity and Access Management 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。
- (オプション) **Attribute** 要素 (**Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName に設定) — 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と WorkSpaces Personal」を参照してください。
- (オプション) **Attribute** 要素 (**Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid に設定) — 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と WorkSpaces Personal」を参照してください。
- (オプション) **Attribute** 要素 (**Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain に設定) — この要素には、サインインしているユーザーの Active Directory DNS 完全修飾ドメイン名 (FQDN) を指定する AttributeValue 要素が 1 つ含まれます。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。値にはサブドメインを含め、domain.com の形式で指定する必要があります。
- (オプション) **Attribute** 要素 (**Name** 属性が https://aws.amazon.com/SAML/Attributes/SessionDuration に設定) — この要素には、再認証が必要となるまで、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アクティブのまま継続される最大時間を指定する AttributeValue 要素が 1 つ含まれます。デフォルト値は 3600 秒 (60 分) です。詳細については、「AWS Identity and Access Management ユーザーガイド」の「SessionDuration SAML 属性」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、セッション継続時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、セッションの有効期限が切れると切断されます。

これらの要素を設定する方法については、「AWS Identity and Access Management 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 8: フェデレーションのリレーステートを設定する

IdP を使用して、WorkSpaces Pools ディレクトリのリレーステートの 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 Pools ディレクトリエンドポイントに誘導されます。このエンドポイントは、SAML 認証レスポンスのリレー状態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
```

次の表に、WorkSpaces SAML 2.0 認証が利用可能な AWS 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 Pools 機能が利用できない AWS リージョンは削除されました。

| 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<br>• (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 |

| リージョン | リレーステートのエンドポイント |
| --- | --- |
| | • (FIPS) workspaces.euc-sso-fips.us-west-2.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 |
| 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 |

| リージョン | リレーステートのエンドポイント |
| --- | --- |
| AWS GovCloud (米国西部 ) | • workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com<br>• (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com<br><br>**Note**<br>AWS GovCloud (US) Regionsでの SAML IdP の使用について詳しくは、「AWS GovCloud (US) ユーザーガイド」の「Amazon WorkSpaces」を参照してください。 |
| AWS GovCloud (米国東部 ) | • workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com<br>• (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com<br><br>**Note**<br>AWS GovCloud (US) Regionsでの SAML IdP の使用について詳しくは、「AWS GovCloud (US) ユーザーガイド」の「Amazon WorkSpaces」を参照してください。 |

## ステップ 9: WorkSpace Pool ディレクトリで SAML 2.0 との統合を有効にする

WorkSpaces Pools ディレクトリで SAML 2.0 認証を有効にするには、次の手順を実行します。

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [Pools ディレクトリ] タブを選択します。
4. 編集するディレクトリの ID を選択します。
5. ページの [認証] セクションで [編集] を選択します。
6. [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。
7. [ユーザーアクセス URL] (「SSO URL」とも呼ばれます) で、プレースホルダーの値を IdP から提供された SSO URL に置き換えます。
8. [IdP ディープリンクパラメータ名] に、設定した IdP とアプリケーションに該当するパラメータを入力します。パラメータ名を省略した場合、デフォルト値は `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 とディープリンクパラメータ名を示します。

| 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.com/saml2/sp/ <app-id>/sso` |
| Okta | `RelayState` | `https://<sub-domain> .okta.com/app/<app-name> /<app-id>/sso/saml` |

| ID プロバイダー | パラメータ | ユーザーアクセス URL |
| --- | --- | --- |
| 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://*<default-tenant-name>* .us.auth0.com/samlp/ *<client-id>* |
| PingFederate | TargetResource | https://*<host>*/idp/startSSO.ping?PartnerSpId= *<sp-id>* |
| PingOne for Enterprise | TargetResource | https://sso.connect.pingidentity.com/sso/sp/initsso?saasid= *<app-id>*&idpid=*<idp-id>* |

9. [保存] を選択します。

> **Important**
>
> ユーザーの SAML 2.0 を取り消しても、セッションは直接切断されません。タイムアウトが発動した後にのみユーザーが削除されます。また、TerminateWorkspacesPoolSession API を使用してセッションを終了することもできます。

## トラブルシューティング

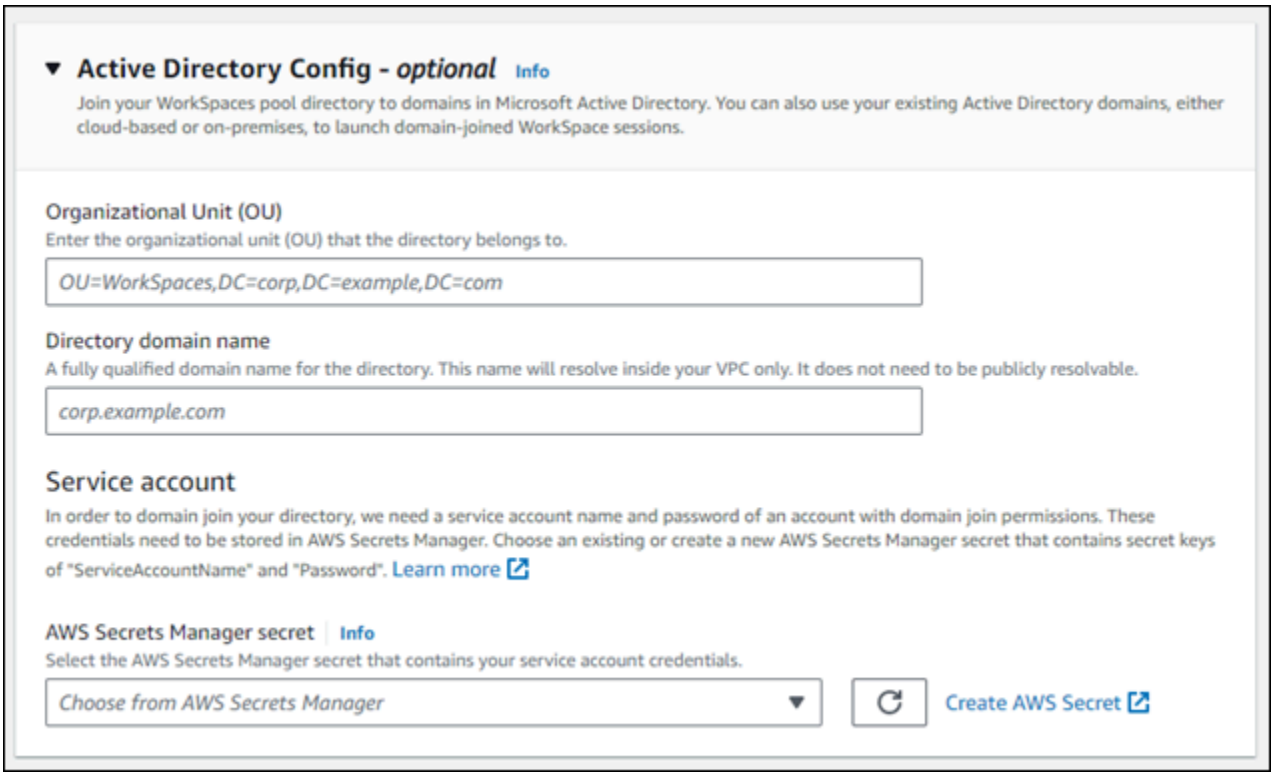
以下の情報は、WorkSpaces Pools に関する特定の問題のトラブルシューティングに役立ちます。

SAML 認証の完了後に WorkSpaces Pools クライアントで「ログインできない」というメッセージを受信しています

SAML クレームPrincipalTag:Emailの nameIDと は、Active Directory で設定されたユーザー名とパスワードと一致する必要があります。一部の IdP では、特定の属性を調整した後、更新、更新、再デプロイが必要になる場合があります。調整を行っても SAML キャプチャに反映されない場合は、変更を有効にするために必要な特定のステップについて、IdP のドキュメントまたはサポートプログラムを参照してください。

## WorkSpaces Pools ディレクトリの Active Directory 情報を指定する

このトピックでは、WorkSpaces コンソールの [WorkSpaces プールディレクトリの作成] ページで Active Directory (AD) の詳細を指定する方法を示します。WorkSpaces Pools で AD を使用する場合は、WorkSpaces Pools ディレクトリを作成するときに AD の詳細を指定する必要があります。WorkSpaces Pools ディレクトリの作成後に [Active Directory 設定] を編集することはできません。以下は、[WorkSpaces プールディレクトリの作成] ページの [Active Directory 設定] セクションの例です。




> **Note**
>
> WorkSpaces Pools ディレクトリを作成する完全なプロセスについては、「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」のトピックで説明しています。このペー

ジで説明されている手順は、WorkSpaces Pools ディレクトリを作成する完全なプロセスの一部の手順のみです。

トピック

- AD の組織単位とディレクトリドメイン名を指定する
- AD のサービスアカウントを指定する

## AD の組織単位とディレクトリドメイン名を指定する

[WorkSpaces プールディレクトリの作成] ページで、AD の組織単位 (OU) とディレクトリドメイン名を指定するには、次の手順を実行します。

1. [組織単位] にプールが属する OU を入力します。WorkSpace コンピュータアカウントは、WorkSpaces Pools ディレクトリに指定した組織単位 (OU) に配置されます。

   > **Note**
   >
   > OU 名にスペースを含めることはできません。スペースを含む OU 名を指定すると、Active Directory ドメインへの再参加を試みたときに、WorkSpaces はコンピュータオブジェクトを正しく循環できず、ドメインに再参加できません。

2. [ディレクトリ名] に、Active Directory ドメインの完全修飾ドメイン名 (FQDN) (例: `corp.example.com`) を入力します。各 AWS リージョンには、特定のディレクトリ名を持つディレクトリ設定値を 1 つだけ含めることができます。

   - WorkSpaces Pools ディレクトリを Microsoft Active Directory のドメインに参加させることができます。また、クラウドベースまたはオンプレミスの既存の Active Directory ドメインを使用して、ドメイン参加済みの WorkSpaces を起動することもできます。
   - また AWS Directory Service for Microsoft Active Directory、 を使用して Active Directory ドメイン AWS Managed Microsoft ADを作成することもできます。その後、そのドメインを使用して WorkSpaces リソースをサポートできます。
   - WorkSpaces を Active Directory ドメインに参加させると、以下のことを行うことができます。
     - ストリーミングセッションからプリンターやファイル共有などの Active Directory リソースにアクセスすることをユーザーとアプリケーションに許可する。

- グループポリシーマネジメントコンソール (GPMC) で使用できるグループポリシー設定を使用して、エンドユーザーエクスペリエンスを定義する。
- アクティブディレクトリログイン認証情報を使用した認証をユーザーに義務付けるアプリケーションをストリーミングする。
- WorkSpaces ストリーミングインスタンスに企業コンプライアンスとセキュリティポリシーを適用する。

3. [サービスアカウント] については、このページの次のセクション「AD のサービスアカウントを指定する」で説明します。

AD のサービスアカウントを指定する

ディレクトリ作成プロセスの一環として WorkSpaces Pools の Active Directory (AD) を設定する場合は、AD の管理に使用する AD サービスアカウントを指定する必要があります。そのためには、サービスアカウントの認証情報を指定する必要があります。認証情報は、 AWS Key Management Service （ AWS KMS) カスタマーマネージドキーを使用して に保存 AWS Secrets Manager および暗号化する必要があります。このセクションでは、 AWS KMS カスタマーマネージドキーと Secrets Manager シークレットを作成して、AD サービスアカウントの認証情報を保存する方法について説明します。

ステップ 1: AWS KMS カスタマーマネージドキーを作成する

AWS KMS カスタマーマネージドキーを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/kms で 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ーを使用します。
3. [キーの作成] を選択してから、[次へ] を選択します。
4. キーの種類として [対称]、キーの使用法として [暗号化および復号化] を選択し、[次へ] を選択します。
5. `WorkSpacesPoolDomainSecretKey` などのキーのエイリアスを入力し、[次へ] を選択します。
6. キー管理者は選択しません。[次へ] を選択して続行します。
7. キーの使用法アクセス許可は定義しません。[次へ] を選択して続行します。
8. ページの [キーポリシー] セクションで、以下を追加します。

```
        {
```

```
            "Sid": "Allow access for Workspaces SP",
            "Effect": "Allow",
            "Principal": {
                "Service": "workspaces.amazonaws.com"
            },
            "Action": "kms:Decrypt",
            "Resource": "*"
        }
```

結果は次の例のようになります。

```
"Statement": [
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::[redacted]:root"
        },
        "Action": "kms:*",
        "Resource": "*"
    },
    {
        "Sid": "Allow access for Workspaces SP",
        "Effect": "Allow",
        "Principal": {
            "Service": [
                "workspaces.amazonaws.com"
            ]
        },
        "Action": "kms:Decrypt",
        "Resource": "*"
    }
```

9. [Finish] を選択してください。

これで、 AWS KMS カスタマーマネージドキーを Secrets Manager で使用する準備ができました。このページの「ステップ 2: AD サービスアカウントの認証情報を保存する Secrets Manager シークレットを作成する」セクションに進みます。

## ステップ 2: AD サービスアカウントの認証情報を保存する Secrets Manager シークレットを作成する

次の手順に従って、AD サービスアカウントの認証情報を保存する Secrets Manager シークレットを作成します。

1. https://console.aws.amazon.com/secretsmanager/ で AWS Secrets Manager コンソールを開きます。

2. [新しいロールの作成] を選択します。
3. [他の種類のシークレット] を選択します。
4. 最初のキーと値のペアについては、キーに Service Account Name を入力し、値にサービスアカウントの名前 (domain\username など) を入力します。
5. 2 番目のキーと値のペアには、キーに Service Account Password、値にサービスアカウントのパスワードを入力します。
6. 暗号化キーで、前に作成した AWS KMS カスタマーマネージドキーを選択し、次へを選択します。
7. シークレットの名前 (WorkSpacesPoolDomainSecretAD など) を入力します。
8. ページの [リソースのアクセス許可] セクションで、[アクセス許可を編集する] を選択します。
9. 以下のアクセス許可ポリシーを入力します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "workspaces.amazonaws.com"
                ]
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

10. [保存] を選択してアクセス許可ポリシーを保存します。
11. [次へ] を選択して続行します。
12. 自動ローテーションは設定しません。[次へ] を選択して続行します。
13. [保存] を選択してシークレットの保存を終了します。

AD サービスアカウントの認証情報が Secrets Manager に保存されました。このページの「ステップ 3: AD サービスアカウントの認証情報が含まれる Secrets Manager シークレットを選択する」セクションに進みます。

ステップ 3: AD サービスアカウントの認証情報が含まれる Secrets Manager シークレットを選択する

次の手順を実行して、WorkSpaces Pools ディレクトリの Active Directory 設定で作成した Secrets Manager シークレットを選択します。

- サービスアカウントで、サービスアカウントの認証情報を含む AWS Secrets Manager シークレットを選択します。シークレットをまだ作成していない場合は、手順に従ってシークレットを作成します。シークレットは、 AWS Key Management Service カスタマーマネージドキーを使用して暗号化する必要があります。

これで、[WorkSpaces プールディレクトリの作成] ページの [Active Directory 設定] セクションのすべてのフィールドで入力が完了したので、WorkSpaces Pools ディレクトリの作成を続行できます。「ステップ 4: WorkSpace Pool ディレクトリを作成する」に移動し、手順 9 を開始します。

## WorkSpaces Pools のディレクトリ情報を更新する

WorkSpaces Pools 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。

### 認証

WorkSpaces Pools に追加の認証オプションを設定できます。プールには SAML 2.0 認証が必要です。

SAML 2.0 ID プロバイダー認証を有効にして設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. 認証に移動し、[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. [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. [ユーザーアクセス URL] に、フェデレーションサインイン中に WorkSpaces Pools クライアントを誘導する URL を入力します。
8. [IdP ディープリンクパラメータ名] (オプション) を入力します。
9. [保存] を選択します。

証明書ベースの認証を有効にして設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. 認証に移動し、[編集] を選択します。
5. [証明書ベースの認証の編集] を選択します。
6. [証明書ベースの認証を有効化] チェックボックスをオンにします。
7. [AWS Certificate Manager (ACM) Private Certificate Authority (CA)] をドロップダウンから選択します。
8. [保存] を選択します。

## セキュリティグループ

ディレクトリの WorkSpaces Pools にセキュリティグループを適用します。

WorkSpaces Pools のセキュリティグループを設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. セキュリティグループに移動し、[編集] を選択します。
5. ドロップダウンからセキュリティグループを選択します。

## Active Directory 設定

組織単位 (OU)、ディレクトリドメイン名、 AWS Secrets Manager シークレットを使用してディレクトリ Active Directory Config を設定します。

Active Directory を設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. Active Directory 設定に移動し、[編集] を選択します。
5. 組織単位 (OU) を検索するには、OU 名の全部または一部の入力を開始し、使用する OU を選択します。

> **Note**
>
> (オプション) OU の選択後、既存の WorkSpaces を再ビルドして OU を更新します。詳細については、WorkSpaces Personal の WorkSpace を再構築するを参照してください。

6. [保存] を選択します。

> **Note**
>
> ディレクトリドメイン名と AWS Secrets Manager シークレットは、プールの作成後に編集することはできません。

## ストリーミングプロパティ

プールされた WorkSpace とローカルデバイス間でユーザーがデータを転送する方法を設定します。

ストリーミングプロパティを設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. ストリーミングプロパティに移動し、[編集] を選択します。
5. 以下のストリーミングプロパティを設定します。

   - クリップボードのアクセス許可
     - ドロップダウンリストから次のいずれかを選択します。
       - コピーアンドペーストを許可する - ローカルデバイスへのコピーとリモートセッションへの貼り付けを許可します。

    - リモートセッションへのペーストを許可する - リモートセッションへの貼り付けを許可します。
    - ローカルデバイスへのコピーを許可する - ローカルデバイスへのコピーを許可します。
    - 無効
  - ローカルデバイスへの出力を許可するかしないかを選択します。
  - 診断ログを許可するかしないかを選択します。
  - スマートカードサインインを許可するかしないかを選択します。
  - ホームフォルダストレージを有効にするには、[ホームフォルダを有効化] を選択します。
6. [保存] を選択します。

## IAM ロール

WorkSpaces Pools の IAM ロールを選択します。

IAM ロールを選択するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. IAM ロールに移動し、[編集] を選択します。
5. ドロップダウンから IAM ロールを選択します。新しい IAM ロールを作成するには、[新しい IAM ロールを作成] を選択します。
6. [保存] を選択します。

## [タグ]

WorkSpaces Pools に新しいタグを追加する

新しいタグを追加するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. 設定するディレクトリを選択します。
4. [タグ] に移動し、[タグの管理] を選択します。
5. [新しいタグの追加] を選択し、使用するキーと値のペアを入力します。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。
6. [Save changes] (変更の保存) をクリックします。

## WorkSpaces Pools ディレクトリの登録を解除する

WorkSpaces Pools ディレクトリの登録を解除するには、次の手順を実行します。

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [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。

# WorkSpaces Pools のネットワークとアクセス

以下のトピックでは、ユーザーの WorkSpaces Pools への接続、および WorkSpaces Pools からネットワークリソースとインターネットへのアクセスを有効にするための情報を提供します。

内容

# WorkSpaces Pools のインターネットアクセス

WorkSpaces Pools の WorkSpaces でインターネットアクセスが必要な場合は、いくつかの方法で有効にできます。インターネットアクセスを有効にする方法を選択するときは、デプロイでサポートする必要があるユーザーの数とデプロイの目標を考慮してください。次に例を示します:

- デプロイで 100 を超える同時実行ユーザーをサポートする必要がある場合は、プライベートサブネットと NAT ゲートウェイを使用して VPC を設定します。
- デプロイでサポートされる同時実行ユーザー数が 100 未満の場合は、パブリックサブネットを使用して新規または既存の VPC を設定できます。
- デプロイでサポートされる同時実行ユーザー数が 100 未満で、WorkSpaces Pools を初めて導入しサービスの使用を開始する場合は、デフォルトの VPC、パブリックサブネット、セキュリティグループを使用できます。

以下のセクションでは、これらの各デプロイオプションについて詳しく説明します。

- 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 (推奨) — この設定では、プライベートサブネットで WorkSpaces Pools ビルダーを起動し、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。ストリーミングインスタンスには、インターネットから直接アクセスできないプライベート IP アドレスが割り当てられます。

  また、[既定のインターネットアクセス] オプションを使用してインターネットアクセスを有効にする設定とは異なり、NAT 設定 では WorkSpaces Pools の WorkSpaces 数が 100 に制限されません。デプロイで 100 を超える同時ユーザーをサポートする必要がある場合は、この設定を使用します。

  NAT ゲートウェイで使用する新しい VPC を作成して設定することも、既存の VPC に NAT ゲートウェイを追加することもできます。
- パブリックサブネットを使用して新しい VPC または既存の VPC を設定する — この設定では、WorkSpaces Pools をパブリックサブネットで起動します。このオプションを有効にすると、WorkSpaces Pools は Amazon VPC パブリックサブネットのインターネットゲートウェイを使用してインターネット接続を提供します。ストリーミングインスタンスには、インターネットから直接アクセスできるパブリック IP アドレスが割り当てられます。この目的のために、新しい VPC を作成するか、既存の VPC を設定できます。

> **Note**
>
> パブリックサブネットを使用して新規または既存の VPC を設定する場合、WorkSpaces Pools で最大 100 の WorkSpaces がサポートされます。デプロイで 100 を超える同時ユーザーをサポートする必要がある場合は、代わりにNAT ゲートウェイ設定を使用します。

- デフォルト VPC、パブリックサブネット、およびセキュリティグループの使用 — WorkSpaces Pools を初めて導入してサービスの使用を開始する場合は、デフォルトのパブリックサブネットで WorkSpaces Pools を起動できます。このオプションを有効にすると、WorkSpaces Pools は Amazon VPC パブリックサブネットのインターネットゲートウェイを使用してインターネット接続を提供します。ストリーミングインスタンスには、インターネットから直接アクセスできるパブリック IP アドレスが割り当てられます。

  デフォルトの VPC は、2013 年 12 月 4 日以降に作成された Amazon Web Services アカウントで使用できます。

  デフォルト VPC には、各アベイラビリティーゾーンのデフォルトのパブリックサブネットと、VPC にアタッチされたインターネットゲートウェイが含まれます。VPC にはデフォルトのセキュリティグループも含まれます。

  > **Note**
  >
  > デフォルトの VPC、パブリックサブネット、セキュリティグループを使用する場合、WorkSpaces Pools で最大 100 の WorkSpaces がサポートされます。デプロイで 100 を超える同時ユーザーをサポートする必要がある場合は、代わりにNAT ゲートウェイ設定を使用します。

## WorkSpaces Pools 用に VPC を設定する

WorkSpaces Pools を設定するときに、WorkSpaces を起動する仮想プライベートクラウド (VPC) と、少なくとも 1 つのサブネットを指定する必要があります。VPC は、Amazon Web Services クラウド内の論理的に分離された領域にある仮想ネットワークです。サブネットは、VPC の IP アドレスの範囲です。

VPC を WorkSpaces Pools に設定する場合、パブリックサブネットとプライベートサブネットのいずれか、または両方のタイプのサブネットを組み合わせて指定できます。パブリックサブネットは、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直接アクセスできます。インターネットゲー

トウェイへのルートを持たないプライベートサブネットには、インターネットへのアクセスを提供するためにネットワークアドレス変換 (NAT) ゲートウェイまたは NAT インスタンスが必要です。

内容



## WorkSpaces Pools の VPC セットアップの推奨事項

WorkSpaces Pools を作成するときは、VPC および使用する 1 つ以上のサブネットを指定します。セキュリティグループを指定することで、VPC に対する追加のアクセスコントロールを提供できます。

以下の推奨事項は、VPC をより効果的かつ安全に設定するのに役立ちます。また、WorkSpaces Pools の効果的なスケーリングをサポートする環境の設定にも役立ちます。WorkSpaces Pools の効果的なスケーリングにより、不必要なリソースの使用と関連コストを回避しながら、WorkSpaces Pools ユーザーの現在の需要や予想される需要に対応できます。

VPC 全体の設定

- WorkSpaces Pools のスケーリングのニーズに確実に対応できる VPC 設定にします。

  WorkSpaces Pools のスケーリングの計画を作成する際には、1 人のユーザーが 1 つの WorkSpaces を必要とすることに注意してください。したがって、WorkSpaces Pools のサイズによって、同時にストリーミングできるユーザーの数が決まります。このため、使用するインスタンスタイプごとに、VPC がサポートできる WorkSpaces の数が、同じインスタンスタイプで予想される同時ユーザー数よりも多いことを確認します。
- WorkSpaces Pools アカウントのクォータ (制限とも呼ばれる) が、予想される需要に対応するのに十分であることを確認します。クォータの引き上げをリクエストするには、https://console.aws.amazon.com/servicequotas/ の [Service Quotas] コンソールを使用します。デフォルトの WorkSpaces Pools クォータに関する情報は、「Amazon WorkSpaces のクォータ」を参照してください。
- WorkSpaces Pools の WorkSpaces にインターネットへのアクセスを提供する場合は、ストリーミングインスタンス用の 2 つのプライベートサブネットと、パブリックサブネットの NAT ゲートウェイで、VPC を設定することをお勧めします。

NAT ゲートウェイを使用すると、プライベートサブネットの WorkSpaces をインターネットや他の AWS サービスに接続できます。ただし、インターネットはこれらの WorkSpaces との接続を開始できません。また、[既定のインターネットアクセス] オプションを使用してインターネットアクセスを有効にする設定とは異なり、NAT 設定 では 100 以上の WorkSpaces がサポートされます。詳細については、「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」を参照してください。

弾性ネットワークインターフェース

- WorkSpaces Pools は、WorkSpaces Pools で必要となる最大容量と同等の Elastic Network Interface (ネットワークインターフェイス) を作成します。デフォルトでは、リージョンごとのネットワークインターフェイスの制限は 5000 です。

  何千もの WorkSpaces など、非常に大規模なデプロイの容量を計画する場合は、同じリージョンで使用される Amazon EC2 インスタンスの数も考慮してください。

サブネット

- VPC に複数のプライベートサブネットを設定する場合は、それぞれを異なるアベイラビリティーゾーンで設定します。これにより、耐障害性が向上し、容量不足エラーを防ぐことができます。同じ AZ で 2 つのサブネットを使用する場合、WorkSpaces Pools は 2 つ目のサブネットを使用しないため、IP アドレスが不足する可能性があります。
- アプリケーションに必要なネットワークリソースが、両方のプライベートサブネットを通じてアクセスできることを確認します。
- 各プライベートサブネットに、予想される同時ユーザーの最大数を考慮するのに十分な数のクライアント IP アドレスを許可するサブネットマスクを設定します。また、予想される増加に対応するために、追加の IP アドレスを許可します。詳細については、VPC and Subnet Sizing for IPv4 を参照してください。
- NAT で VPC を使用している場合は、インターネットアクセス用の NAT ゲートウェイを持つパブリックサブネットを少なくとも 1 つ、できれば 2 つ設定します。プライベートサブネットが存在する同じアベイラビリティーゾーンにパブリックサブネットを設定します。

  WorkSpaces Pools の大規模なデプロイで耐障害性を強化し、容量不足エラーの可能性を軽減するために、VPC 設定を 3 番目のアベイラビリティーゾーンに拡張することを検討してください。この追加のアベイラビリティーゾーンに、プライベートサブネット、パブリックサブネット、および NAT ゲートウェイを含めます。

セキュリティグループ

- セキュリティグループを使用して、VPC への追加のアクセスコントロールを提供します。

  VPC に属するセキュリティグループを使用すると、WorkSpaces Pools ストリーミングインスタンスとアプリケーションに必要なネットワークリソースの間のネットワークトラフィックを制御できます。これらのリソースには、Amazon RDS や Amazon FSx、ライセンスサーバー、データベースサーバー、ファイルサーバー、アプリケーションサーバーなどの他の AWS サービスが含まれる場合があります。
- アプリケーションに必要なネットワークリソースへのアクセスが、セキュリティグループで許可されていることを確認してください。

  セキュリティグループに関する一般的な情報については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用して AWS リソースへのトラフィックを制御する」を参照してください。

## 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

WorkSpaces Pools の WorkSpaces にインターネットへのアクセスを提供する場合は、WorkSpaces 用の 2 つのプライベートサブネットと、パブリックサブネットの NAT ゲートウェイで、VPC を設定することをお勧めします。NAT ゲートウェイで使用する新しい VPC を作成して設定することも、既存の VPC に NAT ゲートウェイを追加することもできます。VPC 設定のその他の推奨事項については、WorkSpaces Pools の VPC セットアップの推奨事項 を参照してください。

NAT ゲートウェイは、プライベートサブネットの WorkSpaces がインターネットまたは他の AWS サービスに接続できるようにしますが、インターネットがそれらの WorkSpaces との接続を開始できないようにします。また、[既定のインターネットアクセス] オプションを使用して WorkSpaces のインターネットアクセスを有効にする設定とは異なり、この設定では WorkSpaces 数が 100 に制限されません。

NAT ゲートウェイと本設定の使用については、Amazon VPC ユーザーガイドの NAT Gateways と VPC with Public and Private Subnets (NAT) を参照してください。

内容

- 新しい VPC の作成と設定
- 既存の VPC に NAT ゲートウェイを追加する
- WorkSpaces Pools のインターネットアクセスを有効にする

新しい VPC の作成と設定

このトピックでは、VPC ウィザードを使用して、パブリックサブネットと 1 つのプライベートサブネットを持つ VPC を作成する方法について説明します。このプロセスの一環として、ウィザードはインターネットゲートウェイと NAT ゲートウェイを作成します。また、パブリックサブネットに関連付けられたカスタムルートテーブルを作成し、プライベートサブネットに関連付けられたメインルートテーブルを更新します。NAT ゲートウェイは、VPC のパブリックサブネットで自動的に作成されます。

ウィザードを使用して初期 VPC 設定を作成したら、2 つ目のプライベートサブネットを追加します。この設定の詳細については、Amazon VPC ユーザーガイドの VPC with Public and Private Subnets (NAT) を参照してください。

> **Note**
>
> すでに VPC がある場合は、代わりに、既存の VPC に NAT ゲートウェイを追加する のステップを実行します。

目次



ステップ 1: Elastic IP アドレスの割り当て

VPC を作成する前に、WorkSpaces リージョンに Elastic IP アドレスを割り当てる必要があります。最初に VPC で使用する Elastic IP アドレスを割り当てて、NAT ゲートウェイに関連付ける必要があります。詳細については、Amazon VPC ユーザーガイドの Elastic IP Addresses を参照してください。

> **Note**
>
> 使用する Elastic IP アドレスには料金が適用される場合があります。詳しい情報については、Amazon EC2 の料金ページの Elastic IP Addresses を参照してください。

Elastic IP アドレスをまだ持っていない場合は、以下のステップを実行します。既存の Elastic IP アドレスを使用する場合は、そのアドレスが別のインスタンスやネットワークインターフェイスに現在関連付けられていないことを確認します。

Elastic IP アドレスを割り当てるには

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の [Network & Security] で、[Elastic IPs] を選択します。
3. [Allocate New Address (新しいアドレスの割り当て)] を選択し、続いて [Allocate (割り当て)] を選択します。
4. Elastic IP アドレスを書き留めます。
5. [Elastic IP] ペインの右上にある [X] アイコンをクリックしてペインを閉じます。

ステップ 2: 新しい VPC を作成する

パブリックサブネットと 1 つのプライベートサブネットを持つ新しい VPC を作成するには、次のステップを実行します。

新しい 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. ナビゲーションペインで、[VPC ダッシュボード] を選択します。
3. Launch VPC Wizard (VPC ウィザードの起動 ) を選択します。
4. [Step 1: Select a VPC Configuration (ステップ 1: VPC 設定を選択する)] ページで [VPC with Public and Private Subnets (パブリックサブネットとプライベートサブネットを持つ VPC)] を選択し、[Select (選択)] を選択します。
5. [Step 2: VPC with Public and Private Subnets (ステップ 2: パブリックサブネットとプライベートサブネットを持つ VPC)] で、VPC を次のように設定します。
   - [IPv4 CIDR block (IPv4 CIDR ブロック)] では、VPC 用の IPv4 CIDR ブロックを指定します。
   - [IPv6 CIDR ブロック] は、デフォルト値の、[No IPv6 CIDR Block (IPv6 CIDR ブロックなし)] のままにしておきます。
   - [VPC name (VPC 名)] にキーの一意の名前を入力します。
6. パブリックサブネットを次のように設定します。

- [Public subnet's IPv4 CIDR (パブリックサブネットの IPv4 CIDR)] に、サブネットの CIDR ブロックを指定します。
- [Availability Zone (アベイラビリティーゾーン)] では、デフォルト値の、[No Preference (指定なし)] のままにしておきます。
- [Public subnet name (パブリックサブネット名)] に、サブネットの名前を入力します (例: `WorkSpaces Public Subnet`)。

7. 最初のプライベートサブネットを次のように設定します。

   - [Private subnet's IPv4 CIDR (プライベートサブネットの IPv4 CIDR)] に、サブネットの CIDR ブロックを入力します。指定した値を書き留めておきます。
   - [Availability Zone (アベイラビリティーゾーン)] で、特定のゾーンを選択し、選択したゾーンを書き留めます。
   - [Private subnet name (プライベートサブネット名)] に、サブネットの名前を入力します (例: `WorkSpaces Private Subnet1`)。
   - 残りのフィールドについては、該当する場合は、デフォルト値をそのまま使用します。

8. [Elastic IP Allocation ID (Elastic IP 割り当て ID)] で、テキストボックスをクリックし、作成した Elastic IP アドレスに対応する値を選択します。このアドレスは NAT ゲートウェイに割り当てられます。Elastic IP アドレスがない場合は、https://console.aws.amazon.com/vpc/ の Amazon VPC コンソールを使用して作成します。

9. [Service endpoints (サービスエンドポイント)] で、環境に Amazon S3 エンドポイントが必要な場合は、エンドポイントを指定します。S3 エンドポイントは、ユーザーにホームフォルダへのアクセスを提供したり、プライベートネットワークのユーザーに対してアプリケーション設定の永続性を有効にしたりするために必要です。

   Amazon S3 エンドポイントを指定するには、次の手順を実行します。

   a. [Add Endpoint (エンドポイントの追加)] を選択します。
   b. [Service (サービス)] で、末尾が「s3」( VPC が作成されるリージョンに対応する `com.amazonaws.`*`region`*`.s3` エントリ ) で終わるエントリをリストから選択します。
   c. [Subnet (サブネット)] で、[Private subnet (プライベートサブネット)] を選択します。
   d. [Policy (ポリシー)] では、既定値の [Full Access (フルアクセス)] のままにします。

10. [Enable DNS hostnames (DNS ホスト名を有効にする)] では、デフォルト値の [Yes (はい)] のままにします。

11. [Hardware tenancy (ハードウェアテナンシー)] では、デフォルト値の [Default (デフォルト)] のままにします。
12. [Create VPC] を選択します。
13. VPC の設定には数分かかることに注意してください。VPC が作成されたら、[OK] を選択します。

### ステップ 3: 2 番目のプライベートサブネットの追加

前のステップ (ステップ 2: 新しい VPC を作成する) で、1 つのパブリックサブネットと 1 つのプライベートサブネットを持つ VPC を作成しました。2 つ目のプライベートサブネットを追加するには、以下のステップを実行します。1 つ目のプライベートサブネットとは異なるアベイラビリティーゾーンに 2 つ目のプライベートサブネットを追加することをお勧めします。

1. ナビゲーションペインで、[サブネット] を選択してください。
2. 前のステップで作成した最初のプライベートサブネットを選択します。サブネットのリストの下にある [Description (説明)] タブで、このサブネットのアベイラビリティーゾーンを書き留めます。
3. サブネットペインの左上にある [Create Subnet (サブネットの作成)] を選択します。
4. [Name tag (名前タグ)] に、プライベートサブネットの名前を入力します (例: `WorkSpaces Private Subnet2`)。
5. [VPC] では、前のステップで作成した VPC を選択します。
6. [Availability Zone (アベイラビリティーゾーン)] で、最初のプライベートサブネットに使用しているアベイラビリティーゾーン以外のアベイラビリティーゾーンを選択します。別のアベイラビリティーゾーンを選択すると、耐障害性が向上し、容量不足エラーを防ぐのに役立ちます。
7. [IPv4 CIDR block (IPv4 CIDR ブロック)] の場合は、新しいサブネットの一意の CIDR ブロック範囲を指定します。たとえば、最初のプライベートサブネットの IPv4 CIDR ブロック範囲が `10.0.1.0/24` である場合、新しいプライベートサブネットに `10.0.2.0/24` CIDR ブロック範囲を指定できます。
8. [Create] (作成) を選択します。
9. サブネットが作成されたら、[Close (閉じる)] を選択します。

### ステップ 4: サブネットルートテーブルの検証と名前付け

VPC を作成して設定したら、以下のステップを実行してルートテーブルの名前を指定し、そのことを確認します。

- NAT ゲートウェイが存在するサブネットに関連付けられたルートテーブルには、インターネットゲートウェイへのインターネットトラフィックを指すルートが含まれます。これにより、NAT ゲートウェイがインターネットにアクセスできるようになります。
- プライベートサブネットに関連付けられたルートテーブルは、インターネットトラフィックを NAT ゲートウェイに向けるように設定されます。これにより、プライベートサブネットのストリーミングインスタンスがインターネットと通信できるようになります。

1. ナビゲーションペインで [Subnets (サブネット)] を選択し、作成したパブリックサブネットを選択します (例: `WorkSpaces Public Subnet`)。

   a. [Route Table (ルートテーブル)] タブで、ルートテーブルの ID を選択します ( たとえば、`rtb-12345678` ) 。

   b. ルートテーブルを選択します。[名前] の下で編集アイコン ( 鉛筆 ) を選択し、名前 ( 例: `workspaces-public-routetable` ) を入力してから、チェックマークを選択して名前を保存します。

   c. パブリックルートテーブルを選択したまま、[ルート] タブで、ローカルトラフィック用に 1 つのルートが存在し、他のすべてのトラフィックをインターネットゲートウェイに送信する VPC 用の別のルートがあることを確認します。以下のテーブルでは、これらの 2 つのルートについて説明しています。

| 送信先 | ターゲット | 説明 |
| --- | --- | --- |
| パブリックサブネット IPv4 CIDR ブロック ( 10.0.0.0/20 など ) | ローカル | パブリックサブネット IPv4 CIDR ブロック内の IPv4 アドレス宛てのリソースからのトラフィックはすべて、VPC 内でローカルにルーティングされます。 |
| その他のすべての IPv4 アドレス宛てのトラフィック ( 0.0.0.0/0 など ) | アウトバウンド (`igw-`*`ID`*) | その他すべての IPv4 アドレス宛てのトラフィックは、VPC ウィザードで作成されたインターネットゲートウェイ ( `igw-`*`ID`*で識別 ) にルーティングされます。 |

2. ナビゲーションペインで [サブネット] を選択し、作成した最初のプライベートサブネットを選択します (例: `WorkSpaces Private Subnet1`)。

a. [ルートテーブル] タブで、ルートテーブルの ID を選択します。

b. ルートテーブルを選択します。[名前] の下で編集アイコン (鉛筆) を選択し、名前 (例: `workspaces-private-routetable`) を入力してから、チェックマークを選択して名前を保存します。

c. [Routes (ルート)] タブで、ルートテーブルに次のルートが含まれていることを確認します。

| 送信先 | ターゲット | 説明 |
| --- | --- | --- |
| パブリックサブネット IPv4 CIDR ブロック ( 10.0.0/20 など ) | ローカル | パブリックサブネット IPv4 CIDR ブロック内の IPv4 アドレス宛てのリソースからのトラフィックはすべて、VPC 内でローカルにルーティングされます。 |
| その他のすべての IPv4 アドレス宛てのトラフィック ( 0.0.0.0/0 など ) | アウトバウンド (nat-*ID*) | その他すべての IPv4 アドレス宛てのトラフィックは、NAT ゲートウェイ ( nat-*ID*で識別 ) にルーティングされます。 |
| S3 バケット宛てのトラフィック ( S3 エンドポイントを指定した場合に適用 )<br><br>[pl-*ID* (com.amazonaws. *#####.s3*)] | ストレージ (vpce-*ID*) | S3 バケット宛てのトラフィックは、S3 エンドポイント ( vpce-*ID* で識別 ) にルーティングされます。 |

3. ナビゲーションペインで [サブネット] を選択し、作成した 2 番目のプライベートサブネットを選択します (例: `WorkSpaces Private Subnet2`)。

4. [ルートテーブル] タブで、ルートテーブルがプライベートルートテーブルであることを確認します (例: `workspaces-private-routetable`)。ルートテーブルが異なる場合は、[編集] を選択してこのルートテーブルを選択します。

次のステップ

WorkSpaces Pools の WorkSpaces でインターネットにアクセスできるようにするには、「WorkSpaces Pools のインターネットアクセスを有効にする」の手順を実行します。

### 既存の VPC に NAT ゲートウェイを追加する

すでに VPC を設定している場合は、次のステップを実行して NAT ゲートウェイを VPC に追加します。新しい VPC を作成する必要がある場合は、「新しい VPC の作成と設定」を参照してください。

既存の VPC に NAT ゲートウェイを追加するには

1. NAT ゲートウェイを作成するには、Amazon VPC ユーザーガイドの Creating a NAT Gateway の手順を完了します。
2. VPC に少なくとも 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。高可用性と耐障害性のために異なるアベイラビリティーゾーンから 2 つのプライベートサブネットを指定することをお勧めします。2 番目のプライベートサブネットを作成する方法については、「ステップ 3: 2 番目のプライベートサブネットの追加」を参照してください。
3. 1 つ以上のプライベートサブネットに関連付けられたルートテーブルを更新して、インターネットバウンドトラフィックを NAT ゲートウェイに向かわせます。これにより、プライベートサブネットのストリーミングインスタンスがインターネットと通信できるようになります。そのためには、Amazon VPC ユーザーガイドの Updating Your Route Table の手順を完了してください。

### 次のステップ

WorkSpaces Pools の WorkSpaces でインターネットにアクセスできるようにするには、「WorkSpaces Pools のインターネットアクセスを有効にする」の手順を実行します。

WorkSpaces Pools のインターネットアクセスを有効にする

NAT ゲートウェイが VPC で利用可能になったら、WorkSpaces Pools でインターネットアクセスを有効にできます。WorkSpaces Pools ディレクトリ を作成するときに、インターネットアクセスを有効にできます。ディレクトリの作成時に NAT ゲートウェイを持つ VPC を選択します。次に、[サブネット 1] にプライベートサブネットを選択し、オプションで [サブネット 2] に別のプライベートサブネットを選択します。VPC にプライベートサブネットがない場合は、2 つ目のプライベートサブネットを作成する必要があります。

WorkSpaces Pools を開始し、プール内の WorkSpace に接続してインターネット参照を行うことによって、インターネット接続をテストできます。

## パブリックサブネットを使用して新しい VPC または既存の VPC を設定する

2013-12-04 以降に Amazon Web Services アカウントを作成した場合は、各 AWS リージョンにデフォルトのパブリックサブネットを含むデフォルトの VPC があります。ただし、WorkSpaces

Pools ディレクトリで使用するために、デフォルト以外の独自の VPC を作成することも、既存の VPC を設定することもできます。このトピックでは、WorkSpaces Pools で使用するデフォルト以外の VPC とパブリックサブネットを設定する方法について説明します。

VPC とパブリックサブネットを設定したら、[既定のインターネットアクセス] オプションを有効にすることで WorkSpaces Pools の WorkSpaces にインターネットへのアクセスを提供できます。このオプションを有効にすると、WorkSpaces Pools では、ストリーミングインスタンスからパブリックサブネットにアタッチされたネットワークインターフェイスに Elastic IP アドレスを関連付けることにより、インターネット接続が有効になります。Elastic IP アドレスは、インターネットからアクセス可能なパブリック IPv4 アドレスです。このため、WorkSpaces Pools の WorkSpaces へのインターネットアクセスを提供する際には NAT ゲートウェイを使用することをお勧めします。また、[既定のインターネットアクセス] が有効になっている場合、最大 100 の WorkSpaces がサポートされます。デプロイで 100 を超える同時ユーザーをサポートする必要がある場合は、代わりにNAT ゲートウェイ設定を使用します。

詳細については、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のステップを参照してください。VPC 設定のその他の推奨事項については、WorkSpaces Pools の VPC セットアップの推奨事項 を参照してください。

目次



## ステップ 1: パブリックサブネットで VPC を設定する

以下のいずれかの方法を使用して、パブリックサブネットで既定以外の独自の VPC を設定できます。

- 1 つのパブリックサブネットを持つ VPC を作成する
- 既存の VPC を設定する

### 1 つのパブリックサブネットを持つ VPC を作成する

VPC ウィザードを使用して新しい VPC を作成すると、ウィザードによってインターネットゲートウェイとパブリックサブネットに関連付けられたカスタムルートテーブルが作成されます。ルートテーブルは、VPC の外部のアドレスを宛先とするすべてのトラフィックをインターネットゲートウェイにルーティングします。この設定の詳細については、Amazon VPC ユーザーガイドの VPC with a Single Public Subnet を参照してください。

1. Amazon VPC ユーザーガイドの Step 1: Create the VPC のステップを実行して、VPC を作成します。
2. WorkSpaces でインターネットにアクセスできるようにするには、「ステップ 2: WorkSpaces Pools の既定のインターネットアクセスを有効にする」の手順を実行します。

### 既存の VPC を設定する

パブリックサブネットが設定されていない既存の VPC を使用する場合は、新しいパブリックサブネットを追加します。パブリックサブネットに加えて、VPC にインターネットゲートウェイをアタッチし、VPC 外部のアドレス宛てのすべてのトラフィックをインターネットゲートウェイにルーティングするルートテーブルも必要です。これらのコンポーネントを設定するには、次のステップを実行します。

1. パブリックサブネットを追加するには、Creating a Subnet in Your VPC のステップを実行します。WorkSpaces Pools で使用する予定の既存の VPC を使用します。

   VPC が IPv6 アドレス指定をサポートするように設定されている場合、[IPv6 CIDR block (IPv6 CIDR ブロック)] リストが表示されます。[Don't assign Ipv6 (Ipv6 を割り当てない)] を選択します。
2. インターネットゲートウェイを作成して VPC にアタッチするには、Creating and Attaching an Internet Gateway のステップを実行します。
3. インターネットトラフィックがインターネットゲートウェイを介してルーティングされるようにサブネットを設定するには、Creating a Custom Route Table に記載されているステップに従います。ステップ 5 では、[Destination (宛先)] に IPv4 形式 (`0.0.0.0/0`) を使用します。
4. WorkSpaces と Image Builder がインターネットにアクセスできるようにするには、「ステップ 2: WorkSpaces Pools の既定のインターネットアクセスを有効にする」の手順を実行します。

### ステップ 2: WorkSpaces Pools の既定のインターネットアクセスを有効にする

WorkSpaces Pools ディレクトリ を作成するときに、インターネットアクセスを有効にできます。ディレクトリの作成時に、パブリックサブネットを持つ VPC を選択します。次に、[サブネット 1] でパブリックサブネットを選択し、オプションで [サブネット 2] に別のパブリックサブネットを選択します。

WorkSpaces Pools を開始し、プール内の WorkSpace に接続してインターネット参照を行うことによって、インターネット接続をテストできます。

# デフォルト VPC、パブリックサブネット、およびセキュリティグループの使用

2013-12-04 以降に作成された Amazon Web Services アカウントには、各 AWS リージョンにデフォルトの VPC があります。デフォルト VPC には、各アベイラビリティーゾーンのデフォルトのパブリックサブネットと、VPC にアタッチされたインターネットゲートウェイが含まれます。VPC にはデフォルトのセキュリティグループも含まれます。WorkSpaces Pools を初めて導入してサービスの使用を開始する場合は、WorkSpaces Pools を作成するときに、デフォルトの VPC とセキュリティグループを選択したままにしておくことができます。次に、少なくとも 1 つのデフォルトサブネットを選択できます。

> **Note**
>
> Amazon Web Services アカウントが 2013 年 12 月 4 日より前に作成されている場合は、新しい VPC を作成するか、既存の VPC を WorkSpaces Pools で使用するように設定する必要があります。WorkSpaces Pools 用の 2 つのプライベートサブネットと、パブリックサブネットの NAT ゲートウェイで、VPC を手動で設定することをお勧めします。詳細については、「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」を参照してください。または、パブリックサブネットでデフォルト以外の VPC を設定することもできます。詳細については、「パブリックサブネットを使用して新しい VPC または既存の VPC を設定する」を参照してください。

WorkSpaces Pools ディレクトリ を作成するときに、インターネットアクセスを有効にできます。

ディレクトリの作成時にデフォルトの VPC を選択します。デフォルトの VPC 名では、`vpc-`*`vpc-id`* `(No_default_value_Name)` という形式が使用されます。

次に、[サブネット 1] でデフォルトのパブリックサブネットを選択し、オプションとして [サブネット 2] で別のデフォルトのパブリックサブネットを選択します。デフォルトのサブネット名は、`subnet-`*`subnet-id`* `|` *`(IPv4 CIDR ####)`* `| Default in` *`availability-zone`* の形式を使用します。

WorkSpaces Pools を開始し、プール内の WorkSpace に接続してインターネット参照を行うことによって、インターネット接続をテストできます。

# WorkSpaces Pools の FedRAMP 認可または DoD SRG コンプライアンスを設定する

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 Pools を設定する必要があります。また、FedRAMP 認可を持っているか、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 認可レベル (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 認可と DoD SRG コンプライアンスのレベルについては、「コンプライアンスプログラムによる対象範囲内のAWS のサービス」を参照してください。

要件

- WorkSpaces Pools 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、以下を確認してください。
>
> - WorkSpaces Pools ディレクトリは次のいずれかです。
>   - 新規でプールに関連付けられていない
>   - STOPPED 状態の既存のプールに関連付けられます
> - Pool ディレクトリは TCP に`StreamingExperiencePreferredProtocol`設定されています。

- WorkSpaces Pools は、FedRAMP 認可を持つ、または DoD SRG に準拠している米国 AWS リージョンで作成する必要があります。
- 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。
  - macOS: 5.20.0 以降
  - Windows: 5.20.0 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/v2/home「https://www.com 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、FedRAMP 認可と DoD SRG コンプライアンスに使用するディレクトリを選択します。
3. ディレクトリの詳細ページで、FIPS 暗号化モードに設定するディレクトリを選択します。
4. エンドポイント暗号化セクションで、編集 を選択し、FIPS 140-2 検証モードを選択します。
5. [保存] を選択します。

## WorkSpaces Pools 機能で Amazon S3 VPC エンドポイントを使用する

WorkSpaces Pools のアプリケーション設定の永続化または WorkSpaces Pools ディレクトリのホームフォルダを有効にすると、WorkSpaces はディレクトリに指定した VPC を使用して Amazon Simple Storage Service (Amazon S3) バケットへのアクセスを提供します。WorkSpaces Pools からプライベート S3 エンドポイントへのアクセスを有効にするには、以下のカスタムポリシーを Amazon S3 の VPC エンドポイントにアタッチします。プライベート Amazon S3 エンドポイントの詳細については、Amazon VPC ユーザーガイドの VPC Endpoints および Endpoints for Amazon S3 を参照してください。

Commercial AWS リージョン

商用 AWS リージョンのリソースには、次のポリシーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<account-id>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
```

```
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ]
        }
    ]
}
```

### AWS GovCloud (US) Regions

商用 AWS GovCloud (US) Regionsのリソースには、次のポリシーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow-WorkSpaces-to-access-S3-buckets",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:sts::<account-id>:assumed-role/
workspaces_DefaultRole/WorkSpacesPoolSession"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
        }
    ]
}
```

# WorkSpaces Pools の VPC への接続

ネットワークリソースとインターネットへの WorkSpaces Pools 接続を有効にするには、WorkSpaces を次のように設定します。

## ネットワークインターフェイス

WorkSpaces Pools の各 WorkSpaces に次のネットワークインターフェイスがあります。

- カスタマーネットワークインターフェイスは、VPC 内だけでなくインターネットでのリソースへの接続を提供し、WorkSpaces 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は、セキュアな WorkSpaces Pools 管理ネットワークに接続します。ユーザーのデバイスへの WorkSpace のインタラクティブなストリーミングに使用され、WorkSpaces Pools が WorkSpace を管理するためにも使用されます。

WorkSpaces Pools は、管理ネットワークインターフェース用の IP アドレスをプライベート IP アドレス範囲 (198.19.0.0/16) から選択します。この範囲を VPC CIDR に使用することや、この範囲で VPC を他の VPC にピアリング接続することは避けてください。競合が生じて、WorkSpaces に接続できなくなることがあります。また、WorkSpace にアタッチされているネットワークインターフェイスは一切編集あるいは削除しないでください。これも、WorkSpace の未接続を引き起こす場合があります。

## 管理ネットワークインターフェイス IP アドレス範囲とポート

管理ネットワークインターフェイス IP アドレス範囲は、198.19.0.0/16 です。次のポートはすべての WorkSpaces 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。

- ポート 8300 のインバウンド TCP。これはストリーミング接続の確立に使用されます。
- ポート 3128 のアウトバウンド TCP。これは WorkSpaces の管理に使用されます。
- ポート 8000 と 8443 のインバウンド TCP。これらは WorkSpaces の管理に使用されます。
- ポート 8300 のインバウンド UDP。これは UDP でのストリーミング接続の確立に使用されます。

管理ネットワークインターフェイスでインバウンドの範囲 198.19.0.0/16 に制限します。

> **Note**
>
> Amazon DCV BYOL Windows WorkSpaces Pools では、10.0.0.0/8 IP アドレス範囲がすべての AWS リージョンで使用されます。これらの IP 範囲は、BYOL WorkSpaces Pools の管理トラフィック用に選択した /16 CIDR ブロックに追加されます。

通常の状況では、WorkSpaces Pools は WorkSpaces に対してこれらのポートを正常に設定します。これらのいずれかのポートをブロックするセキュリティソフトウェアまたはファイアウォールソフトウェアが WorkSpace にインストールされている場合、WorkSpaces は適切に機能することもあれば、アクセスできないこともあります。

IPv6 を無効にしないでください。IPv6 を無効にすると、WorkSpaces Pools は正しく機能しません。Windows 用の IPv6 の設定については、「上級ユーザー向けに Windows で IPv6 を構成するためのガイダンス」を参照してください。

> **Note**
>
> WorkSpaces Pools は VPC 内の DNS サーバーに依存して、存在しないローカルドメイン名に対して存在しないドメイン (NXDOMAIN) レスポンスを返します。これにより、WorkSpaces Pools で管理されるネットワークインターフェイスは管理サーバーとやり取りできます。
> Simple AD を使用してディレクトリを作成すると、 はユーザーに代わって DNS サーバーとしても機能する 2 つのドメインコントローラー AWS Directory Service を作成します。これらのドメインコントローラーは NXDOMAIN レスポンスを返さないため、WorkSpaces Pools で使用することはできません。

## カスタマーネットワークインターフェイスポート

- インターネット接続の場合、すべての接続先に対して次のポートが開いている必要があります。変更された、またはカスタムセキュリティグループを使用している場合、手動で必須ルールを追加する必要があります。詳細については、Amazon VPC ユーザーガイドの Security Group Rules を参照してください。
  - TCP 80 ( HTTP )
  - TCP 443 ( HTTPS )
  - UDP 4195

- ディレクトリに WorkSpaces を結合させる場合、WorkSpaces Pools VPC とディレクトリコントローラの間で次のポートが開かれている必要があります。
  - 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 1024-65535 - RPC 用ダイナミックポート

  ポートの完全なリストについては、Microsoft ドキュメンテーション の「Active Directory および Active Directory ドメインサービスのポート要件」を参照してください。
- すべての WorkSpace では、EC2 メタデータサービスへのアクセスができるようにポート 80 ( HTTP ) が IP アドレス `169.254.169.254` に開放されている必要があります。IP アドレス範囲 `169.254.0.0/16` は、WorkSpaces Pools サービスの管理トラフィックで使用するために予約されています。この範囲を除外しないと、ストリーミングの問題が発生する可能性があります。

## WorkSpaces Pools へのユーザー接続

ユーザーは、デフォルトのパブリックインターネットエンドポイントを介して WorkSpaces Pools の WorkSpaces に接続できます。

デフォルトで WorkSpaces Pools は、パブリックインターネットを介してストリーミング接続をルーティングするように設定されています。ユーザーを認証し、WorkSpaces Pools が機能するために必要なウェブアセットを配信するためには、インターネットに接続できることが必須です。このトラフィックを許可するには、「許可されたドメイン」に示されたドメインを許可する必要があります。

> **Note**
>
> ユーザー認証では、WorkSpaces Pools は Security Assertion Markup Language 2.0 (SAML 2.0) をサポートしています。詳細については、「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」を参照してください。

次のトピックでは、WorkSpaces Pools へのユーザー接続を有効にする方法について説明します。

内容



## 推奨帯域幅

WorkSpaces Pools のパフォーマンスを最適化するには、ネットワーク帯域幅とレイテンシーがユーザーのニーズに対応できるレベルであることが不可欠です。

WorkSpaces Pools では、さまざまなネットワーク条件でユーザーが安全にアプリケーションにアクセスしてストリーミングできるよう、NICE Desktop Cloud Visualization (DCV) を使用します。帯域幅の使用量を減らすために、NICE DCV では H.264 ベースのビデオ圧縮とエンコードが使用されます。ストリーミングセッション中、アプリケーションの視覚的な出力は圧縮され、HTTPS で AES-256 暗号化ピクセルストリームとしてユーザーにストリーミングされます。ストリームを受信すると、復号されてユーザーのローカル画面に出力されます。ユーザーが自分のストリーミングアプリケーションを操作するときは、NICE DCV プロトコルでユーザーの入力が取得され、HTTPS でユーザーのストリーミングアプリケーションに返送されます。

この処理の間、ネットワーク状況は常に測定され、WorkSpaces Pools に情報が送信されます。WorkSpaces Pools は、リアルタイムでビデオとオーディオのエンコードを変更することで変化するネットワーク状況に動的に対応し、さまざまなアプリケーションとネットワーク状況に合わせた高品質のストリームを生成します。

WorkSpaces Pools ストリーミングセッションで推奨される帯域幅とレイテンシーはワークロードによって異なります。たとえば、グラフィックを多用するアプリケーションを使用してコンピュータ支援設計タスクを実行するユーザーは、ビジネス生産性アプリケーションを使用してドキュメントを作成するユーザーよりも多くの帯域幅と短いレイテンシーを必要とします。

以下の表では、WorkSpaces Pools ストリーミングセッションで推奨されるネットワーク帯域幅およびレイテンシーのガイダンスを、一般的なワークロード別に示しています。

各ワークロードでの推奨帯域幅は、個々のユーザーが特定の時点で何が必要になる可能性があるかに基づいています。これらの推奨事項には、持続的なスループットに必要になる帯域幅は反映されていません。ストリーミングセッション中に画面上での変化がわずか数ピクセルである場合、持続的なスループットはさらに低くなります。使用可能な帯域幅が少ないユーザーでもアプリケーションをストリーミングできますが、最適なフレームレートや画質を得られない可能性があります。

| ワークロード | 説明 | ユーザーあたりの推奨帯域幅 | 推奨最大ラウンドトリップレイテンシー |
| --- | --- | --- | --- |
| 基幹業務アプリケーション | ドキュメント作成アプリケーション、データベース分析ユーティリティ | 2 Mbps | 150 ミリ秒未満 |
| グラフィックスアプリケーション | コンピュータ支援設計およびモデリングアプリケーション、写真およびビデオ編集 | 5 Mbps | 100 ミリ秒未満 |
| 高忠実度 | マルチモニター対応の忠実度の高いデータセットやマップ | 10 Mbps | 50 ミリ秒未満 |

## WorkSpaces Pools ユーザーデバイスの IP アドレスとポートの要件

インターネットエンドポイントを使用している場合、WorkSpaces Pools ユーザーのデバイスにはポート 443 (TCP) およびポート 4195 (UDP) でのアウトバウンドアクセスが必要となります。ドメイン名解決に DNS サーバーを使用している場合は、ポート 53 (UDP) でのアウトバウンドアクセスが必要です。

- ポート 443 は、インターネットエンドポイントを使用している場合の、WorkSpaces Pools ユーザーのデバイスと WorkSpaces との HTTPS 通信に使用されます。通常の場合、ストリーミングセッション中にエンドユーザーがウェブを閲覧すると、ウェブブラウザはストリーミングトラフィックに広範囲のソースポートをランダムに選択します。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。
- ポート 4195 は、インターネットエンドポイントを使用している場合の、WorkSpaces Pools ユーザーのデバイスと WorkSpaces との UDP HTTPS 通信に使用されます。現在、これは Windows ネイティブクライアントでのみサポートされます。VPC エンドポイントを使用している場合、UDP はサポートされません。

- ポート 53 は、WorkSpaces Pools ユーザーのデバイスと DNS サーバーとの通信に使用されます。パブリックドメイン名を解決できるように、このポートは DNS サーバーの IP アドレスに対して開い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、このポートはオプションです。

### 許可されたドメイン

WorkSpaces Pools ユーザーが WorkSpaces にアクセスできるようにするには、ユーザーによって WorkSpaces へのアクセスが開始されるネットワーク上のさまざまなドメインを、管理者が許可する必要があります。詳細については、「WorkSpaces Personal の IP アドレスとポートの要件」を参照してください。このページには、WorkSpaces Personal に適用される内容が示されていますが、WorkSpaces Pools にも適用されることに注意してください。

> **Note**
>
> S3 バケットの名前に「.」文字が含まれている場合、使用されるドメインは `https://s3.<aws-region>.amazonaws.com` です。S3 バケットの名前に「.」文字が含まれていない場合、使用されるドメインは `https://<bucket-name>.s3.<aws-region>.amazonaws.com` です。

## WorkSpaces プールを作成する

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

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

### プールを設定して作成する

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces]、[プール] の順に選択します。
3. [WorkSpaces プールの作成] を選択します。

4. [オンボーディング] (オプション) で、[お客様のユースケースに基づいた推奨事項]を選択すると、使用する WorkSpace のタイプに応じて推奨事項を取得できます。WorkSpaces Pools を使用することがわかっている場合は、この手順を省略できます。
5. [WorkSpaces の設定] で、次の情報を入力します。

   - [名前] に、プール用の一意の名前識別子を入力します。特殊文字は使用できません。
   - [説明] に、プールの説明を入力します (最大 256 文字)。
   - [バンドル] で、WorkSpaces に使用するバンドルのタイプを以下から選択します。
     - ベースの WorkSpaces バンドルを使用 - ドロップダウンからバンドルを 1 つ選択します。選択したバンドルタイプの詳細を確認するには、[バンドルの詳細] を選択します。プールに提供されるバンドルを比較するには、[すべてのバンドルを比較] を選択します。
     - 独自のカスタムバンドルを使用 - 過去に作成したバンドルを選択します。カスタムバンドルを作成するには、「WorkSpaces Personal のカスタム WorkSpaces イメージとバンドルを作成する」を参照してください。
   - 実行モードでは、以下から選択してプールの即時可用性と料金を設定します。
     - AutoStop — プールインスタンスには、ユーザーに接続されているインスタンスに対してのみ、選択したバンドルに基づいて時間単位の使用料が請求されます。ユーザーに接続されていないプール内のインスタンスには、停止したインスタンスの時間単位の料金が請求されます。ユーザーがセッションを開始すると、1～2 分間待機した後にストリーミングが開始されます。
     - AlwaysOn — 実行中のすべてのプールインスタンスには、ユーザーが接続されていない場合でも、該当する時間単位の使用料が請求されます。このモードは、ストリーミングの開始を待つ必要がないユーザーに最適です。
   - [Maximum session duration in minutes] (セッションの最大継続時間 (分単位)) には、ストリーミングセッションがアクティブな状態を維持できる最大時間を選択します。この制限に達する 5 分前にユーザーがまだストリーミングインスタンスに接続されている場合は、切断される前に、開いているドキュメントを保存するように求められます。この時間が経過すると、インスタンスが終了され、新しいインスタンスに置き換えられます。WorkSpaces Pools コンソールで設定できる最大セッション時間は 5,760 分 (96 時間) です。WorkSpaces Pools API と CLI を使用して設定できる最大セッション時間は 432,000 秒 (120 時間) です。
   - [Disconnect timeout in minutes (切断タイムアウト (分単位))] では、ユーザーが切断した後にストリーミングセッションをアクティブのままにする時間を選択します。切断、またはこの時間間隔内のネットワークの中断の後、ユーザーが再接続を試みる場合、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。

- ユーザーがプールツールバーで [セッションの終了] や [ログアウト] を選択してセッションを終了した場合、切断タイムアウトは適用されません。代わりに、開いているドキュメントを保存するかどうかの確認がユーザーに求められ、その後すぐにストリーミングインスタンスから切断されます。ユーザーが使用しているインスタンスは終了されます。
- [Idle disconnect timeout in minutes (アイドル切断タイムアウト (分単位))] では、ユーザーがストリーミングセッションから切断されるまでにアイドル状態 (非アクティブ) であることができる時間と、[Disconnect timeout in minutes (切断タイムアウト (分単位))] 期間の開始時刻を選択します。ユーザーは、アイドル状態が原因で切断される前に通知されます。ユーザーが [Disconnect timeout in minutes (切断タイムアウト (分単位))] で指定した期間が経過する前にストリーミングセッションへの再接続を試みると、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。この値を 0 に設定すると無効になります。この値を無効にした場合、ユーザーはアイドル状態が原因で切断されることはありません。

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

- [スケジュールされた容量のポリシー] (オプション) で、[新しいスケジュールされた容量を追加] を選択します。予想される同時ユーザーの最小数に基づいて、プールの最小数のインスタンスと最大数のインスタンスをプロビジョニングする日時を指定します。
- [手動スケーリングポリシー] (オプション) で、プールの容量を増減するために使用するプールのスケーリングポリシーを指定します。[手動スケーリングポリシー] を展開して、新しいスケーリングポリシーを追加します。

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

- [新しいスケールアウトポリシーを追加] を選択し、指定された容量使用率が指定されたしきい値を下回るか超えるかした場合に指定されたインスタンスを追加するための値を入力します。
- [新しいスケールインポリシーを追加] を選択し、指定された容量使用率が指定されたしきい値を下回るか超えるかした場合に指定されたインスタンスを削除するための値を入力します。

- [タグ] で、使用するキーペアの値を指定します。キーとしては、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。

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

# WorkSpaces Pools を管理する

WorkSpaces Pools は、指定したイメージを実行する WorkSpaces で構成されます。

内容



## WorkSpaces Pools の実行モード

WorkSpaces Pools の実行モードによって、即時の可用性と支払い方法が決まります。WorkSpaces Pools を作成するときに、次の実行モードから選択できます。

- AutoStop — WorkSpaces Pools のインスタンスには、ユーザーに接続されているインスタンスに対してのみ、選択したバンドルに基づいて時間単位の使用料が請求されます。ユーザーに接続され

ていない WorkSpaces Pools 内のインスタンスには、停止インスタンスの時間単位の低料金が請求されます。ユーザーがセッションを開始すると、1～2 分後にストリーミングが開始されます。

- AlwaysOn — WorkSpaces Pools のインスタンスを実行すると、ユーザーが接続されていない場合でも、適用される時間単位の使用料が請求されます。このモードは、ストリーミングの開始を待つ必要がないユーザーに最適です。

詳細については、WorkSpaces の料金を参照してください。

内容



### 実行モードを変更する

WorkSpaces Pools が停止状態のときに、実行モードを切り替えることができます。

WorkSpaces Pools の実行モードを変更するには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、WorkSpaces と Pools を選択します。
3. WorkSpaces Pools を選択して変更し、停止状態であることを確認します。次に、アクションと実行モードの変更を選択します。
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。

を使用して WorkSpaces Pools の実行モードを変更するには AWS CLI

- update-workspaces-pool コマンドを使用します。

## WorkSpaces Pools のバンドル

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、およびソフトウェアリソースの組み合わせです。WorkSpace を起動するときに、必要に応じてバンドルを選択します。WorkSpaces で使用できるデフォルトのバンドルはパブリックバンドルと呼ばれます。WorkSpaces で利用可能なさまざまな公開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。

次の表は、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ています。

| 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 |
| --- | --- | --- | --- |
| [Windows Server 2019] | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro |
| Windows Server 2022 | 含まれる | DCV | Standard、Performance、Power、PowerPro、Graphics.G4dn、GraphicsPro.G4dn |

> **Note**
>
> - ベンダーでサポートされ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 サポートでもサポートされません。

## プールの変更

WorkSpaces Pools の作成後、以下を変更できます。

- ディレクトリ ID (WorkSpaces Pools が停止している場合)
- 基本的な詳細
- バンドルとハードウェア
- セッションの切断設定
- 容量とスケーリング
- スケーリングアクティビティ
- [タグ]

WorkSpaces Pools を変更するには

1. ナビゲーションペインで [WorkSpaces]、[プール] の順に選択します。

2. 変更するプールを選択します。
3. 変更するセクションに移動し、[編集] を選択します。
4. 目的の変更を行い、[保存] を選択します。

## プールを削除する

プールを削除してリソースを解放し、アカウントに対して意図しない料金が発生することを回避できます。未使用で実行中のプールを停止することをお勧めします。

プールを削除するには

1. ナビゲーションペインで [WorkSpaces]、[プール] の順に選択します。
2. 停止するタスク実行を選択し、[停止] を選択します。プールを停止するには約 5 分かかります。
3. プールのステータスが [停止済み] になったら、[削除] を選択します。

## WorkSpaces Pools の自動スケーリング

自動スケーリングを使用してプールのサイズを自動的に変更し、利用可能なインスタンスをユーザーの需要に合わせて提供することができます。プールのサイズによって、同時にストリーミングできるユーザーの数が決まります。ユーザーセッションごとに 1 つのインスタンスが必要です。プールの容量は、インスタンスの観点から指定できます。プール設定と自動スケーリングポリシーに基づいて、必要な数のインスタンスが利用可能になります。さまざまな使用状況メトリクスに基づいてプールのサイズを自動的に調整するスケーリングポリシーを定義し、利用可能なインスタンスの数を最適化してユーザーの需要に合わせることができます。自動スケーリングを無効にして、固定されたサイズでプールを運用することもできます。

> **Note**
>
> - WorkSpaces Pools のスケーリングの計画を策定する際には、ネットワーク設定が要件を満たしていることを確認してください。
> - スケーリングを使用する場合は、Application Auto Scaling API を使用します。WorkSpaces Pools で自動スケーリングが正しく機能するためには、Application Auto Scaling に、プールを記述および更新して Amazon CloudWatch アラームを記述するアクセス許可と、管理者に代わってプールの容量を変更するアクセス許可が必要です。

以下のトピックでは、WorkSpaces Pools の自動スケーリングを理解して使用するうえで役立つ情報を示します。

内容



## スケーリングの概念

WorkSpaces Pools のスケーリングは、Application Auto Scaling によって行われます。詳細については、Application Auto Scaling API リファレンス を参照してください。

WorkSpaces Pools の自動スケーリングを効果的に使用するには、以下の用語と概念を理解しておく必要があります。

プールの最小容量/最小ユーザーセッション数

インスタンスの最小数。インスタンスの数がこの値を下回ることはできません。また、スケーリングポリシーによってプールがこの値より小さくスケールされることはありません。例えば、プールの最小容量を 2 に設定した場合、プールのインスタンス数が 2 を下回ることはありません。

プールの最大容量/最大ユーザーセッション数

インスタンスの最大数。インスタンスの数がこの値を上回ることはできません。また、スケーリングポリシーによってプールがこの値より大きくスケールされることはありません。例えば、プールの最大容量を 10 に設定した場合、プールのインスタンス数が 10 を上回ることはありません。

希望するユーザーセッション容量

実行中または保留中のセッションの合計数。これはプールが安定した状態でサポートできる同時ストリーミングセッションの合計数を表します。

スケーリングポリシーアクション

[スケーリングポリシー条件] が満たされた場合に、ケーリングポリシーによってプールで実行されるアクションです。[% capacity] または [number of instance(s)] に基づいてアクションを選択で

きます。例えば、[希望するユーザーセッション容量] が 4 に、[スケーリングポリシーアクション] が「容量を 25% 追加」に設定されている場合、[スケーリングポリシー条件] が満たされると [希望するユーザーセッション容量] が 25% 増加して 5 になります。

スケーリングポリシー条件

[Scaling Policy Action] で設定されたアクションをトリガーする条件。この条件は、スケーリングポリシーのメトリクス、比較演算子、しきい値を含みます。例えば、プールの使用率が 50% を超えたときにプールをスケールする場合は、スケーリングポリシー条件を「容量使用率 > 50% になった場合」にする必要があります。

スケーリングポリシーメトリクス

お客様のスケーリングポリシーはこのメトリクスに基づいています。スケーリングポリシーには、次のメトリクスを使用できます。

容量使用率

プールで使用されているインスタンスの割合。このメトリクスを使用すると、プールの使用率に基づいてプールをスケールできます。たとえば、[Scaling Policy Condition]: 「容量使用率 < 25%」の場合、[Scaling Policy Action]: 「25% の容量を削除」を実行します。

使用可能な容量

ユーザーに提供可能なプールのインスタンスの数。このメトリクスを使用して、ユーザーがストリーミングセッションを開始するための、使用可能なメモリ容量のバッファを維持できます。たとえば、[Scaling Policy Condition]: 「使用可能な容量 < 5」 の場合、[Scaling Policy Action]: 「5 インスタンスを追加」を実行します。

容量不足エラー

容量不足により拒否されたセッションリクエストの数。このメトリクスを使用して、容量不足のためにストリーミングセッションを開始できないユーザーの新しいインスタンスをプロビジョニングできます。たとえば、[Scaling Policy Condition]: 「容量不足エラー > 0」の場合、[Scaling Policy Action]: 「1 インスタンスを追加」を実行します。

## コンソールを使用したプールスケーリングの管理

WorkSpaces コンソールを使用してスケーリングを設定および管理できます。この操作は、プールの作成中、または随時 [プール] タブを使用して行うことができます。プールを作成したら、[スケーリングポリシー] タブに移動して、プールに新しいスケーリングポリシーを追加します。詳細については、「WorkSpaces プールを作成する」を参照してください。

ユーザーの環境はさまざまに異なるため、需要に応じてスケーリングを制御するようにスケーリングポリシーを定義します。一定数のユーザーが予想される場合やスケーリングを無効にする他の理由がある場合には、ユーザーセッションのインスタンス数を固定してプールを設定できます。

これを行うには、最小容量を希望するインスタンス数に設定し、最大容量を少なくとも最小容量の値になるように調整します。これにより検証エラーを回避できますが、プールはスケールされないため、最大容量は最終的に無視されます。次に、対象プールのすべてのスケーリングポリシーを削除します。

コンソールを使用してプールのスケーリングポリシーを設定するには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、[プール] を選択します。
3. プールを選択します。
4. 選択したプールのページで、容量とスケーリングのセクションまで下にスクロールします。
5. [編集] を選択します。
6. 既存のポリシーを編集し、フィールドで希望する値を設定して、[保存] を選択します。ポリシーの変更は数分以内で有効になります。
7. また、[新しいスケジュールされた容量を追加]、[新しいスケールアウトポリシーを追加]、または [新しいスケールインポリシーを追加] を選択して、新しい容量とスケーリングポリシーを追加することもできます。

次の例は、5 人のユーザーがプールに接続して切断する場合のスケーリングアクティビティの使用状況グラフです。　この例では、プールに次のスケーリングポリシーが使用されています。

- 最小容量 = 10
- 最大容量 = 50
- スケールアウト = プールの容量使用率が 75% を超えた場合、インスタンスを 5 つ追加
- スケールイン = プールの容量使用率が 25% 未満になった場合、インスタンスを 6 つの削除

> **Note**
>
> セッション中、スケールアウトイベントの発生時には 5 つの新しいインスタンスが起動します。スケールインイベントの発生時には、アクティブなユーザーセッションがないインスタンスが十分あり、インスタンスの合計数が最小容量である 10 インスタンスを下回ら

ない場合、6 つのインスタンスが再利用されます。ユーザーセッションが実行中であるインスタンスは再利用されません。実行中のユーザーセッションがないインスタンスのみが再利用されます。

## CLI AWS を使用したプールスケーリングの管理

AWS Command Line Interface（ AWS CLI) を使用してプールスケーリングを設定および管理できます。スケールインおよびスケールアウトのクールダウン時間の設定など、より高度な機能については、 CLI AWS を使用します。スケーリングポリシーコマンドを実行する前に、プールをスケーラブルなターゲットとして登録する必要があります。これを行うには、以下の register-scalable-target コマンドを使用します。

```
aws application-autoscaling register-scalable-target
  --service-namespace workspaces \
  --resource-id workspacespool/PoolId \
  --scalable-dimension workspaces:workspacespool:DesiredUserSessions \
  --min-capacity 1 --max-capacity 5
```

例

- 例 1: 容量使用率に基づくスケーリングポリシーの適用
- 例 2: 容量不足エラーに基づくスケーリングポリシーの適用
- 例 3: 低容量使用率に基づくスケーリングポリシーの適用
- 例 4: スケジュールに基づくプールの容量の変更
- 例 5: ターゲット追跡スケーリングポリシーの適用

### 例 1: 容量使用率に基づくスケーリングポリシーの適用

この AWS CLI の例では、使用率 >= 75% の場合にプールを 25% スケールアウトするスケーリングポリシーを設定します。

次の put-scaling-policy コマンドは使用率ベースのスケーリングポリシーを定義します。

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
utilization.json
```

scale-out-utilization.json ファイルの内容は以下のようになります。

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 25
            }
        ],
        "Cooldown": 120
    }
}
```

コマンドが成功した場合、一部の詳細はアカウントおよびリージョンで固有ですが、出力は次のようになります。この例では、ポリシー識別子は e3425d21-16f0-d701-89fb-12f98dac64af です。

```
{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:e3425d21-16f0-
d701-89fb-12f98dac64af:resource/workspaces/workspacespool/PoolId:policyName/scale-out-
utilization-policy"}
```

ここで、このポリシーの CloudWatch アラームを設定します。該当する名前、リージョン、アカウント番号、およびポリシー識別子を使用します。前のコマンドで返されたポリシー ARN を --alarm-actions パラメータに使用できます。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Available User Session Capacity exceeds 75 percent" \
--metric-name AvailableUserSessionCapacity \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 300 \
--threshold 75 \
--comparison-operator GreaterThanOrEqualToThreshold \
--dimensions "Name=WorkSpaces pool ID,Value=PoolId" \
--evaluation-periods 1 --unit Percent \
```

```
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

例 2: 容量不足エラーに基づくスケーリングポリシーの適用

この AWS CLI の例では、プールからInsufficientCapacityErrorエラーが返された場合にプールを 1 だけスケールアウトするスケーリングポリシーを設定します。

次のコマンドは、容量不足に基づくスケーリングポリシーを定義します。

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
capacity.json
```

scale-out-capacity.json ファイルの内容は以下のようになります。

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "ChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 1
            }
        ],
        "Cooldown": 120
    }
}
```

コマンドが成功した場合、一部の詳細はアカウントおよびリージョンで固有ですが、出力は次のようになります。この例では、ポリシー識別子は f4495f21-0650-470c-88e6-0f393adb64fc です。

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:f4495f21-0650-470c-88e6-0f393adb64fc:resource/
workspaces/workspacespool/PoolId:policyName/scale-out-insufficient-capacity-policy"}
```

ここで、このポリシーの CloudWatch アラームを設定します。該当する名前、リージョン、アカウント番号、およびポリシー識別子を使用します。前のコマンドで返されたポリシー ARN を `--alarm-actions` パラメータに使用できます。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when out of capacity is > 0" \
--metric-name InsufficientCapacityError \
--namespace AWS/WorkSpaces \
--statistic Maximum \
--period 300 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 1 --unit Count \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

例 3: 低容量使用率に基づくスケーリングポリシーの適用

AWS CLI この例では、 UserSessionsCapacityUtilizationが低い場合に実際の容量を減らすためにプールをスケールインするスケーリングポリシーを設定します。

以下のコマンドは、容量超過に基づくスケーリングポリシーを定義します。

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-in-
capacity.json
```

`scale-in-capacity.json` ファイルの内容は以下のようになります。

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
```

```
                "MetricIntervalUpperBound": 0,
                "ScalingAdjustment": -25
            }
        ],
        "Cooldown": 360
    }
}
```

コマンドが成功した場合、一部の詳細はアカウントおよびリージョンで固有ですが、出力は次のようになります。この例では、ポリシー識別子は 12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90 です。

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90:resource/
workspaces/workspacespool/PoolId:policyName/scale-in-utilization-policy"}
```

ここで、このポリシーの CloudWatch アラームを設定します。該当する名前、リージョン、アカウント番号、およびポリシー識別子を使用します。前のコマンドで返されたポリシー ARN を --alarm-actions パラメータに使用できます。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Capacity Utilization is less than or equal to 25
 percent" \
--metric-name UserSessionsCapacityUtilization \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 120 \
--threshold 25 \
--comparison-operator LessThanOrEqualToThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 10 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

例 4: スケジュールに基づくプールの容量の変更

スケジュールに基づいてプールの容量を変更すると、予測可能な需要の変動に応じてプールの容量をスケールすることができます。たとえば、稼働日の最初に、特定の数のユーザーが同時にストリーミング接続をリクエストすることが予期されます。スケジュールに基づいてプール容量を変更するに

は、Application Auto Scaling PutScheduledAction API アクションまたは put-scheduled-action AWS CLI コマンドを使用できます。

プール容量を変更する前に、WorkSpaces describe-workspaces-pools AWS CLI コマンドを使用して、現在のプール容量を一覧表示できます。

```
aws workspaces describe-workspaces-pools --name PoolId
```

現在のプールの容量は、次の出力のように表示されます (JSON 形式で表示)。

```
{
    "CapacityStatus": {
        "AvailableUserSessions": 1,
        "DesiredUserSessions": 1,
        "ActualUserSessions": 1,
        "ActiveUserSessions": 0
    },
}
```

次に、put-scheduled-action コマンドを使用してプールの容量を変更するスケジュールされたアクションを作成します。たとえば、次のコマンドでは、毎日午前 9:00 時 (UTC) に最小容量を 3 に変更し、最大容量を 5 に変更します。

> **Note**
>
> cron 式の場合は、アクションを実行するタイミングを UTC で指定します。詳細については、「Cron 式」を参照してください。

```
aws application-autoscaling put-scheduled-action --service-namespace workspaces \
--resource-id workspacespool/PoolId \
--schedule="cron(0 9 * * ? *)" \
--scalable-target-action MinCapacity=3,MaxCapacity=5 \
--scheduled-action-name ExampleScheduledAction \
--scalable-dimension workspaces:workspacespool:DesiredUserSessions
```

プールの容量を変更するスケジュールされたアクションが正しく作成されたことを確認するには、describe-scheduled-actions コマンドを実行します。

```
aws application-autoscaling describe-scheduled-actions --service-namespace workspaces
 --resource-id workspacespool/PoolId
```

スケジュールされたアクションが正常に作成された場合、出力は次のようになります。

```
{
    "ScheduledActions": [
        {
            "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
            "Schedule": "cron(0 9 * * ? *)",
            "ResourceId": "workspacespool/ExamplePool",
            "CreationTime": 1518651232.886,
            "ScheduledActionARN": "<arn>",
            "ScalableTargetAction": {
                "MinCapacity": 3,
                "MaxCapacity": 5
            },
            "ScheduledActionName": "ExampleScheduledAction",
            "ServiceNamespace": "workspaces"
        }
    ]
}
```

詳細については、「Application Auto Scaling ユーザーガイド」の「スケジュールされたスケーリング」を参照してください。

例 5: ターゲット追跡スケーリングポリシーの適用

ターゲット追跡スケーリングでは、プールの容量使用率レベルを指定できます。

ターゲット追跡スケーリングポリシーを作成すると、Application Auto Scaling は、スケーリングポリシーをトリガーする CloudWatch アラームを自動的に作成および管理します。スケーリングポリシーは、指定されたターゲット値、またはそれに近い値に容量使用率を維持するため、必要に応じて容量を追加または削除します。アプリケーションの可用性を高めるために、プールのスケールアウトはメトリクスに比例して可能な限り迅速に行われますが、スケールインはより緩やかに行われます。

次の put-scaling-policy コマンドは、WorkSpaces のプールに 75% の容量使用率を維持するターゲット追跡スケーリングポリシーを定義します。

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://config.json
```

config.json ファイルの内容は以下のようになります。

```
{
  "PolicyName":"target-tracking-scaling-policy",
  "ServiceNamespace":"workspaces",
  "ResourceId":"workspacespool/PoolId",
  "ScalableDimension":"workspaces:workspacespool:DesiredUserSessions",
  "PolicyType":"TargetTrackingScaling",
  "TargetTrackingScalingPolicyConfiguration":{
    "TargetValue":75.0,
    "PredefinedMetricSpecification":{
      "PredefinedMetricType":"WorkSpacesAverageUserSessionsCapacityUtilization"
    },
    "ScaleOutCooldown":300,
    "ScaleInCooldown":300
  }
}
```

コマンドが成功した場合、一部の詳細はアカウントおよびリージョンで固有ですが、出力は次のようになります。この例では、ポリシー識別子は 6d8972f3-efc8-437c-92d1-6270f29a66e7 です。

```
{
    "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/workspaces/workspacespool/PoolId:policyName/
target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d"
        }
    ]
}
```

詳細については、Application Auto Scaling ユーザーガイドの「ターゲット追跡スケーリングポリシー」を参照してください。

### 追加リソース

Application Auto Scaling AWS CLI コマンドまたは API アクションの使用の詳細については、次のリソースを参照してください。

- AWS CLI コマンドリファレンスの application-autoscaling セクション
- Application Auto Scaling API リファレンスhttps://docs.aws.amazon.com/autoscaling/application/APIReference/
- アプリケーション Auto Scaling ユーザーガイドhttps://docs.aws.amazon.com/autoscaling/application/userguide/

## WorkSpaces Pools での Active Directory の使用

WorkSpaces Pools の Windows WorkSpaces を Microsoft Active Directory のドメインに参加させることで、既存の Active Directory ドメイン (クラウドベースまたはオンプレミス) を使用して、ドメイン参加済みのストリーミングインスタンスを起動することができます。 AWS Directory Service for Microsoft Active Directoryとも呼ばれる を使用して Active Directory ドメインを作成し AWS Managed Microsoft AD、それを使用して WorkSpaces Pools リソースをサポートすることもできます。の使用の詳細については AWS Managed Microsoft AD、「 AWS Directory Service 管理ガイド」の「Microsoft Active Directory」を参照してください。

WorkSpaces Pools を Active Directory ドメインに参加させると、以下のことを行うことができます。

- ストリーミングセッションからプリンターやファイル共有などのアクティブディレクトリリソースにアクセスすることをユーザーとアプリケーションに許可する。
- グループポリシーマネジメントコンソール (GPMC) で使用できるグループポリシー設定を使用して、エンドユーザーエクスペリエンスを定義する。
- アクティブディレクトリログイン認証情報を使用した認証をユーザーに義務付けるアプリケーションをストリーミングする。
- WorkSpaces Pools の WorkSpaces に企業コンプライアンスとセキュリティポリシーを適用する。

内容

# アクティブディレクトリドメインの概要

WorkSpaces Pools で Active Directory ドメインを使用するには、それらが連携して動作する仕組みと、必要な設定タスクを理解する必要があります。次のタスクを実行する必要があります。

1. 必要に応じて、アプリケーションのエンドユーザーエクスペリエンスとセキュリティ要件を定義できるように、グループポリシーを設定します。
2. WorkSpaces Pools にドメイン参加済みディレクトリを作成します。
3. SAML 2.0 ID プロバイダーで WorkSpaces Pools アプリケーションを作成し、直接または Active Directory グループを使用してエンドユーザーに割り当てます。

## ユーザー認証フロー

1. ユーザーが `https://applications.exampleco.com` を参照します。サインインページがユーザーの認証をリクエストします。
2. フェデレーションサービスが組織の ID ストアからの認証をリクエストします。
3. ID ストアはユーザーを認証し、フェデレーションサービスに認証レスポンスを返します。
4. 認証が成功すると、フェデレーションサービスはユーザーのブラウザに SAML アサーションを送信します。
5. ユーザーのブラウザは、SAML アサーションを AWS サインイン SAML エンドポイント (`https://signin.aws.amazon.com/saml`) に投稿します。 AWS サインインは SAML リクエストを受け取り、リクエストを処理し、ユーザーを認証し、認証トークンを WorkSpaces Pools サービスに転送します。
6. WorkSpaces Pools は AWS、 からの認証トークンを使用してユーザーを認可し、ブラウザにアプリケーションを表示します。
7. ユーザーはアプリケーションを選択し、WorkSpaces Pools ディレクトリで有効になっている Windows ログイン認証方法に応じて、Active Directory ドメインパスワードを入力するか、スマー

トカードを選択するよう求められます。両方の認証方法が有効になっている場合、ユーザーはドメインパスワードを入力するか、スマートカードを使用するかを選択できます。証明書ベースの認証は、プロンプトを省略してユーザーの認証にも使用できます。

8. ドメインコントローラーに接続してユーザーを認証します。
9. ドメインで認証された後、ユーザーのセッションがドメインに接続できる状態で開始されます。

ユーザーの視点から見ると、このプロセスは透過的です。ユーザーはまず組織の内部ポータルに移動し、 AWS 認証情報を入力することなく WorkSpaces Pools ポータルにリダイレクトされます。アクティブディレクトリドメインのパスワードまたはスマートカードの認証情報のみが必要です。

ユーザーがこのプロセスを開始する前に、必要な資格およびグループポリシーを使用して Active Directory を設定し、ドメイン参加済みの WorkSpaces Pools ディレクトリを作成しておく必要があります。

## WorkSpaces Pools で Active Directory の使用を開始する前に

WorkSpaces Pools で Microsoft Active Directory ドメインを使用する前に、次の要件と考慮事項に注意してください。

内容



### アクティブディレクトリドメイン環境

- WorkSpaces を参加させる Microsoft Active Directory ドメインが必要です。Active Directory ドメインがない場合、またはオンプレミスの Active Directory 環境を使用する場合は、AWS 「 クラウド上の Active Directory ドメインサービス: クイックスタートリファレンスデプロイ」を参照してください。
- WorkSpaces Pools で使用するドメインでコンピュータオブジェクトを作成および管理するためのアクセス許可が付与された、ドメインサービスアカウントが必要です。詳細については、Microsoft ドキュメントで How to Create a Domain Account in Active Directory を参照してください。

この Active Directory ドメインを WorkSpaces Pools と関連付けるには、サービスアカウント名とパスワードを入力します。WorkSpaces Pools はこのアカウントを使用して、ディレクトリ内にコンピュータオブジェクトを作成して管理します。詳細については、「アクティブディレクトリコンピュータオブジェクトを作成および管理するための許可の付与」を参照してください。

- WorkSpaces Pools で Active Directory ドメインを登録する場合は、組織単位 (OU) の識別名が必要です。この目的のために OU を作成します。デフォルトのコンピュータコンテナは OU ではなく、WorkSpaces Pools で使用することはできません。詳細については、「組織単位の識別子名を検索する」を参照してください。
- WorkSpaces Pools で使用予定のディレクトリは、完全修飾ドメイン名 (FQDN) を使用して、WorkSpaces を起動する仮想プライベートクラウド (VPC) 経由でアクセスできることが必要です。詳細については、Microsoft ドキュメントの Active Directory and Active Directory Domain Services Port Requirements を参照してください。

## WorkSpaces Pools のドメイン参加済み WorkSpaces

ドメインに参加している WorkSpaces からアプリケーションストリーミングを行うには SAML 2.0 ベースのユーザーフェデレーションが必要です。また、Active Directory ドメインへの参加をサポートする Windows イメージを使用する必要があります。2017 年 7 月 24 日以降に公開されたすべてのパブリックイメージはアクティブディレクトリドメインへの参加をサポートします。

## グループポリシー設定

次のグループポリシー設定の内容を確認します。WorkSpaces Pools でのドメインユーザーの認証とログインがブロックされないように、必要に応じて、次のセクションで説明するように設定を更新します。更新しないと、ユーザーが WorkSpaces にログインしようとしたときに失敗する場合があります。「不明なエラーが発生しました」というエラーメッセージが表示される場合があります。

- [Computer Configuration] (コンピュータの構成) > [Administrative Templates] (管理用テンプレート) > [Windows Components] (Windows コンポーネント) > [Windows Logon Options] (Windows ログオンオプション) > [Disable or Enable software Secure Attention Sequence] (ソフトウェアの Secure Attention Sequence を無効または有効にする) から、[Services] (サービス) に対して [Enabled] (有効) に設定します。
- [Computer Configuration (コンピュータの構成)] > [Administrative Templates (管理用テンプレート)] > [System (システム)] > [Logon (ログオン)] > [Exclude credential providers (認証情報プロバイダーを除外する)] から、次の CLSID が一覧にないことを確認します。`e7c1bab5-4b49-4e64-a966-8d99686f8c7c`

- [Computer Configuration (コンピュータの構成)] > [Policies (ポリシー)] > [Windows Settings (Windows 設定)] > [Security Settings (セキュリティ設定)] > [Local Policies (ローカルポリシー)] > [Security Options (セキュリティオプション)] > [Interactive Logon (対話型ログオン)] > [Interactive Logon (対話型ログオン)]: ログオンしようとしているユーザーへのメッセージテキストから、この値を [Not defined (未定義)] に設定します。
- [Computer Configuration (コンピュータの構成)] > [Policies (ポリシー)] > [Windows Settings (Windows 設定)] > [Security Settings (セキュリティ設定)] > [Local Policies (ローカルポリシー)] > [Security Options (セキュリティオプション)] > [Interactive Logon (対話型ログオン)] > [Interactive Logon (対話型ログオン)]: ログオンしようとしているユーザーへのメッセージタイトルから、この値を [Not defined (未定義)] に設定します。

### スマートカード認証

WorkSpaces Pools の WorkSpaces への Windows サインインでは、Active Directory ドメインのパスワード、または Common Access Card (CAC) や Personal Identity Verification (PIV) などのスマートカードを使用できます。サードパーティーの証明機関 (CA) を使用してスマートカードサインインを有効にするようにアクティブディレクトリ環境を構成する詳細方法については、Microsoft ドキュメントの Guidelines for enabling smart card logon with third-party certification authorities を参照してください。

## 証明書ベースの認証

Microsoft Active Directory に参加している WorkSpaces Pools では、証明書ベースの認証を使用できます。これにより、ユーザーがログインするときに Active Directory ドメインパスワードの入力を求めるユーザープロンプトが省略されます。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、 で AWS Private Certificate Authority （ AWS Private CA) リソースを使用します AWS アカウント。を使用すると AWS Private CA、ルート CA と下位 CAs を含むプライベート認証機関 (CA) 階層を作成できます。独自の CA 階層を作成し、そこから内部ユーザーを認証する

証明書を発行することもできます。詳細については、「 とは AWS Private CA」を参照してください。

証明書ベースの認証に AWS Private CA を使用すると、WorkSpaces Pools は WorkSpaces Pools 内の各 WorkSpace のセッション予約時に自動的にユーザーの証明書をWorkSpaces。証明書で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、ユーザーを Active Directory に対して認証します。

証明書ベースの認証は、Windows インスタンスを実行するドメイン参加済みの WorkSpaces Pools でサポートされています。

内容



## 前提条件

証明書ベースの認証を使用する前に、以下のステップを完了します。

1. SAML 2.0 統合を使用して、証明書ベースの認証を使用するように WorkSpaces Pools ディレクトリを設定します。詳細については、「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」を参照してください。

   > **Note**
   >
   > 証明書ベースの認証を使用する場合は、プールディレクトリ内で [スマートカードサインイン] を有効にしないでください。

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、「ステップ 7: 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。この属性を使用して、Active Directory ユーザーとの強力なマッピングを実行できます。`ObjectSid` 属性が SAML_Subject `NameID` で指定されたユーザーの 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、「ステップ 7: 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。

> **Note**
>
> Microsoft KB5014754 によると、 `ObjectSid` 属性は 2025 年 9 月 10 日以降、証明書ベースの認証に必須になります。

4. SAML 2.0 設定で使用する IAM ロールの信頼ポリシーに `sts:TagSession` アクセス権限を追加します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS STS でのタグ付けの規則」を参照してください。この権限は、証明書ベースの認証を使用する場合に必要です。詳細については、「ステップ 5: 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 で設定されていない場合は、 AWS プライベート CA を使用してプライベート認証機関 (CA) を作成します。証明書ベースの認証を使用するには、 AWS プライベート CA が必要です。詳細については、「AWS Private Certificate Authority ユーザーガイド」で AWS Private CA のデプロイ計画に関するセクションを参照してください。証明書ベースの認証の多くのユースケースでは、以下の AWS プライベート CA 設定が一般的です。
   - CA タイプオプション
     - 使用期間が短い証明書 CA 使用モード – CA が証明書ベースの認証のためにエンドユーザー証明書のみを発行する場合に推奨されます。
     - ルート CA を含む単一レベルの階層 – 下位 CA を選択して既存の CA 階層と統合します。
   - 主要なアルゴリズムオプション – RSA 2048
   - サブジェクト識別名オプション – 最も適切なオプションを使用して、Active Directory の信頼されたルート証明機関ストアでこの CA を識別します。
   - 証明書失効オプション – CRL のディストリビューション

   > **Note**
   >
   > 証明書ベースの認証には、WorkSpaces Pools の WorkSpaces とドメインコントローラーの両方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、 AWS 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、またはパブリックアクセスをブロックする場合は Amazon S3 バケットにアクセスできる CloudFront 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、「AWS Private Certificate Authority ユーザーガイド」で証明書失効リスト (CRL) の計画に関するセクションを参照してください。

6. プライベート CA に `euc-private-ca` という名前のキーでタグ付けし、WorkSpaces Pools の証明書ベースの認証で使用する CA を指定します。このキーには値は必要ありません。詳細については、「AWS Private Certificate Authority ユーザーガイド」のプライベート CA のタグ管理に関するセクションを参照してください。
7. 証明書ベースの認証では、仮想スマートカードを使用してログオンします。詳細については、「サードパーティーの証明機関でスマートカードオンを有効にするためのガイドライン」を参照してください。以下の手順に従ってください。
   a. スマートカードユーザーを認証するには、ドメインコントローラー証明書を使用して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、スマートカードによるログオンを可能にするドメインコントローラーが証明書に自動的に登録されます。Active Directory 証明書サービスがない場合は、「サードパーティー 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。 AWS プライベート CA を使用してドメインコントローラー証明書を作成できます。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**
      >
      > AWS Managed Microsoft AD を使用する場合は、ドメインコントローラー証明書の要件を満たす Amazon EC2 インスタンスで証明書サービスを設定できます。Active Directory 証明書サービスで設定された Managed Microsoft AD のデプロイ例については、「新しい Amazon Virtual Private Cloud に Active Directory をデプロイする」を参照してください。 AWS
      > AWS Managed Microsoft AD と Active Directory Certificate Services では、コントローラーの VPC セキュリティグループから Certificate Services を実行する Amazon EC2 インスタンスへのアウトバウンドルールも作成する必要があります。証明書の自動登録を有効にするには、セキュリティグループに TCP ポート 135 とポート 49152 ~ 65535 へのアクセスを提供する必要があります。Amazon EC2 インスタンスは、ドメインコントローラーを含むドメインインスタンスからの同じポートへのインバウンドアクセスも許可する必要があります。 AWS Managed Microsoft AD のセキュリティグループを見つける方法の詳細については、「VPC サブネットとセキュリティグループを設定する」を参照してください。

   b. AWS プライベート CA コンソール、または SDK または CLI で、プライベート CA 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。

c. プライベート CA を Active Directory に公開します。ドメインコントローラーまたはドメイン結合マシンにログオンします。プライベート CA 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、グループポリシーと Microsoft PKI Health ツール (PKIView) 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てから、プライベート CA 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 WorkSpaces Pools の WorkSpaces に公開されるまでに数分かかる場合があります。

> **Note**
>
> WorkSpaces Pools の WorkSpaces がドメインに参加したときに、Active Directory が、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。

> **Note**
>
> 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 Support 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を構成する」を参照してください。

## 証明書ベースの認証

証明書ベースの認証を使用する前に、以下の手順を完了します。

証明書ベースの認証

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com」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. [Pools ディレクトリ] タブを選択します。
4. 設定するディレクトリを選択します。
5. ページの [認証] セクションで [編集] を選択します。
6. ページの [証明書ベースの認証] セクションで [証明書ベースの認証の編集] を選択します。
7. [証明書ベースの認証を有効にする] を選択します。
8. [AWS Certificate Manager (ACM) Private Certificate Authority (CA)] ドロップダウンで証明書を選択します。

   ドロップダウンに表示するには、プライベート CA を同じ AWS アカウント と AWS リージョンに保存する必要があります。また、プライベート CA には `euc-private-ca` という名前のキーをタグ付けする必要があります。
9. フォールバックのディレクトリログを設定します。フォールバックを使用すると、証明書ベースの認証に失敗した場合でも、ユーザーは AD ドメインのパスワードでログインできます。これは、ユーザーがドメインパスワードを知っている場合にのみ推奨されます。フォールバックがオフになっていると、ロック画面や Windows のログオフが発生した場合に、セッションによってユーザーの接続が切断される可能性があります。フォールバックがオンになっている場合、セッションはユーザーに AD ドメインパスワードの入力を求めます。
10. [保存] を選択します。

これで証明書ベースの認証が有効になりました。ユーザーがドメインに参加している WorkSpaces を使用して SAML 2.0 で WorkSpaces Pools ディレクトリを認証する際、ドメインパスワードのプロンプトは表示されません。証明書ベースの認証が有効になっているセッションに接続すると、「証明書ベースの認証で接続します」という内容のメッセージが表示されます。

## 証明書ベースの認証の管理

証明書ベースの認証を有効にしたら、次のタスクを確認します。

プライベート CA 証明書

一般的な設定では、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プライベート CA を置き換える方法、またはプライベート CA を新しい有効期間で再発行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

WorkSpaces Pools の証明書ベースの認証 AWS Private Certificate Authority 用に によって発行されたエンドユーザー証明書は、更新や取り消しを必要としません。これらは使用期間が短い証明書です。WorkSpaces Pools は、新しいセッションごとに、または期間の長いセッションの場合は 24 時間ごとに新しい証明書を自動的に発行します。こうしたエンドユーザー証明書の使用は、WorkSpaces Pools セッションで管理されます。セッションが終わると、WorkSpaces Pools はその証明書の使用を停止します。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 Certificate Authority 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

CloudTrail を使用して、WorkSpaces Pools によるプライベート CA への API コールを記録できます。詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrailとは」および「AWS Private Certificate Authority ユーザーガイド」の CloudTrail の使用に関するセクションを参照してください。CloudTrail イベント履歴では、WorkSpaces Pools EcmAssumeRoleSession ユーザー名で作成された acm-pca.amazonaws.com イベントソースの GetCertificate および IssueCertificate のイベント名を表示できます。これらのイベントは、WorkSpaces Pools の証明書ベースの認証リクエストごとに記録されます。詳細については、「AWS CloudTrail ユーザーガイド 」の「CloudTrail イベント履歴でのイベントの表示」を参照してください。

## PCA のクロスアカウント共有を有効にする

プライベート CA (PCA) のクロスアカウント共有を使用すると、他のアカウントに一元的な CA を使用するアクセス許可を付与できます。CA は、AWS Resource Access Manager (RAM) を使用して証明書を生成および発行し、アクセス許可を管理できます。これにより、アカウントごとのプライベート CA は不要になります。プライベート CA のクロスアカウント共有は、同じ AWS リージョン内で生じる AppStream 2.0 の証明書ベースの認証 (CBA) で使用できます。

WorkSpaces Pools の CBA でプライベート CA の共有リソースを使用するには、次の手順を実行します。

1. CBA のプライベート CA を一元化された で設定します AWS アカウント。詳細については、「the section called “証明書ベースの認証”」を参照してください。
2. プライベート CA を WorkSpaces Pools リソース AWS アカウント が CBA を利用するリソースと共有します。これを行うには、「How to use AWS RAM to share your ACM Private CA cross-account」の手順に従います。ステップ 3 の証明書を作成する手順は実行する必要はありません。プライベート 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場合は、 AWS Resource Access Manager 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、 AWS Resource Access Manager リソースアカウントのプライベート CA のリソース共有が `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 Pools サービスロールが使用する PCA テンプレートと一致しています。
3. 共有が成功したら、リソースアカウントのプライベート CA コンソールを使用して、共有プライベート CA を表示します。
4. API または CLI を使用して、プライベート CA の ARN を WorkSpaces Pools ディレクトリの CBA に関連付けます。現時点では、WorkSpaces Pools コンソールは、共有プライベート CA の ARN の選択をサポートしていません。詳細については、「Amazon WorkSpaces サービス API リファレンス」を参照してください。

## WorkSpaces Pools の Active Directory 管理

WorkSpaces Pools で Active Directory をセットアップして使用するには、次の管理タスクを行う必要があります。

タスク

- アクティブディレクトリコンピュータオブジェクトを作成および管理するための許可の付与
- 組織単位の識別子名を検索する
- カスタムイメージのローカル管理者権限を付与する
- ユーザーがアイドル状態の場合にストリーミングセッションをロックする

- ドメイン信頼関係を使用するように WorkSpaces Pools を設定する

## アクティブディレクトリコンピュータオブジェクトを作成および管理するための許可の付与

WorkSpaces Pools に Active Directory コンピュータオブジェクト操作の実行を許可するには、十分なアクセス許可を持つアカウントが必要です。ベストプラクティスとして、必要最小限のアクセス許可のみを持つアカウントを使用します。最小限のアクティブディレクトリ組織単位 (OU) 許可は以下のとおりです。

- コンピュータオブジェクトの作成
- パスワードの変更
- [Reset Password] (パスワードのリセット)
- 説明の書き込み

アクセス許可をセットアップする前に、まず以下の操作を行う必要があります。

- ドメインに参加済みのコンピュータまたは EC2 インスタンスにアクセスします。
- Active Directory User and Computers MMC スナップインをインストールします。詳細については、Microsoft ドキュメントの「Installing or Removing Remote Server Administration Tools for Windows 7」を参照してください。
- 適切なアクセス権限を持つドメインユーザーとしてログインし、OU のセキュリティ設定を変更します。
- アクセス権限を委任するユーザーアカウント、サービスアカウント、またはグループを作成または指定します。

最小限のアクセス権限をセットアップするには

1. ドメインまたはドメインコントローラーで [Active Directory Users and Computers] (アクティブディレクトリユーザーとコンピュータ) を開きます。
2. 左のナビゲーションペインで、ドメイン参加権限を提供する最初の OU を選択して、コンテキスト (右クリック) メニューを開き、[制御の委任] を選択します。
3. [Delegation of Control Wizard] ページで、[Next]、[Add] の順に選択します。
4. [ユーザー、コンピュータ、グループの選択] で、事前に作成したユーザーアカウント、サービスアカウント、またはグループを選択し、[OK] を選択します。

5. [Tasks to Delegate] (委任するタスク) ページで、[Create a custom task to delegate] (委任するカスタムタスクの作成) を選択し、[Next (次へ) を選択します。
6. [Only the following objects in the folder]、[Computer objects] を選択します。
7. [Create selected objects in this folder]、[Next] を選択します。
8. [Permissions] で、[Read]、[Write]、[Change Password]、[Reset Password]、[Next] の順に選択します。
9. [Completing the Delegation of Control Wizard] ページで情報を確認し、[Finish] を選択します。
10. これらのアクセス権限を必要とする追加の OU に対して、ステップ 2 ~ 9 を繰り返します。

グループにアクセス権限を委任した場合は、強力なパスワードを持つユーザーアカウントまたはサービスアカウントを作成し、そのアカウントをグループに追加します。こうすることで、ディレクトリに WorkSpaces を接続するための十分な権限がこのアカウントに与えられます。WorkSpaces Pools ディレクトリ設定を作成するときはこのアカウントを使用します。

## 組織単位の識別子名を検索する

WorkSpaces Pools で Active Directory ドメインを登録する場合は、組織単位 (OU) の識別名が必要です。この目的のために OU を作成します。デフォルトのコンピュータコンテナは OU ではなく、WorkSpaces Pools で使用することはできません。以下に、この名前を取得する手順を示します。

> **Note**
>
> 識別子名は、**OU=** で始まる必要があります。また、その名前をコンピュータオブジェクトに使用することはできません。

この手順を完了するには、まず以下の操作を行う必要があります。

- ドメインに参加済みのコンピュータまたは EC2 インスタンスにアクセスします。
- Active Directory User and Computers MMC スナップインをインストールします。詳細については、Microsoft ドキュメントの「Installing or Removing Remote Server Administration Tools for Windows 7」を参照してください。
- 適切なアクセス権限を持つドメインユーザーとしてログインし、OU のセキュリティプロパティを読み取ります。

OU 識別子名を確認するには

1. ドメインまたはドメインコントローラーで [Active Directory Users and Computers] (アクティブディレクトリユーザーとコンピュータ) を開きます。
2. [View] で、[Advanced Features] が有効になっていることを確認します。
3. 左のナビゲーションペインで、WorkSpaces コンピュータオブジェクトに使用する最初の OU を選択し、コンテキスト (右クリック) メニューを開いて [プロパティ] を選択します。
4. [Attribute Editor] を選択します。
5. [Attributes] の下の [distinguishedName] で、[View] を選択します。
6. [値] で識別子名を選択し、コンテキストメニューを開き、[コピー] を選択します。

## カスタムイメージのローカル管理者権限を付与する

デフォルトでは、Active Directory ドメインユーザーにイメージのローカル管理者権限はありません。この権限を付与するには、ディレクトリのグループポリシーの設定を使用するか、手動でイメージのローカル管理者アカウントを使用します。ローカル管理者権限をドメインユーザーに付与すると、それらのユーザーは、WorkSpaces Pools でアプリケーションをインストールしたり、カスタムイメージを作成したりできます。

内容



### グループポリシー設定を使用する

ローカル管理者権限をアクティブディレクトリのユーザーやグループに付与したり、または指定された OU のすべてのコンピュータオブジェクトに付与したりするには、グループポリシー設定を使用します。ローカル管理者のアクセス許可を付与するアクティブディレクトリユーザーまたはグループが既に存在している必要があります。グループポリシー設定を使用するには、まず、以下の操作を行う必要があります。

- ドメインに参加済みのコンピュータまたは EC2 インスタンスにアクセスします。
- グループポリシーマネジメントコンソール (GPMC) の MMC スナップインをインストールします。詳細については、Microsoft ドキュメントの「Installing or Removing Remote Server Administration Tools for Windows 7」を参照してください。

- アクセス許可を持つドメインユーザーとしてログインし、グループポリシーオブジェクト (GPO) を作成します。GPO を適切な OU にリンクします。

グループポリシー設定を使用して、ローカル管理者のアクセス許可を付与するには

1. ディレクトリまたはドメインコントローラーで、管理者としてコマンドプロンプトを開き、`gpmc.msc` と入力し、ENTER キーを押します。
2. 左のコンソールツリーで、新しい GPO を作成する OU、または既存の GPO を使用する OU を選択して、以下のいずれかの操作を行います。
   - コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, Link it here] を選択して、新しい GPO を作成します。[Name] に、この GPO のわかりやすい名前を入力します。
   - 既存の GPO を選択します。
3. GPO のコンテキストメニューを開き、[編集] を選択します。
4. コンソールツリーで、[Computer Configuration] (コンピュータの構成)、[設定]、[Windows Settings] (Windows 設定)、[Control Panel Settings] (コントロールパネル設定)、[Local Users and Groups] (ローカルユーザーおよびグループ) の順に選択します。
5. [Local Users and Groups] (ローカルユーザーおよびグループ) を選択して、コンテキストメニューを開き、[新規]、[Local Group] (ローカルグループ) の順に選択します。
6. [Action] で、[Update] を選択します。
7. [Group name] で、[Administrators(built-in)] を選択します。
8. [メンバー] で、[追加] を選択して、ストリーミングインスタンスに対するローカル管理者権限を割り当てるアクティブディレクトリユーザーアカウントまたはグループを指定します。[Action] で、[Add to this group] を選択し、[OK] を選択します。
9. この GPO を他の OU に適用するには、追加の OU を選択して、コンテキストメニューを開き、[Link an Existing GPO] (既存の GPO のリンク) を選択します。
10. ステップ 2 で指定した新規または既存の GPO 名を使用して、GPO までスクロールし、[OK] を選択します。
11. この設定が必要な追加の OU に対して、ステップ 9 および 10 を繰り返します。
12. 再度 [OK] を選択して、[New Local Group Properties] (新規のローカルグループプロパティ) ダイアログボックスを閉じます。
13. 再度 [OK] を選択し、GPMC を閉じます。

新しい設定を GPO に適用するには、実行中の Image Builder またはフロートを停止して再起動する必要があります。GPO がリンクされている OU の Image Builder およびフリートのローカル管理者権限が、ステップ 8 で指定したアクティブディレクトリユーザーおよびグループに自動的に付与されます。

WorkSpace でローカル管理者グループを使用してイメージを作成する

Active Directory ユーザーまたはグループにイメージのローカル管理者権限を付与するには、これらのユーザーまたはグループをイメージのローカル管理者グループに手動で追加します。

ローカル管理者権限を付与するアクティブディレクトリユーザーまたはグループが既に存在している必要があります。

1. イメージのビルドに使用する WorkSpace に接続します。WorkSpace が実行中でありドメイン参加済みである必要があります。
2. [開始]、[管理ツール] の順に選択し、[コンピュータの管理] をダブルクリックします。
3. 左のナビゲーションペインで、[Local Users and Groups] を選択して [Groups] フォルダを開きます。
4. [Administrators] グループを開いて [Add...] を選択します。
5. ローカル管理者権限を割り当てるアクティブディレクトリユーザーまたはグループをすべて選択して、[OK] を選択します。再度 [OK] を選択して、[管理者プロパティ] ダイアログボックスを閉じます。
6. コンピュータの管理を閉じます。
7. Active Directory ユーザーとしてログインし、そのユーザーに WorkSpaces のローカル管理者権限があるかどうかを確認するには、[管理者コマンド]、[ユーザーの切り替え] の順に選択し、該当するユーザーの認証情報を入力します。

## ユーザーがアイドル状態の場合にストリーミングセッションをロックする

WorkSpaces Pools では、GPMC の設定を使用して、ユーザーが一定時間アイドル状態になったときにストリーミングセッションをロックできます。GPMC を使用するには、まず、以下の操作を行う必要があります。

- ドメインに参加済みのコンピュータまたは EC2 インスタンスにアクセスします。
- GPMC をインストールします。詳細については、Microsoft ドキュメントの「Installing or Removing Remote Server Administration Tools for Windows 7」を参照してください。

- アクセス許可を持つドメインとしてログインし、GPO を作成します。GPO を適切な OU にリンクします。

ユーザーがアイドル状態のときに自動的にストリーミングインスタンスをロックするには

1. ディレクトリまたはドメインコントローラーで、管理者としてコマンドプロンプトを開き、`gpmc.msc` と入力し、ENTER キーを押します。
2. 左のコンソールツリーで、新しい GPO を作成する OU、または既存の GPO を使用する OU を選択して、以下のいずれかの操作を行います。
   - コンテキスト (右クリック) メニューを開き、[Create a GPO in this domain, Link it here] を選択して、新しい GPO を作成します。[Name] に、この GPO のわかりやすい名前を入力します。
   - 既存の GPO を選択します。
3. GPO のコンテキストメニューを開き、[編集] を選択します。
4. [User Configuration] (ユーザーの構成) を [ポリシー]、[Administrative Templates] (管理用テンプレート)、[コントロールパネル] の順に展開し、[Personalization] (パーソナライズ) を選択します。
5. [スクリーンセーバーの有効化] をダブルクリックします。
6. [Enable screen saver] (スクリーンセーバーの有効化) ポリシー設定で、[有効] を選択します。
7. [適用]、[OK] の順に選択します。
8. [スクリーンセーバーの指定] をダブルクリックします。
9. [Force specific screen saver] (スクリーンセーバーの指定) ポリシー設定で、[有効] を選択します。
10. [Screen saver executable name (スクリーンセーバーの実行ファイル名)] に **`scrnsave.scr`** と入力します。この設定が有効になると、システムによってユーザーのデスクトップに黒いスクリーンセーバーが表示されます。
11. [適用]、[OK] の順に選択します。
12. [スクリーンセーバーのパスワード保護] をダブルクリックします。
13. [Password protect the screen saver] (スクリーンセーバーのパスワード保護) ポリシー設定で、[有効] を選択します。
14. [適用]、[OK] の順に選択します。
15. [スクリーンセーバーのタイムアウト] をダブルクリックします。

16. [Screen saver timeout] (スクリーンセーバーのタイムアウト) ポリシー設定で、[有効] を選択します。
17. [Seconds] (秒) に、スクリーンセーバーが適用されるまでのユーザーのアイドル時間の長さを指定します。アイドル時間を 10 分に設定するには、600 秒を指定します。
18. [適用]、[OK] の順に選択します。
19. コンソールツリーの [User Configuration] (ユーザーの構成) を、[ポリシー]、[Administrative Templates] (管理用テンプレート)、[システム] の順に展開し、[Ctrl+Alt+Del Options] を選択します。
20. [コンピュータのロック解除] をダブルクリックします。
21. [Remove Lock Computer] (コンピュータのロック解除) ポリシー設定で、[無効] を選択します。
22. [適用]、[OK] の順に選択します。

## ドメイン信頼関係を使用するように WorkSpaces Pools を設定する

WorkSpaces Pools は、あるドメインにファイルサーバー、アプリケーション、コンピュータオブジェクトなどのネットワークリソースが存在し、別のドメインにユーザーオブジェクトが存在する Active Directory ドメイン環境をサポートします。コンピュータオブジェクト操作に使用するドメインサービスアカウントが、WorkSpaces Pools コンピュータオブジェクトと同じドメインにある必要はありません。

ディレクトリ設定を作成する際、適切なアクセス許可を持つサービスアカウントを指定して、サーバー、アプリケーション、コンピュータオブジェクト、その他のネットワークリソースが存在するアクティブディレクトリドメインのコンピュータオブジェクトを管理します。

エンドユーザーアクティブディレクトリアカウントには、以下に対して「Allowed to Authenticate」許可が必要です。

- WorkSpaces Pools コンピュータオブジェクト
- ドメインのドメインコントローラー

詳細については、「アクティブディレクトリコンピュータオブジェクトを作成および管理するための許可の付与」を参照してください。

## 詳細情報

このトピックに関連する詳細情報については、以下のリソースを参照してください。

- Microsoft Active Directory — の使用に関する情報 AWS Directory Service。

# WorkSpaces Pools の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、およびソフトウェアリソースの組み合わせです。WorkSpace を起動するときに、必要に応じてバンドルを選択します。WorkSpaces で使用できるデフォルトのバンドルはパブリックバンドルと呼ばれます。WorkSpaces で利用可能なさまざまな公開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。

Windows WorkSpaces を起動してカスタマイズした場合は、その WorkSpace からカスタムイメージを作成して WorkSpaces Pools で使用できます。Linux は WorkSpaces Pools ではサポートされていません。

カスタムイメージには、WorkSpace の OS、ソフトウェア、設定のみが含まれます。カスタムバンドルは、WorkSpace の起動元になるカスタムイメージとハードウェアの両方を組み合わせたものです。

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 WorkSpaces Pools を作成するときにこのカスタムバンドルを指定して、プール内の新しい WorkSpaces が同じ一貫した構成 (ハードウェアとソフトウェア) になるようにします。

WorkSpaces にソフトウェアの更新や追加ソフトウェアのインストールが必要な場合は、カスタムバンドルを更新し、そのバンドルにより WorkSpaces を再構築できます。

WorkSpaces Pools 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。次の表は、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ています。

| 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/サポート終了日 |
|---|---|---|---|---|
| [Windows Server 2019] | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro | 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/サポート終了日 |
| --- | --- | --- | --- | --- |
| Windows Server 2022 | 含まれる | DCV | Standard、Performance、Power、PowerPro、Graphics.G4dn、GraphicsPro.G4dn | 2031 年 10 月 14 日 |

> **Note**
>
> - ベンダーでサポートされなくなったオペレーティングシステムのバージョンは、動作が保証されず、 AWS サポートでもサポートされません。

トピック

- WorkSpaces Pools のバンドルオプション
- WorkSpaces Pools のカスタムイメージとカスタムバンドルを作成する
- WorkSpaces Pools のカスタムイメージとカスタムバンドルを管理する
- セッションスクリプトを使用してユーザーのストリーミングエクスペリエンスを管理する

## WorkSpaces Pools のバンドルオプション

WorkSpaces Pools で使用する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。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。プロトコルの詳細については、「WorkSpaces Personal 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、「WorkSpaces Personal のクライアントネットワークの要件」を参照してください。

WorkSpaces Pools では、次のパブリックバンドルを使用できます。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、Standard、Performance、Power、PowerPro

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
- E 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
- E 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
- E 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
- E 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。

### 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
- E 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 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
- E 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。

## WorkSpaces Pools のカスタムイメージとカスタムバンドルを作成する

WorkSpaces Pools は、Windows のイメージとバンドルのみをサポートします。Windows または WorkSpace を起動してカスタマイズした場合は、その WorkSpace 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。

カスタムイメージには、WorkSpace の OS、ソフトウェア、設定のみが含まれます。カスタムバンドルは、WorkSpace の起動元になるカスタムイメージとハードウェアの両方を組み合わせたものです。

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 WorkSpaces を起動するときにこのカスタムバンドルを指定して、新しい WorkSpaces が同じ一貫した構成 (ハードウェアとソフトウェア) になるようにします。

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**
>
> - カスタムバンドルの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。

目次



## 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。WorkSpace のイメージを作成するには、C ドライブに 12,884,901,888 バイト (または 12 GiB) を超える空き容量があり、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 のステータスが [利用可能] で、変更の状態が [なし] であることが必要です。
- WorkSpaces イメージ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。
- WorkSpace 上で実行されるすべてのアプリケーションサービスは、ドメインユーザー資格情報の代わりにローカルシステムアカウント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。
- WorkSpace は暗号化しないでください。暗号化された WorkSpace からのイメージの作成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、イメージから起動する WorkSpaces は正しく機能しません。詳細については、「the section called “必須の設定とサービスコンポーネント”」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
- WorkSpaces Pools は、バンドル/イメージルートボリュームの最大サイズ 200 GB のみをサポートします。Windows カスタムイメージを作成するときは、ルートボリュームサイズが 200 GB 未満であることを確認します。

## ベストプラクティス

WorkSpace からイメージを作成する前に、以下を実行します。

- 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。
- WorkSpace をプライベートサブネットにデプロイし、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 WorkSpace の最小ボリュームサイズを使用し、カスタムバンドルの作成時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プログラム (Windows の機能/バージョンの更新プログラムを除く) とすべてのアプリケーション更新プログラムを WorkSpace にインストールします。
- バンドルに含めるべきでない WorkSpace からキャッシュされたデータを削除します (たとえば、ブラウザの履歴、キャッシュされたファイル、ブラウザの Cookie など)。
- バンドルに含めるべきではない WorkSpace から構成設定を削除します (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ます。デフォルトでは、リージョンごとに 40 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 制限のフォームを使用します。

- 暗号化された WorkSpace 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。暗号化された WorkSpace からのイメージの作成は現在サポートされていません。
- WorkSpace でウイルス対策ソフトウェアを実行している場合は、イメージの作成時に無効にします。
- WorkSpace でファイアウォールを有効にしている場合は、ファイアウォールによって必要なポートがブロックされていないことを確認します。詳細については、「WorkSpaces Personal の IP アドレスとポートの要件」を参照してください。
- Windows WorkSpaces の場合、イメージを作成する前にグループポリシーオブジェクト (GPO) を設定しないでください。
- Windows WorkSpaces の場合、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。
- ENA、NVMe、PV ドライバーなど、WorkSpaces のネットワーク依存関係ドライバーを必ず更新してください。この作業は、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)、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に関する説明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。この作業は、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 および 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

カスタムイメージから起動した WorkSpaces の場合、デフォルトのコンピュータ名の形式を使用する代わりに、コンピュータ名の形式にカスタムプレフィックスを指定できます。デフォルトでは、Windows 10 WorkSpaces のコンピュータ名の形式は `DESKTOP-XXXXX` であり、Windows 11 WorkSpaces のコンピュータ名の形式は `WORKSPA-XXXXX` です。カスタムプレフィックスを指定する手順は以下のとおりです。

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で `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml` 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。

WorkSpace の Windows エクスプローラーから C: ドライブにアクセスするには、アドレスバーに C:\ 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 のドキュメントの「ComputerName」をご参照ください。
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、<RegisteredOrganization> に Amazon.com、<RegisteredOwner> に **EC2** を指定した場合、カスタムバンドルから作成された WorkSpaces のコンピュータ名は EC2AMAZ-*xxxxxxx* で始まります。

   <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。

## ステップ 2: Image Checker を実行する

Windows WorkSpace がイメージ作成の要件を満たしていることを確認するには、Image Checker アプリケーションを実行することをお勧めします。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。Image Checker は Windows WorkSpaces でのみ使用できます。

> **Important**
>
> - WorkSpace は、Image Checker によって実行されるすべてのテストに合格した後に、イメージの作成に使用できます。
> - Image Checker を実行する前に、WorkSpace に最新の Windows セキュリティと累積更新プログラムがインストールされていることを確認します。

Image Checker を入手するには、以下のいずれかを実行します。

- WorkSpace を再起動します。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 から Amazon WorkSpaces Image Checker をダウンロードし、 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、[Run (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。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、テストの失敗と警告の原因となる問題を解決し、WorkSpace がすべてのテストに合格するまで Image Checker の実行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. WorkSpace 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。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ことが必要

最新バージョンの Microsoft Windows PowerShell をインストールします。

> **Important**
>
> WorkSpace の PowerShell 実行ポリシーは、RemoteSigned スクリプトを許可するように設定する必要があります。実行ポリシーを確認するには、Get-ExecutionPolicy PowerShell コマンドを実行します。実行ポリシーが Unrestricted または RemoteSigned に設定されていない場合は、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 設定では、イメージの作成に必要な Amazon WorkSpaces でスクリプトを実行できます。

C および D ドライブのみが存在できる

イメージの作成に使用される WorkSpace には、`C` および `D` ドライブのみが存在できます。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 の累積的な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 のイメージ作成プロセスでサポートされます。

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 サポート 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 WorkSpaces では、ユーザープロファイル (`D:\Users\`*`username`*) は合計で 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 WorkSpaces では、ドライブ C には 12 GB 以上の空き容量が必要です。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 WorkSpaces では、FAILED メッセージが表示され、ディスク容量が 2 GB を超えている場合は、無視できます。

### ドメインアカウントで実行できるサービスがない

イメージ作成プロセスを実行するために、WorkSpace にドメインアカウントで実行できるサービスがありません。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] を選択してください。

### DHCP を使用するように WorkSpace を設定することが必要

静的 IP アドレスの代わりに DHCP を使用するように、WorkSpace のすべてのネットワークアダプター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] を選択してください。
9. WorkSpace 上のすべてのネットワークアダプターに対してこのプロセスを繰り返します。

### 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] を選択してください。

### ユーザープロファイルが存在することが必要

イメージの作成に使用する WorkSpace には、ユーザープロファイル (`D:\Users\`*`username`*) が必要です。このテストに失敗した場合は、AWS サポート 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のパスに、System32 と Windows PowerShell のエントリがありません。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] を選択してください。
7. WorkSpace を再起動します。

> **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ために、WorkSpace の環境変数のパスを、新しく作成された WorkSpace または新しい Windows インスタンスのパスと比較できます。

### 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] を選択してください。

### 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] を選択してください。

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。

WorkSpace に存在できるユーザープロファイルは 1 つのみ

イメージの作成に使用している WorkSpace に存在できる WorkSpaces ユーザープロファイル (`D:\Users\`*`username`*) は 1 つのみです。WorkSpace の対象ユーザーに属していないユーザープロファイルを削除します。

イメージの作成用に、WorkSpace に 3 つのユーザープロファイルのみを含めることができます。

- WorkSpace の対象ユーザーのユーザープロファイル (`D:\Users\`*`username`*)
- 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、および対象の WorkSpaces ユーザー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、その追加の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、WorkSpace に属していない他のプロファイルを削除します。
6. [OK] を 2 回選択し、コントロールパネルを閉じます。
7. WorkSpace を再起動します。

### 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、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を行っていない WorkSpace 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

Image Checker で実行されるすべてのテストに WorkSpace が合格したにもかかわらず、WorkSpace からイメージを作成できない場合は、以下の点を確認します。

- WorkSpace が Domain Guests 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、以下の PowerShell コマンドを実行します。

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- 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。イメージを作成しようとする前に、継承がブロックされて GPO が適用されていない新しい組織単位 (OU) に、WorkSpace 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] を選択してください。

## 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、次の手順を実行して、WorkSpaces コンソールを使用してカスタムイメージとカスタムバンドルを作成します。プログラムによって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」の「CreateWorkspaceImage」を参照してください。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 リファレンスの CreateWorkspaceBundle を参照してください。

WorkSpaces コンソールを使用して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. 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。
2. https://console.aws.amazon.com/workspaces/v2/home://www.com」で WorkSpaces コンソールを開きます。
3. ナビゲーションペインで [WorkSpaces] を選択します。
4. WorkSpace を選択して詳細ページを開き、[Create image] (イメージ) の作成を選択します。WorkSpace の状態が [Stopped] (停止) の場合、[Actions] (アクション)、[Start WorkSpaces] (WorkSpaces の起動) の順に選択してから、[Actions] (アクション)、[Create Image] (イメージの作成) を選択する必要があります。
5. 続行する前に WorkSpace を再起動するように求めるメッセージが表示されます。WorkSpace を再起動すると、Amazon WorkSpaces ソフトウェアが最新バージョンに更新されます。

   メッセージを閉じて、WorkSpaces Personal の WorkSpace を再起動する のステップに従って WorkSpace を再起動します。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、WorkSpace のステータスが [利用可能]で、変更の状態が [なし] 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。イメージが作成されている間、WorkSpace のステータスは [Suspended (停止)] となり、WorkSpace は使用できません。

   説明には特殊文字のダッシュ (-) を使用しないでください。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。WorkSpace のステータスが [Available] (使用可能) に変わると、イメージは完成です (これには最長 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。
9. バンドル名と説明を入力し、次の操作を行います。

   - [Bundle hardware type] (バンドルハードウェアタイプ) で、このカスタムバンドルから WorkSpaces を起動するときに使用するハードウェアを選択します。
   - ルートボリュームのデフォルトの使用可能なサイズの組み合わせは、WorkSpace あたり 200 GB です。
10. 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アイテム

Windows WorkSpace からイメージを作成すると、C ドライブの内容全体が含まれます。

- 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\

## WorkSpaces Pools のカスタムイメージとカスタムバンドルを管理する

カスタムイメージとカスタムバンドルを管理するプロセスは、WorkSpaces Personal も WorkSpaces Pools も同じです。イメージとバンドルの管理方法の詳細については、このガイドの WorkSpaces Personal セクションにある以下のドキュメントを参照してください。

> **Note**
>
> WorkSpaces Personal で使用できるカスタムバンドルと WorkSpaces Pools で使用できるカスタムバンドルの主な違いは、使用できるオペレーティングシステムとベースとなるパブリックバンドルです。WorkSpaces Pools でサポートされているオペレーティングシステムとバンドルについては、「
>
> > 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、およびソフトウェアリソースの組み合わせです。WorkSpace を起動するときに、必要に応じてバンドルを選択します。WorkSpaces で使用できるデフォルトのバンドルはパブリックバンドルと呼ばれます。WorkSpaces で利用可能なさまざまな公開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。
> >
> > 次の表は、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ています。
>
> | | | | |
> |---|---|---|---|
> | [Windows Server 2019] | 含まれる | DCV | Value、Standard、Performance、Power、PowerPro |
> | Windows Server 2022 | 含まれる | DCV | Standard、Performance、Power、PowerPro、 |

| | | | |
|---|---|---|---|
| | | | Graphics.G4dn、GraphicsPro.G4dn |

| | 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 |
|---|---|---|---|---|

> **Note**
>
> - ベンダーでサポートされ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 サポートでもサポートされません。

」を参照してください。

- WorkSpaces Personal のカスタムバンドルを更新する.
- WorkSpaces Personal でカスタムイメージをコピーする.
- WorkSpaces Personal でカスタムイメージを共有または共有解除する.
- WorkSpaces Personal でカスタムバンドルまたはイメージを削除する.

## セッションスクリプトを使用してユーザーのストリーミングエクスペリエンスを管理する

WorkSpaces Pools には、インスタンスセッションスクリプトが用意されています。ユーザーのストリーミングセッションで特定のイベントが発生したときに、これらのスクリプトを使用して独自のカスタムスクリプトを実行できます。例えば、ユーザーのストリーミングセッションが開始される前に、カスタムスクリプトを使用して WorkSpaces Pools 環境を準備できます。ユーザーがストリーミングセッションを完了した後に、カスタムスクリプトを使用してストリーミングインスタンスをクリーンアップすることもできます。

セッションスクリプトは WorkSpace イメージ内で指定します。これらのスクリプトはユーザーコンテキストまたはシステムコンテキスト内で実行されます。セッションスクリプトが情報、エラー、またはデバッグメッセージの書き込みに標準出力を使用する場合は、オプションで、それらを Amazon Web Services アカウント内の Amazon S3 バケットに保存することができます。

内容



## ストリーミングセッションの開始前にスクリプトを実行する

ユーザーのアプリケーションが起動されてストリーミングセッションが開始されるまでに最大 60 秒間実行されるようにスクリプトを設定できます。それにより、ユーザーがアプリケーションのストリーミングを開始する前に WorkSpaces Pools 環境をカスタマイズできます。セッションスクリプトが実行されると、読み込みスピナーがユーザーに表示されます。スクリプトが正常に完了するか、最大待機時間が経過すると、ユーザーのストリーミングセッションが開始されます。スクリプトが正常に完了しなかった場合は、エラーメッセージがユーザーに表示されます。ただし、ユーザーはストリーミングセッションの使用を禁止されません。

Windows インスタンスでファイル名を指定するときは、ダブルバックスラッシュを使用する必要があります。例えば、次のようになります。

```
C:\\Scripts\\Myscript.bat
```

二重のバックスラッシュを使用しないと、.json ファイル形式が正しくないことを示すエラーが表示されます。

> **Note**
>
> スクリプトは正常に完了したら、値 0 を返します。スクリプトが 0 以外の値を返した場合、WorkSpaces はユーザーにエラーメッセージを表示します。

ストリーミングセッションの開始前にスクリプトを実行すると、以下のプロセスが発生します。

1. ユーザーが、ドメインに参加していない WorkSpaces Pool の WorkSpace に接続されます。接続には SAML 2.0 を使用します。
2. 以下のいずれかのプロセスが発生します。
   - ユーザーに対してアプリケーション設定の永続化が有効になっている場合は、ユーザーのカスタマイズ内容と Windows の設定内容を保存しているアプリケーション設定の Virtual Hard Disk (VHD) ファイルがダウンロードされてマウントされます。この場合は、Windows ユーザーのログインが必要です。

     アプリケーション設定の永続化については、WorkSpaces Pools ユーザーのアプリケーション設定の永続化を有効にする を参照してください。
   - アプリケーション設定の永続化が有効になっていない場合、Windows ユーザーはすでにログインしています。
3. セッションスクリプトが起動されます。ユーザーに対して永続的ストレージが有効になっている場合は、ストレージコネクタのマウントも開始されます。永続的ストレージについては、WorkSpaces Pools で永続的ストレージを有効にして管理する を参照してください。

   > **Note**
   >
   > ストリーミングセッションを開始するためにストレージコネクタのマウントを完了する必要はありません。セッションスクリプトが完了したとき、まだストレージコネクタのマウントが完了していなくても、ストリーミングセッションは開始されます。
   > ストレージコネクタのマウント状況のモニタリングについては、セッションスクリプトで永続的ストレージを使用する を参照してください。

4. セッションスクリプトは完了するかタイムアウトします。
5. ユーザーのストリーミングセッションが開始されます。

## ストリーミングセッションの終了後にスクリプトを実行する

ユーザーのストリーミングセッションの終了後にスクリプトを実行するように設定することもできます。例えば、ユーザーが WorkSpaces クライアントのツールバーから [セッションの終了] を選択したとき、またはユーザーが許容される最大セッション時間に達したときに、スクリプトを実行できます。これらのセッションスクリプトを使用して、ストリーミングインスタンスが終了する前に WorkSpaces 環境をクリーンアップすることもできます。たとえば、スクリプトを使用してファイルロックを解除したり、ログファイルをアップロードしたりできます。ストリーミングセッションの終了後にスクリプトを実行すると、以下のプロセスが発生します。

1. ユーザーの WorkSpaces ストリーミングセッションが終了します。
2. セッション終了スクリプトが起動されます。
3. セッション終了スクリプトが完了またはタイムアウトします。
4. Windows ユーザーのログアウトが発生します。
5. 以下のうち該当する一方が実行されるか、両方が同時に実行されます。
   - ユーザーに対してアプリケーション設定の永続化が有効になっている場合、ユーザーのカスタマイズ内容と Windows 設定内容を保存しているアプリケーション設定の VHD ファイルがマウント解除され、アカウントの Amazon S3 バケットにアップロードされます。
   - ユーザーに対して永続的ストレージが有効になっている場合、ストレージコネクタは最後の同期を完了し、マウント解除されます。
6. WorkSpace が終了します。

## セッションスクリプトを作成および指定する

WorkSpaces Pools の WorkSpaces のセッションスクリプトを作成して指定するには、次の手順を実行します。

1. カスタムイメージを作成する Windows WorkSpaces に接続します。
2. ディレクトリがまだ存在しない`/AWSEUC/SessionScripts`場合は作成します。
3. セッションスクリプト設定テンプレートを使用して、設定ファイルが存在しない`/AWSEUC/SessionScripts/config.json`場合は作成します。
4. `C:\AWSEUC\SessionScripts` に移動し、`config.json` 設定ファイルを開きます。

   セッションスクリプトパラメータについては、セッションスクリプト設定ファイル を参照してください。
5. 変更が終了したら、`config.json` ファイルを保存して閉じます。
6. WorkSpace からイメージを作成する手順を完了します。詳細については、「WorkSpaces Pools のカスタムイメージとカスタムバンドルを作成する」を参照してください。

## セッションスクリプト設定ファイル

Windows インスタンス上のセッションスクリプト設定ファイルを見つけるには、`C:\AWSEUC\SessionScripts\config.json` に移動します。ファイル形式は次のとおりです。

> **Note**
>
> 設定ファイルは JSON 形式です。このファイルに入力したテキストが有効な JSON 形式であることを確認します。

```
{
  "SessionStart": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  },
  "SessionTermination": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  }
}
```

セッションスクリプト設定ファイルでは、以下のパラメータを使用できます。

**SessionStart/SessionTermination**

オブジェクトの名前に基づいて該当するセッションイベントで実行するセッションスクリプト。

型: 文字列

必須: いいえ

使用できる値: **SessionStart**、**SessionTermination**

**WaitingTime**

セッションスクリプトの最大期間 (秒単位)。

タイプ: 整数

必須: いいえ

制約: 最大期間は 60 秒です。セッションスクリプトは、この期間内に完了しない場合、停止されます。スクリプトを引き続き実行する必要がある場合は、別のプロセスとして起動してください。

**Executables**

実行するセッションスクリプトの詳細。

型: 文字列

必須: はい

制約: セッションイベントごとに実行できるスクリプトの最大数は 2 です (1 つはユーザーコンテキスト用、もう 1 つはシステムコンテキスト用)。

**Context**

セッションスクリプトを実行するコンテキスト。

型: 文字列

必須: はい

使用できる値: **user**、**system**

**`Filename`**

実行するセッションスクリプトへの完全パス。このパラメータを指定しない場合、セッションスクリプトは実行されません。

型: 文字列

必須: いいえ

制約: ファイル名と完全パスの最大長は 1,000 文字です。

使用できる値: **`.bat`**、**`.exe`**、**`.sh`**

> **Note**
>
> Windows PowerShell ファイルを使用することもできます。詳細については、「Windows PowerShell ファイルの使用」を参照してください。

**`Arguments`**

セッションスクリプトまたは実行可能ファイルの引数。

型: 文字列

必須: いいえ

長さの制限: 最大長は 1,000 文字です。

**`S3LogEnabled`**

このパラメータの値が **`True`** に設定されていると、セッションスクリプトによって作成されたログを保存するための S3 バケットが Amazon Web Services アカウント内に作成されます。デフォルトではこの値は **`True`** に設定されます。詳細については、このトピックの後半の「セッションスクリプト出力のログ記録」セクションを参照してください。

型: ブール

必須: いいえ

使用できる値: **`True`**、**`False`**

### Windows PowerShell ファイルの使用

Windows PowerShell ファイルを使用するには、`filename` パラメータに PowerShell ファイルへの絶対パスを指定します。

```
"filename":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
```

次に、**`arguments`** パラメータにセッションスクリプトを指定します。

```
"arguments": "-File \"C:\\path\\to\\session\\script.ps1\"",
```

最後に、PowerShell 実行ポリシーで PowerShell ファイルの実行が許可されていることを確認します。

### セッションスクリプト出力のログ記録

設定ファイルでこのオプションが有効になっていると、セッションスクリプトから標準出力に書き込まれた出力が WorkSpaces Pools によって自動的に収集されます。この出力はアカウントの Amazon S3 バケットにアップロードされます。トラブルシューティングやデバッグの目的でログファイルを確認できます。

> **Note**
>
> ログファイルは、セッションスクリプトが値を返したときか、**`WaitingTime`** に設定された時間を経過したときの、どちらか早いほうでアップロードされます。

### セッションスクリプトで永続的ストレージを使用する

WorkSpaces の永続的ストレージを有効にすると、セッション開始スクリプトの実行時にストレージのマウントが開始されます。マウントされている永続的ストレージにスクリプトが依存している場合は、コネクタが使用可能になるまで待つことができます。WorkSpaces は、以下のキーで、Windows WorkSpaces の Windows レジストリにあるストレージコネクタのマウントステータスを維持します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AWSEUC\Storage\<provided user
                name>\<Storage connector>
```

レジストリキーの値は以下のとおりです。

- 提供されたユーザー名 — アクセスモードで提供されたユーザー ID。アクセスモードと各モードの値は以下のとおりです。
  - ユーザープール — ユーザーの E メールアドレス。
  - ストリーミング URL — ユーザー ID。
  - SAML — NameID。ユーザー名にスラッシュが含まれる場合 (ドメインユーザーの SAMAccountName が含まれる場合など)、スラッシュは「-」文字に置き換えられます。
- ストレージコネクタ — ユーザーに対して有効になっている永続的ストレージオプションに対応するコネクタ。ストレージコネクタの値は以下のとおりです。
  - HomeFolder

ストレージコネクタの各レジストリキーには MountStatus DWORD 値が含まれています。次の表は、MountStatus に指定できる値の一覧です。

> **Note**
>
> これらのレジストリキーを表示するには、イメージに Microsoft .NET Framework バージョン 4.7.2 以降がインストールされている必要があります。

| 値 | 説明 |
| --- | --- |
| 0 | ストレージコネクタはこのユーザーに対して有効になっていない |
| 1 | ストレージコネクタのマウントが進行中 |
| 2 | ストレージコネクタのマウントに成功した |
| 3 | ストレージコネクタのマウントに失敗した |
| 4 | ストレージコネクタのマウントは有効ですが、まだマウントされていません |

## セッションスクリプトログに対して Amazon S3 バケットストレージを有効にする

セッションスクリプト設定で Amazon S3 のログ記録を有効にすると、WorkSpaces Pools によってセッションスクリプトから標準出力に書き込まれた出力が収集されます。出力は、Amazon Web Services アカウント内の S3 バケットに定期的にアップロードされます。WorkSpaces Pool は、すべての AWS リージョンについて、アカウントとリージョンに固有のバケットをアカウントに作成します。

これらの S3 バケットを管理するための設定タスクを実行する必要はありません。それらのタスクは WorkSpaces サービスによって完全に管理されています。各バケットに保存されているログファイルは、転送時には Amazon S3 の SSL エンドポイントを使用して暗号化され、保管時には Amazon S3 管理の暗号化キーを使用して暗号化されます。バケットは、以下にあるような特定の形式で命名されます。

```
wspool-logs-<region-code>-<account-id-without-hyphens>-random-identifier
```

***<region-code>***

これは、セッションスクリプトログに対して Amazon S3 バケットストレージを有効にして WorkSpaces Pool を作成する AWS リージョンコードです。

***<account-id-without-hyphens>***

ご自身の Amazon Web Services アカウント ID ランダムな ID は、そのリージョン内のその他バケットとの競合が発生しないことを確実にします。バケット名の最初の部分 `wspool-logs` は、複数のアカウントやリージョンにまたがる場合でも変更されません。

例えば、アカウント番号 `123456789012` の米国西部 (オレゴン) リージョン (`us-west-2`) のイメージでセッションスクリプトを指定した場合、WorkSpaces Pools では、そのリージョンのアカウント内に以下の名前で Amazon S3 バケットが作成されます。適切なアクセス許可を持つ管理者のみが、このバケットを削除できます。

```
wspool-logs-us-west-2-1234567890123-abcdefg
```

セッションスクリプトを無効にしても、S3 バケットに保存されているログファイルは削除されません。ログファイルを完全に削除するには、Amazon S3 コンソールまたは API を使用して、ユーザーまたは適切なアクセス許可を持つ別の管理者が削除する必要があります。WorkSpaces Pools には、バケットの誤った削除を防止するバケットポリシーが追加されます。

セッションスクリプトを有効にすると、開始されるストリーミングセッションごとに固有のフォルダが作成されます。

アカウントの S3 バケットでログファイルが保存されているフォルダへのパスは、以下の構造になります。

```
<bucket-name>/<stack-name>/<fleet-name>/<access-mode>/<user-id-SHA-256-hash>/<session-id>/SessionScriptsLogs/<session-event>
```

***<bucket-name>***

セッションスクリプトが保存されている S3 バケットの名前。名前の形式については、このセクションで先ほど説明しました。

***<stack-name>***

セッションが発生したスタックの名前。

***<fleet-name>***

セッションスクリプトが実行されている WorkSpaces Pools の名前。

***<access-mode>***

ユーザーの ID メソッド: WorkSpaces API または CLI の場合は `custom`、SAML の場合は `federated`、ユーザープールのユーザーの場合は `userpool`。

***<user-id-SHA-256-hash>***

ユーザー固有のフォルダ名。この名前は、ユーザー識別子から生成された小文字の SHA-256 ハッシュ 16 進数文字列を使用して作成されます。

***<session-id>***

ユーザーのストリーミングセッションの識別子。ユーザーの各ストリーミングセッションでは一意の ID が生成されます。

***<session-event>***

セッションスクリプトログを生成したイベント。イベント値は `SessionStart` と `SessionTermination` です。

以下のフォルダ構造の例は、test-stack と test-fleet から始まるストリーミングセッションに当てはまります。セッションでは`testuser@mydomain.com`、 の ID からユーザー AWS アカウント ID の

API と123456789012、test-stack米国西部 (オレゴン) リージョン () の設定グループを使用しますus-west-2。

```
wspool-logs-us-west-2-1234567890123-abcdefg/test-stack/test-fleet/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13/05yd1391-4805-3da6-
f498-76f5x6746016/SessionScriptsLogs/SessionStart/
```

このフォルダ構造の例には、ユーザーコンテキストセッション開始スクリプト用の 1 つのログファイルと、必要に応じてシステムコンテキストセッション開始スクリプト用の 1 つのログファイルが含まれています。

# WorkSpaces Pools のモニタリング

モニタリングは、WorkSpaces Pools の信頼性、可用性、および性能を維持するうえで重要な部分です。

内容



## WorkSpaces Pools のメトリクスとディメンション

Amazon WorkSpaces は、次の WorkSpaces Pools メトリクスおよびディメンション情報を Amazon CloudWatch に送信します。

WorkSpaces Pools は、メトリクスを CloudWatch に毎分 1 回送信します。AWS/Workspaces 名前空間には、次のメトリクスが含まれます。

### プール使用状況メトリクス

| メトリクス | 説明 |
| --- | --- |
| ActiveUserSessionCapacity | ストリーミングセッションに現在使用中のユーザーセッションの数。<br><br>単位: カウント<br><br>有効な統計: Average、Minimum、Maximum |

| メトリクス | 説明 |
| --- | --- |
| ActualUserSessionCapacity | ストリーミングに使用可能であるか、現在ストリーミング中であるプールの合計数。<br>`ActualUserSessionCapacity = AvailableUserSessionCapacity + ActiveUserSessionCapacity`<br>単位: カウント<br>有効な統計: Average、Minimum、Maximum |
| AvailableUserSessionCapacity | 現在、ユーザーストリーミングに使用可能なアイドル状態のプールセッションの数。<br>`AvailableUserSessionCapacity = ActualUserSessionCapacity - ActiveUserSessionCapacity`<br>単位: カウント<br>有効な統計: Average、Minimum、Maximum |
| PendingUserSessionCapacity | プールにプロビジョニングされるセッションの数。プロビジョニングの完了後にプールがサポートできるストリーミングセッションの追加の数を表します。<br>単位: カウント<br>有効な統計: Average、Minimum、Maximum |

| メトリクス | 説明 |
| --- | --- |
| UserSessionsCapacityUtilization | プールで使用中のセッションの割合 (%)。次の数式を使用します。<br>`UserSessionCapacityUtilization = (ActiveUserSessionCapacity / ActualUserSessionCapacity) * 100`<br>このメトリクスをモニタリングすると、プールの必要な容量値を増減する決定に役立ちます。<br>単位: パーセント<br>有効な統計: Average、Minimum、Maximum |
| DesiredUserSessionCapacity | 実行中または保留中のセッションの合計数。これはプールが安定した状態でサポートできる同時ストリーミングセッションの合計数を表します。<br>`DesiredUserSessionCapacity = ActualUserSessionCapacity + PendingUserSessionCapacity`<br>単位: カウント<br>有効な統計: Average、Minimum、Maximum |
| InsufficientCapacityError | 容量不足により拒否されたセッションリクエストの数。<br>このメトリクスを使用して、ストリーミングセッションを待機中のユーザーを通知するようアラームを設定できます。<br>単位: カウント<br>有効な統計: Average、Minimum、Maximum、Sum |

# WorkSpaces Pools で永続的ストレージを有効にして管理する

WorkSpaces Pools は、永続的ストレージのホームフォルダをサポートしています。WorkSpaces Pools 管理者は、ユーザーの永続的ストレージを有効にして管理するために、次のタスクの実行方法を理解しておく必要があります。

内容



# WorkSpaces Pools ユーザーのホームフォルダを有効にして管理する

WorkSpaces Pools でホームフォルダを有効にすると、ユーザーはストリーミングセッション中に永続的ストレージのフォルダにアクセスできます。ユーザーがホームフォルダにアクセスするために必要な設定はありません。ユーザーが自分のホームフォルダに保存したデータは、Amazon Web Services アカウントの Amazon Simple Storage Service バケットに自動的にバックアップされ、そのユーザーの後のセッションで使用できるようになります。

転送中のファイルやフォルダは Amazon S3 の SSL エンドポイントを使用して暗号化されます。保管中のファイルやフォルダは Amazon S3 で管理される暗号化キーを使用して暗号化されます。

ホームフォルダは WorkSpaces Pools の WorkSpaces で次のデフォルトの場所に保存されます。

- シングルセッションの、ドメイン参加していない Windows WorkSpaces の場合: `C:\Users\PhotonUser\My Files\Home Folder`
- ドメイン参加している Windows WorkSpaces の場合: `C:\Users\%username%\My Files\Home Folder`

ホームフォルダを保存先とするようにアプリケーションを設定する場合は、該当パスを管理者として使用します。ユーザーがホームフォルダを見つけられない場合があります。アプリケーションによっては、File Explorer の最上位フォルダとしてホームフォルダを表示する、リダイレクトを認識しないためです。このような場合は、File Explorer 内の同じディレクトリを参照することで、ユーザーがホームフォルダにアクセスにできます。

目次



## 計算集約型アプリケーションに関連するファイルとディレクトリ

WorkSpaces Pools ストリーミングセッションでは、計算集約型アプリケーションに関連付けられた大きなファイルとディレクトリを永続ストレージに保存すると、基本的な生産性アプリケーション

に必要なファイルとディレクトリを保存するよりも時間がかかる場合があります。たとえば、アプリケーションが大量のデータを保存したり、同じファイルを頻繁に変更したりする場合は、1 回の書き込み操作を実行するアプリケーションによって作成されたファイルを保存する場合よりも時間がかかる場合があります。また、多くの小さなファイルを保存するのに時間がかかる場合があります。

コンピューティング負荷の高いアプリケーションに関連付けられたファイルとディレクトリをユーザーが保存し、WorkSpaces Pools の永続的ストレージオプションが期待どおりに動作しない場合は、Amazon FSx for Windows File Server や AWS Storage Gateway ファイルゲートウェイなどのサーバーメッセージブロック (SMB) ソリューションを使用することをお勧めします。以下は、これらの SMB ソリューションでの使用に適した、計算集約型アプリケーションに関連するファイルとディレクトリの例です。

- 統合開発環境 (IDE) 用の Workspace フォルダ
- ローカルデータベースファイル
- グラフィックシミュレーションアプリケーションによって作成されたスクラッチスペースフォルダ

詳細については、「AWS Storage Gateway ユーザーガイド」の「ファイルゲートウェイ」を参照してください。

## WorkSpaces Pools ユーザーのホームフォルダを有効にする

ホームフォルダを有効にする前に、以下を実行する必要があります。

- Amazon S3 アクションの正しい AWS Identity and Access Management (IAM) アクセス許可があることを確認します。
- 2017 年 5 月 18 日以降にリリースされた AWS ベースイメージから作成されたイメージを使用します。
- インターネットアクセスまたは Amazon S3 の VPC エンドポイントを設定して、Virtual Private Cloud (VPC) から Amazon S3 へのネットワーク接続を有効にします。詳細については、「WorkSpaces Pools のネットワークとアクセス」および「WorkSpaces Pools 機能で Amazon S3 VPC エンドポイントを使用する」を参照してください。

ディレクトリの作成中 (「」を参照SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する )、またはディレクトリの作成後に WorkSpaces Pools AWS Management Console の を使用して、ホームフォルダを有効または無効にできます。ホームフォルダは、 AWS リージョンごとに Amazon S3 バケットにバックアップされます。

AWS リージョンの WorkSpaces Pools ディレクトリで初めてホームフォルダを有効にすると、サービスによって、同じリージョンの対象アカウントに Amazon S3 バケットが作成されます。同じバケットを使用して、そのリージョンのすべてのユーザーおよびすべてのディレクトリのホームフォルダのコンテンツが保存されます。詳細については、「Amazon S3 バケットのストレージ」を参照してください。

ディレクトリの作成時にホームフォルダを有効にするには

- 「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」の手順に従い、[Enable Home Folders (ホームフォルダを有効にする)] が選択されていることを確認します。

既存のディレクトリのホームフォルダを有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. 左側のナビゲーションペインで [ディレクトリ] を選択し、ホームフォルダを有効にするディレクトリを選択します。
3. ディレクトリリストの下の [ストレージ] をクリックし、[ホームフォルダを有効化] を選択します。
4. [Enable Home Folders] ダイアログボックスで、[Enable] を選択します。

## ホームフォルダを管理する

目次



### ホームフォルダを無効にする

既にホームフォルダに保存されているユーザーコンテンツを失うことなく、ディレクトリのホームフォルダを無効にできます。ディレクトリのホームフォルダを無効にすると、次のようになります。

- ディレクトリのアクティブなストリーミングセッションに接続されているユーザーはエラーメッセージを受け取ります。ホームフォルダにコンテンツを保存できなくなることが通知されます。

- ホームフォルダが無効になったディレクトリを使用する新しいセッションでは、ホームフォルダは表示されません。
- 1 つのディレクトリのホームフォルダを無効にしても、他のディレクトリでは無効になりません。
- すべてのディレクトリでホームフォルダが無効になっている場合でも、WorkSpaces Pools でユーザーコンテンツが削除されることはありません。

ディレクトリのホームフォルダへのアクセスを復元するには、このトピックの前半で説明した手順に従って、ホームフォルダをもう一度有効にします。

ディレクトリの作成時にホームフォルダを無効にするには

- 「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」の手順に従い、[Enable Home Folders (ホームフォルダを有効にする)] オプションが選択解除されていることを確認します。

既存のディレクトリのホームフォルダを無効にするには

1. https://console.aws.amazon.com/workspaces/v2/home で WorkSpaces コンソールを開きます。
2. 左側のナビゲーションペインで [ディレクトリ] を選択し、ホームフォルダを有効にするディレクトリを選択します。
3. ディレクトリリストの下の [ストレージ] をクリックし、[ホームフォルダを有効化] を選択解除します。
4. [Disable Home Folders] ダイアログボックスで、CONFIRM (大文字と小文字は区別されます) と入力し選択を確認します。次に [Disable] を選択します。

Amazon S3 バケットのストレージ

WorkSpaces Pools は、アカウントで作成された Amazon S3 バケットを使用して、ホームフォルダに保存されているユーザーコンテンツを管理します。 AWS リージョンごとに、WorkSpaces Pools はアカウントにバケットを作成します。そのリージョン内のディレクトリのストリーミングセッションから生成されたすべてのユーザーコンテンツが、そのバケットに保存されます。このバケットは、管理者が入力または設定することなく、サービスによって完全に管理されます。このバケットの名前は、次のように特定の形式で付けられます。

```
wspool-home-folder-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

ここで*<region-code>*、 はディレクトリが作成される AWS リージョンコードで、 *<account-id-without-hyphens>* は Amazon Web Services アカウント ID です。*>random-identifier<* は WorkSpaces サービスによって生成されるランダムな識別子番号です。バケット名の最初の部分 `wspool-home-folder-` は、複数のアカウントやリージョンにまたがる場合でも変更されません。

例えば、アカウント番号 123456789012 で米国西部 (オレゴン) リージョン (us-west-2) のディレクトリのホームフォルダを有効にした場合、サービスによってこのリージョンに以下の名前で Amazon S3 バケットが作成されます。適切なアクセス許可を持つ管理者のみが、このバケットを削除できます。

```
wspool-home-folder-us-west-2-123456789012
```

前述のとおり、ディレクトリでホームフォルダを無効にしても、Amazon S3 バケットに保存されたユーザーコンテンツは削除されません。ユーザーコンテンツを完全に削除するには、適切なアクセス権限を持った管理者が、Amazon S3 コンソールから行う必要があります。WorkSpaces Pools には、バケットの誤った削除を防止するバケットポリシーが追加されます。

ホームフォルダコンテンツの同期

ホームフォルダが有効になっている場合、WorkSpaces Pools では、コンテンツを保存するユーザーごとに一意のフォルダが作成されます。このフォルダは、 Amazon Web Services アカウント (リージョン) にある S3 バケット内のユーザー名のハッシュを使用する、一意の Amazon S3 プレフィックスとして作成されます。WorkSpaces Pools によって Amazon S3 にホームフォルダが作成されると、そのフォルダ内のアクセスされたコンテンツは S3 バケットから WorkSpaces にコピーされます。これにより、ユーザーはストリーミングセッション中に、WorkSpace Pool の WorkSpace からホームフォルダのコンテンツにすばやくアクセスすることができます。S3 バケット内のユーザーのホームフォルダコンテンツに加えられた変更と、WorkSpace Pool の WorkSpace 上のホームフォルダコンテンツにユーザーが加えた変更は、Amazon S3 と WorkSpaces Pools の間で次のように同期されます。

1. ユーザーの WorkSpaces Pools ストリーミングセッションの開始時に、WorkSpaces Pools は、使用している Amazon Web Services アカウントとリージョンの Amazon S3 バケットに保存されているそのユーザーのホームフォルダファイルをカタログ化します。
2. ユーザーのホームフォルダコンテンツは、ストリーミング元の WorkSpaces Pools の WorkSpace にも保存されます。ユーザーが WorkSpace のホームフォルダにアクセスすると、カタログ化されたファイルの一覧が表示されます。

3. WorkSpaces Pools は、ユーザーがストリーミングアプリケーションを使用してストリーミングセッション中にファイルを開いた後にのみ、S3 バケットから WorkSpace にファイルをダウンロードします。
4. WorkSpaces Pools によってファイルが WorkSpace にダウンロードされたら、ファイルがアクセスされた後に同期が行われます
5. ユーザーがストリーミングセッション中にファイルを変更した場合、WorkSpaces Pools は定期的に、またはストリーミングセッションの最後に、新しいバージョンのファイルを WorkSpace から S3 バケットにアップロードします。ただし、ストリーミングセッション中にファイルは S3 バケットから再度ダウンロードされません。

以下のセクションでは、Amazon S3 でユーザーのホームフォルダファイルを追加し、置き換え、削除するときの同期動作について説明します。

目次



### Amazon S3 ユーザーのホームフォルダに追加したファイルの同期

S3 バケット内のユーザーのホームフォルダに新しいファイルを追加すると、WorkSpaces Pools はファイルをカタログ化して、数分以内にユーザーのホームフォルダ内にあるファイルの一覧に表示します。ただし、ストリーミングセッション中にユーザーがアプリケーションでファイルを開くまで、ファイルは S3 バケットから WorkSpace にダウンロードされません。

### Amazon S3 ユーザーのホームフォルダで置き換えたファイルの同期

ユーザーがストリーミングセッション中に WorkSpaces Pools の WorkSpace のホームフォルダにあるファイルを開き、そのユーザーのアクティブなストリーミングセッション中に S3 バケットのホームフォルダにある同じファイルが新しいバージョンに置き換えられた場合、新しいバージョンのファイルは WorkSpace にすぐにはダウンロードされません。新しいバージョンは、ユーザーが新しいストリーミングセッションを開始してファイルを再度開いた後にのみ、S3 バケットから WorkSpace にダウンロードされます。

### Amazon S3 ユーザーのホームフォルダから削除したファイルの同期

ユーザーがストリーミングセッション中に WorkSpaces Pools の WorkSpace のホームフォルダにあるファイルを開き、そのユーザーのアクティブなストリーミングセッション中に S3 バケットのホームフォルダから同じファイルが削除されると、そのファイルはユーザーが次のいずれかの操作を行った後に WorkSpace から削除されます。

- ホームフォルダを再度開く
- ホームフォルダを更新する

### ホームフォルダの形式

ユーザーのフォルダの階層は、次のセクションで説明するように、ユーザーがストリーミングセッションを起動する方法によって異なります。

#### SAML 2.0

SAML フェデレーションを使用して作成されたセッションでは、ユーザーフォルダ構造は次のようになります。

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

この場合、*user-id-SHA-256-hash* は、SAML フェデレーションリクエストに渡された NameID SAML 属性値から生成された、小文字の SHA-256 ハッシュ 16 進文字列を使用して作成されたフォルダ名です。2 つの異なるドメインに属する同じ名前のユーザーを区別するには、NameID 形式で domainname\username を含む SAML リクエストを送信します。詳細については、「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」を参照してください。

次の例のフォルダ構造は、米国西部 (オレゴン) リージョン の NameID SAMPLEDOMAIN\testuser、アカウント ID 123456789012 と SAML フェデレーションを使用したセッションアクセスに適用されます。

```
wspool-home-folder-us-west-2-123456789012/user/
federated/8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901
```

NameID 文字列の一部またはすべてが大文字の場合 (例ではドメイン名 *SAMPLEDOMAIN*)、WorkSpaces Pools では、文字列を大文字化したものに基づいて ハッシュ値が生成されます。この例では、SAMPLEDOMAIN\testuser のハッシュ値は

8DD9A642F511609454D344D53CB861A71190E44FED2B8AF9FDE0C507012A9901 です。そのユーザーのフォルダで、この値は、8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901 のように小文字で表示されます。

ウェブサイトを使用するか、オンラインで入手できるオープンソースコーディングライブラリを使用して、NameID の SHA-256 ハッシュ値を生成してユーザーのフォルダを識別できます。

その他のリソース

Amazon S3 バケットの管理とベストプラクティスの詳細については、Amazon Simple Storage Service ユーザーガイドにある次のトピックを参照してください。

- Amazon S3 ポリシーにより、ユーザーにユーザーデータへのオフラインアクセスを提供できます。詳細については、IAM ユーザーガイドの Amazon S3: Allows IAM Users Access to Their S3 Home Directory, Programmatically and In the Console を参照してください。
- WorkSpaces Pools によって使用される Amazon S3 バケットに保存されたコンテンツに対して、ファイルのバージョニングを有効にできます。詳細については、「バージョニングの使用」を参照してください。

# WorkSpaces Pools ユーザーのアプリケーション設定の永続化を有効にする

WorkSpaces Pools では、Windows ベースのディレクトリの永続的なアプリケーション設定をサポートしています。つまり、ユーザーのアプリケーションのカスタマイズや Windows 設定は各ストリーミングセッション後に自動的に保存され、次のセッションで適用されます。ユーザーが設定できる永続的なアプリケーション設定の例としては、ブラウザのお気に入り、設定、ウェブページのセッション、アプリケーション接続プロファイル、プラグイン、UI のカスタマイズなどが挙げられます。これらの設定は、アプリケーション設定の永続化が有効になっている AWS リージョン内のアカウントの Amazon Simple Storage Service (Amazon S3) バケットに保存されます。設定は、各 WorkSpaces Pools ストリーミングセッションで使用できます。

> **Note**
>
> S3 バケットに保存されているデータには、標準 Amazon S3 料金が適用される場合があります。詳細については、Amazon S3 の料金 を参照してください。

内容



# アプリケーション設定の永続化の仕組み

永続的なアプリケーション設定は Virtual Hard Disk (VHD) ファイルに保存されます。このファイルは、アプリケーション設定の永続化が有効になっているディレクトリから、ユーザーが初めてアプリケーションをストリーミングしたときに作成されます。ディレクトリに関連付けられている WorkSpaces Pools がデフォルトのアプリケーションおよび Windows 設定が含まれているイメージに基づいている場合、このデフォルト設定がユーザーの最初のストリーミングセッションで使用されます。

ストリーミングセッションが終了すると、VHD はアンマウントされ、アカウント内の Amazon S3 バケットにアップロードされます。バケットは、 AWS リージョンのディレクトリで永続的なアプリケーション設定を初めて有効にしたときに作成されます。バケットは、 AWS アカウントと リージョンに固有です。VHD は、伝送時には Amazon S3 SSL エンドポイントを使用して暗号化され、保管時には AWS マネージド CMK を使用して暗号化されます。

VHD は、`C:\Users\%username%` と `D:\%username%` の両方で WorkSpace にマウントされます。WorkSpace が Active Directory ドメインに参加していない場合、Windows ユーザー名は PhotonUser になります。WorkSpace が Active Directory ドメインに参加している場合、Windows ユーザー名はログインユーザーの名前になります。

アプリケーション設定の永続性は複数のオペレーティングシステムのバージョン間では機能しません。例えば、Windows Server 2019 のイメージを使用する WorkSpaces Pools でアプリケーション設定の永続性を有効にしている場合、別のオペレーティングシステム (Windows Server 2022 など) を実行するイメージを使用するように WorkSpaces Pools を更新すると、以前のストリーミングセッションの設定はそのディレクトリのユーザーには保存されません。代わりに、新しいイメージを使用するように WorkSpaces Pools を更新した後、ユーザーが WorkSpace からストリーミングセッションを起動するときに、新しい Windows ユーザープロファイルが作成されます。ただし、イメージで同じオペレーティングシステムに更新を適用すると、以前のストリーミングセッションからのユーザーのカスタマイズと設定が保存されます。同じオペレーティングシステムへの更新がイメージに適用された場合は、ユーザーが WorkSpace からストリーミングセッションを起動するときに、同じ Windows ユーザープロファイルが使用されます。

> **Important**
>
> WorkSpaces Pools は、WorkSpace が Microsoft Active Directory ドメインに参加している場合にのみ、Microsoft Data Protection API に依存するアプリケーションをサポートします。WorkSpace が Active Directory ドメインに参加していない場合、Windows ユーザーの PhotonUser は WorkSpace ごとに異なります。DPAPI セキュリティモデルの機能上の理由から、このシナリオで DPAPI を使用するアプリケーションではユーザーのパスワードは保持されません。 WorkSpaces が Active Directory ドメインに参加していて、そのユーザーがドメインユーザーである場合、Windows ユーザー名はログインしているユーザーの名前となり、DPAPI を使用するアプリケーションではユーザーのパスワードが保持されます。

WorkSpaces Pools では、次のフォルダを除いて、このパスにあるすべてのファイルとフォルダが自動的に保存されます。

- 問い合わせ
- Desktop
- ドキュメント
- ダウンロード
- リンク
- 画像
- Saved Games
- 検索
- 動画

これらのフォルダ外で作成されたファイルとフォルダは、VHD 内に保存され、Amazon S3 と同期されます。プールのデフォルトの VHD 最大サイズは 5 GB です。保存された VHD のサイズは、それに含まれるファイルとフォルダの合計サイズです。WorkSpaces Pools では、ユーザーの `HKEY_CURRENT_USER` レジストリハイブが自動的に保存されます。新規ユーザー (Amazon S3 にプロファイルが存在しないユーザー) の場合、WorkSpaces Pools はデフォルトのプロファイルを使用して初期プロファイルを作成します。このプロファイルは、Image Builder の `C:\users\default` に作成されます。

> **Note**
>
> ストリーミングセッションが開始する前に、VHD 全体を WorkSpace にダウンロードする必要があります。このため、VHD に大量のデータが保持されていると、ストリーミングセッションの開始が遅れる場合があります。詳細については、「アプリケーション設定の永続化を有効にするためのベストプラクティス」を参照してください。

アプリケーション設定の永続化を有効にする場合、設定グループを指定する必要があります。設定グループは、このディレクトリからのストリーミングセッションで、保存されているどのアプリケーション設定を使用するかを決定します。WorkSpaces Pools は、 AWS アカウントの S3 バケット内に個別に保存される設定グループの新しい VHD ファイルを作成します。設定グループを複数のディレクトリ間で共有すると、同じアプリケーション設定が各ディレクトリで使用されます。ディレクトリが独自のアプリケーション設定を必要とする場合は、このディレクトリ限定の設定グループを指定します。

## アプリケーション設定の永続化を有効にする

内容



### アプリケーション設定の永続化を有効にするための前提条件

アプリケーション設定の永続化を有効にするには、まず、以下のことを行う必要があります。

- 2017 年 12 月 7 日以降 AWS に によって公開されたベースイメージから作成されたイメージを使用します。
- インターネットアクセスまたは Amazon S3 の VPC エンドポイントを設定して、Virtual Private Cloud (VPC) から Amazon S3 へのネットワーク接続を有効にします。詳細については、WorkSpaces Pools のネットワークとアクセス の「ホームフォルダと VPC エンドポイント」セクションを参照してください。

## アプリケーション設定の永続化を有効にするためのベストプラクティス

WorkSpaces へのインターネットアクセスを提供せずに、アプリケーション設定の永続化を有効にするには、VPC エンドポイントを使用します。このエンドポイントは、WorkSpaces Pools 内の WorkSpaces が接続する VPC 内に存在する必要があります。WorkSpaces Pools からエンドポイントへのアクセスを有効にするには、カスタムポリシーをアタッチする必要があります。カスタムポリシーを作成する方法については、WorkSpaces Pools のネットワークとアクセス の「ホームフォルダと VPC エンドポイント」を参照してください。プライベート Amazon S3 エンドポイントの詳細については、Amazon VPC ユーザーガイドの VPC Endpoints および Endpoints for Amazon S3 を参照してください。

## アプリケーション設定の永続化を有効にする方法

ディレクトリの作成中または作成後に、WorkSpaces コンソールを使用してアプリケーション設定の永続化を有効または無効にできます。 AWS リージョンごとに、永続的なアプリケーション設定がアカウントの S3 バケットに保存されます。

AWS リージョン内のディレクトリに対してアプリケーション設定の永続化を初めて有効にすると、WorkSpaces Pools は同じリージョンの AWS アカウントに S3 バケットを作成します。同じバケットに、その AWS リージョン内のすべてのユーザーとすべてのディレクトリのアプリケーション設定 VHD ファイルを保存します。詳細については、ユーザーのアプリケーション設定の VHD を管理する の Amazon S3 バケットストレージ を参照してください。

ディレクトリの作成時にアプリケーション設定の永続化を有効にするには

- 「SAML 2.0 を設定して WorkSpaces Pools ディレクトリを作成する」の手順に従い、[Enable Application Settings Persistence (アプリケーション設定の永続化を有効にする)] が選択されていることを確認します。

既存のディレクトリでアプリケーション設定の永続化を有効にするには

1. https://console.aws.amazon.com/workspaces/v2/home「https://www.com で WorkSpaces コンソールを開きます。
2. 左のナビゲーションペインで、[プール] を選択し、アプリケーション設定の永続化を有効にするプールを選択します。
3. ページの [設定] セクションで、[編集] を選択します。
4. ページの [アプリケーションの永続性] セクションで、[アプリケーション設定の永続化を有効化] を選択します。

5. [Save changes] (変更の保存) をクリックします。

これにより、新しいストリーミングセッションでアプリケーション設定の永続化が有効になります。

# ユーザーのアプリケーション設定の VHD を管理する

内容



## Amazon S3 バケットのストレージ

アプリケーション設定の永続化を有効にすると、ユーザーのアプリケーションのカスタマイズと Windows 設定は、 AWS アカウントで作成された Amazon S3 バケットに保存されている Virtual Hard Disk (VHD) ファイルに自動的に保存されます。 AWS リージョンごとに、WorkSpaces Pools によってアカウントおよびリージョン固有のバケットがアカウント内に作成されます。ユーザーが行ったすべてのアプリケーション設定が該当リージョンのバケットに保存されます。

これらの S3 バケットを管理するための設定タスクは一切不要です。WorkSpaces Pools サービスによって完全に管理されます。各バケットに保存された VHD ファイルは、伝送時には Amazon S3 の SSL エンドポイントを使用して暗号化され、保管時には AWS マネージド CMK を使用して暗号化されます。バケットは、以下にあるような特定の形式で命名されます。

```
wspool-app-settings-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

***region-code***

これは、アプリケーション設定の永続化を使用してディレクトリが作成される AWS リージョンコードです。

***account-id-without-hyphens***

AWS アカウント ID。ランダムな識別子により、該当リージョンで他のバケットとの競合が発生することはありません。バケット名の最初の部分 `wspool-app-settings` は、複数のアカウントやリージョンにまたがる場合でも変更されません。

例えば、アカウント番号 123456789012 で、米国西部 (オレゴン) リージョン (us-west-2) のディレクトリに対してアプリケーション設定の永続化を有効にすると、WorkSpaces Pools は、該当リージョンのアカウント内に次に示す名前で Amazon S3 バケットを作成します。適切なアクセス許可を持つ管理者のみが、このバケットを削除できます。

```
wspool-app-settings-us-west-2-1234567890123-abcdefg
```

アプリケーション設定の永続化を無効にしても、S3 バケットに保存された VHD は削除されません。設定 VHD を完全に削除するには、Amazon S3 コンソールまたは API を使用して、ユーザーまたは適切なアクセス許可を持つ別の管理者が削除する必要があります。WorkSpaces Pools には、バケットの誤った削除を防止するバケットポリシーが追加されます。

アプリケーション設定の永続化を有効にすると、設定 VHD を保存するために設定グループごとに固有のフォルダが作成されます。S3 バケットのフォルダの階層は、次のセクションで説明するように、ユーザーがストリーミングセッションを起動する方法によって異なります。

アカウントの S3 バケットで設定 VHD が保存されているフォルダへのパスは、次の構造になります。

```
bucket-name/Windows/prefix/settings-group/access-mode/user-id-SHA-256-hash
```

***bucket-name***

ユーザーのアプリケーション設定が保存されている S3 バケットの名前。名前の形式については、このセクションで先ほど説明しました。

***prefix***

Windows バージョン固有のプレフィックス。例えば、v4 for Windows Server 2012 R2 です。

***settings-group***

設定グループの値。この値は、同じアプリケーション設定を共有する 1 つ以上のディレクトリに適用されます。

***access-mode***

ユーザーの ID メソッド: WorkSpaces Pools API または CLI の場合は `custom`、SAML の場合は `federated`、ユーザープールのユーザーの場合は `userpool`。

***user-id-SHA-256-hash***

ユーザー固有のフォルダ名。この名前は、ユーザー ID から生成された小文字の SHA-256 ハッシュ 16 進数文字列を使用して作成されます。

次のフォルダ構造の例は、ユーザー ID が 、ID が testuser@mydomain.com、米国西部 (オレゴン) リージョン (us-west-2) AWS アカウント 123456789012の設定グループtest-stackで API または CLI を使用してアクセスされるストリーミングセッションに適用されます。

```
wspool-app-settings-us-west-2-1234567890123-abcdefg/Windows/v4/test-stack/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13
```

ユーザーのフォルダを確認するには、ウェブサイトを使用するか、オンラインで入手できるオープンソースコーディングライブラリを使用して、ユーザー ID の小文字の SHA-256 ハッシュ値を生成します。

## ユーザーのアプリケーション設定をリセットする

ユーザーのアプリケーション設定をリセットするには、 AWS アカウントの S3 バケットから VHD および関連するメタデータファイルを検索して削除する必要があります。ユーザーのアクティブなストリーミングセッションが進行中は、この操作を実行しないでください。ユーザーの VHD とメタデータファイルを削除すると、次回、ユーザーがアプリケーション設定の永続化が有効になっているストリーミングインスタンスからセッションを起動したときに、WorkSpaces Pools によって当該ユーザーの新しい設定 VHD が作成されます。

ユーザーのアプリケーション設定をリセットするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Bucket name (バケット名)] リストで、リセットするアプリケーション設定 VHD が含まれている S3 バケットを選択します。
3. VHD が含まれているフォルダを見つけます。S3 バケットのフォルダ構造内を移動する詳しい方法については、このトピックの前半にある「Amazon S3 バケットのストレージ」を参照してください。
4. [名前] のリストで、VHD と REG の横にあるチェックボックスをオンにし、[詳細]、[削除] の順に選択します。
5. [Delete objects (オブジェクトの削除)] ダイアログボックスで、VHD と REG が表示されていることを確認し、[削除] を選択します。

該当する設定グループに基づいてアプリケーション設定の永続化が有効になっているプールから次回ユーザーがストリーミングすると、新しいアプリケーション設定 VHD が作成されます。この VHD は、セッションの最後に S3 バケットに保存されます。

## Amazon S3 オブジェクトのバージョニングを有効にしてユーザーのアプリケーション設定を元に戻す

Amazon S3 オブジェクトのバージョニングとライフサイクルポリシーを使用して、ユーザーによるアプリケーション設定の変更を管理できます。Amazon S3 オブジェクトのバージョニングを使用すると、あらゆるバージョンの設定 VHD を保持、取得、復元できます。これにより、意図しないユーザーのアクションとアプリケーションの障害の両方から復旧できます。バージョニングを有効にすると、各ストリーミングセッション後に、新しいバージョンのアプリケーション設定 VHD が Amazon S3 と同期されます。新しいバージョンは以前のバージョンを上書きしないため、ユーザーの設定に問題が生じた場合は、以前のバージョンの VHD に戻すことができます。

> **Note**
>
> 各バージョンのアプリケーション設定 VHD は、別個のオブジェクトとして Amazon S3 に保存され、相応に課金されます。

S3 バケットでのオブジェクトのバージョニングは、デフォルトでは有効にならないため、明示的に有効にする必要があります。

アプリケーション設定 VHD でオブジェクトのバージョニングを有効にするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Bucket name (バケット名)] リストで、オブジェクトのバージョニングを有効にするアプリケーション設定 VHD が含まれている S3 バケットを選択します。
3. [Properties] (プロパティ) を選択します。
4. [Versioning (バージョニング)]、[Enable versioning (バージョニングの有効化)]、[Save (保存)] の順に選択します。

古いバージョンのアプリケーション設定 VHD を失効させるには、Amazon S3 ライフサイクルポリシーを使用できます。詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 バケットのライフサイクルポリシーを作成する方法を教えてください」を参照してください。

### ユーザーのアプリケーション設定 VHD を前のバージョンに戻すには

ユーザーのアプリケーション設定 VHD を前のバージョンに戻すには、該当する S3 バケットから以降のバージョンの VHD を削除します。ユーザーがアクティブなストリーミングセッションを進行中は、この操作を実行しないでください。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Bucket name (バケット名)] リストで、前のバージョンに戻すユーザーのアプリケーション設定 VHD が含まれている S3 バケットを選択します。
3. VHD が含まれているフォルダを見つけて選択します。S3 バケットのフォルダ構造内を移動する詳しい方法については、このトピックの前半にある「Amazon S3 バケットのストレージ」を参照してください。

   フォルダを選択すると、設定 VHD および関連するメタデータファイルが表示されます。
4. VHD とメタデータファイルのバージョンを一覧表示するには、[Show (表示)] を選択します。
5. 以前に戻す VHD のバージョンを見つけます。
6. [Name (名前)] リストで、以降のバージョンの VHD および関連するメタデータファイルの横にあるチェックボックスをオンにし、[More (詳細)]、[Delete (削除)] の順に選択します。
7. 前のバージョンに戻すアプリケーション設定 VHD および関連するメタデータファイルが以降のバージョンであることを確認します。

該当する設定グループに基づいてアプリケーション設定の永続化が有効になっているプールから次回ユーザーがストリーミングを行うと、前のバージョンに戻したユーザー設定が表示されます。

## アプリケーション設定 VHD のサイズを拡大する

プールのデフォルトの VHD 最大サイズは 5 GB です。ユーザーがアプリケーション設定の領域を増やす必要がある場合は、該当するアプリケーション設定 VHD を Windows コンピュータにダウンロードして拡大できます。次に、S3 バケット内の現在の VHD を、拡大したものに置き換えます。ユーザーがアクティブなストリーミングセッションを進行中は、この操作を実行しないでください。

> **Note**
>
> Virtual Hard Disk (VHD) の物理サイズを減らすには、セッションを終了する前にごみ箱を空にします。これにより、アップロードとダウンロードの時間も短縮され、全体的なユーザーエクスペリエンスが向上します。

### アプリケーション設定 VHD のサイズを拡大するには

> **Note**
>
> ユーザーがアプリケーションのストリーミングを行う前に、VHD 全体をダウンロードする必要があります。アプリケーション設定 VHD のサイズを拡大すると、ユーザーがアプリケーションのストリーミングセッションを開始するまでの所要時間が長くなる場合があります。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Bucket name (バケット名)] リストで、拡大するアプリケーション設定 VHD が含まれている S3 バケットを選択します。
3. VHD が含まれているフォルダを見つけて選択します。S3 バケットのフォルダ構造内を移動する詳しい方法については、このトピックの前半にある「Amazon S3 バケットのストレージ」を参照してください。

   フォルダを選択すると、設定 VHD および関連するメタデータファイルが表示されます。
4. `Profile.vhdx` ファイルを Windows コンピュータのディレクトリにダウンロードします。ダウンロードが完了しても、ブラウザを閉じないでください。拡大した VHD をアップロードするためにブラウザを後で再び使用します。
5. Diskpart を使用して VHD のサイズを 7 GB に拡大するには、管理者としてコマンドプロンプトを開き、以下のコマンドを入力します。

   ```
   diskpart
   ```

   ```
   select vdisk file="C:\path\to\application\settings\profile.vhdx"
   ```

   ```
   expand vdisk maximum=7000
   ```
6. 次に、以下の Diskpart コマンドを入力して、VHD を見つけてアタッチし、ボリュームを一覧表示します。

   ```
   elect vdisk file="C:\path\to\application\settings\profile.vhdx"
   ```

   ```
   attach vdisk
   ```

```
list volume
```

出力で、ラベル「AwsEucUsers」が付いているボリュームの番号を書き留めます。次のステップで、このボリュームを選択して拡大します。

7. 次のコマンドを入力します。*<volume-number>* はボリューム一覧の出力の数値です。

```
select volume <volume-number>
```

8. 次のコマンドを入力します。

```
extend
```

9. 以下のコマンドを入力して、VHD のパーティションのサイズが正常に拡大したこと (この例では 7 GB) を確認します。

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
list volume
```

10. 次のコマンドを入力して VHD をデタッチし、アップロードできるようにします。

```
detach vdisk
```

11. Amazon S3 コンソールのブラウザに戻り、[Upload (アップロード)]、[Add files (ファイルの追加)] の順に選択し、拡大した VHD を選択します。
12. [アップロード] を選択します。

VHD をアップロードすると、該当する設定グループに基づいてアプリケーション設定の永続化が有効になっているプールから次回ユーザーがストリーミングを行ったときに、拡大したアプリケーション設定 VHD を使用できます。

# WorkSpaces Pools のトラブルシューティング通知コード

WorkSpaces で Active Directory を設定および使用する際に発生する可能性があるドメイン参加の問題の通知コードと解決手順を以下に示します。

DOMAIN_JOIN_ERROR_ACCESS_DENIED

メッセージ: アクセスが拒否されました。

解決策: ディレクトリで指定されたサービスアカウントに、コンピュータオブジェクトを作成するアクセス許可、または既存のものを再利用するアクセス許可がありません。アクセス許可を検証して WorkSpaces プールを起動します。

DOMAIN_JOIN_ERROR_LOGON_FAILURE

メッセージ: ユーザー名またはパスワードに誤りがあります。

解決策: ディレクトリで指定されたサービスアカウントのユーザー名またはパスワードが無効です。ディレクトリに設定された AWS Secrets Manager シークレットの認証情報を更新して、WorkSpaces プールを起動します。

DOMAIN_JOIN_NERR_PASSWORD_EXPIRED

メッセージ: このユーザーのパスワードの有効期限が切れています。

解決策: AWS Secrets Manager シークレット内のサービスアカウントのパスワードの有効期限が切れています。まず、WorkSpaces プールを停止し、WorkSpaces ディレクトリで指定されたシークレットのパスワードを変更してから、WorkSpaces プールを起動します。

DOMAIN_JOIN_ERROR_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED

メッセージ: コンピュータをドメインに結合できませんでした。このドメインで作成が許可されているコンピュータアカウントの最大数を超過しています。システム管理者に問い合わせて、この制限をリセットまたは引き上げます。

解決策: ディレクトリで指定されたサービスアカウントに、コンピュータオブジェクトを作成するアクセス許可、または既存のものを再利用するアクセス許可がありません。アクセス許可を検証して WorkSpaces プールを起動します。

DOMAIN_JOIN_ERROR_INVALID_PARAMETER

メッセージ: パラメータが正しくありません。このエラーは、`LpName` パラメータが NULL であるか、`NameType` パラメータが `NetSetupUnknown` または不明な名前タイプとして指定されている場合に返されます。

解決策: このエラーは、OU の識別名が正しくない場合に発生します。OU を検証して、もう一度試してください。このエラーが引き続き発生する場合は、 にお問い合わせください AWS サポート。詳細については、AWS サポート センターを参照してください。

DOMAIN_JOIN_ERROR_MORE_DATA

メッセージ: その他のデータを使用できます。

解決策: このエラーは、OU の識別名が正しくない場合に発生します。OU を検証して、もう一度試してください。このエラーが引き続き発生する場合は、 にお問い合わせください AWS サポート。詳細については、AWS サポート センターを参照してください。

DOMAIN_JOIN_ERROR_NO_SUCH_DOMAIN

メッセージ: 指定されたドメイン名が存在しないか、接続できませんでした。

解決策: ストリーミングインスタンスが Active Directory ドメインに接続できませんでした。ネットワーク接続を確保するには、VPC、サブネット、およびセキュリティグループ設定を確認します。

DOMAIN_JOIN_NERR_WORKSTATION_NOT_STARTED

メッセージ: Workstation サービスが開始されていません。

解決策: Workstation サービスの開始時にエラーが発生しました。イメージでサービスが有効になっていることを確認します。このエラーが引き続き発生する場合は、 にお問い合わせください AWS サポート。詳細については、AWS サポート センターを参照してください。

DOMAIN_JOIN_ERROR_NOT_SUPPORTED

メッセージ: リクエストはサポートされていません。このエラーは、リモートコンピュータが `lpServer` パラメータで指定されており、この呼び出しがリモートコンピュータでサポートされていない場合に返されます。

解決策: サポート AWS サポート が必要な場合は、 にお問い合わせください。詳細については、AWS サポート センターを参照してください。

DOMAIN_JOIN_ERROR_FILE_NOT_FOUND

メッセージ: 指定されたファイルがシステムで見つかりません。

解決策: このエラーは、無効な組織単位 (OU) の識別子名が指定されている場合に発生します。識別子名の先頭には、**OU=** を付ける必要があります。OU 識別子名を検証し、再試行してください。

DOMAIN_JOIN_INTERNAL_SERVICE_ERROR

メッセージ: アカウントは既に存在しています。

Resolution (解決策): このエラーは、次の状況で発生する可能性があります。

- 問題がアクセス許可に関連していない場合は、Netdom ログでエラーがないか確認し、正しい OU を指定したことを確認してください。
- ディレクトリで指定されたサービスアカウントに、コンピュータオブジェクトを作成するアクセス許可、または既存のものを再利用するアクセス許可がありません。このような場合は、アクセス許可を検証して WorkSpaces プールを起動します。
- WorkSpaces で作成したコンピュータオブジェクトは、作成後に作成先の OU から移動されます。この場合、最初の WorkSpaces プールは正常に作成されますが、コンピュータオブジェクトを使用する新しい WorkSpaces プールは失敗します。Active Directory が指定先の OU でコンピュータオブジェクトを検索し、ドメイン内の別の場所で同じ名前のオブジェクトを検出すると、ドメイン参加は失敗します。
- WorkSpaces ディレクトリで指定されている OU の名前には、ディレクトリのカンマの前または後にスペースが含まれています。この場合、WorkSpaces プールが Active Directory ドメインへの再参加を試みると、WorkSpaces はコンピュータオブジェクトを正しく循環できず、ドメインに再参加できません。WorkSpaces プールでこの問題を解決するには、次の手順を実行します。

  1. WorkSpaces プールを停止します。
  2. WorkSpaces プールの Active Directory ドメイン設定を編集して、WorkSpaces プールが参加しているディレクトリおよびディレクトリ OU を削除します。
  3. WorkSpaces ディレクトリを更新して、スペースを含まない OU を指定します。
  4. WorkSpaces プールの Active Directory ドメイン設定を編集して、更新されたディレクトリ OU でディレクトリを指定します。

  WorkSpaces プールでこの問題を解決するには、次の手順を実行します。

  1. WorkSpaces プールを削除します。
  2. WorkSpaces ディレクトリを更新して、スペースを含まない OU を指定します。
  3. 新しい WorkSpaces プールを作成し、更新されたディレクトリ OU でディレクトリを指定します。

WORKSPACES_POOL_SESSION_RESERVATION_ERROR

メッセージ: 現在、WorkSpaces Pools に関連付けられたサブネットのアベイラビリティーゾーン [us-west-1] でリクエストされたセッションに十分なキャパシティーがありません。追加のキャパシティーをプロビジョニングする作業を進めます。それまでの間、次のいずれかの AZ [us-west-2、us-west-3] を使用して、サブネットを変更するか別のサブネットを関連付けてください。

解決方法: EC2 で十分なキャパシティーが確保されるか、ディレクトリ上の他の AZ のサブネットに更新されるまで待ちます。

INSUFFICIENT_CAPACITY_ERROR_WORKSPACES_POOL_AZ

メッセージ: 現在、アベイラビリティーゾーン (AZ) [<影響を受けている AZ>] でリクエストされたセッションに十分なキャパシティーがありません。追加のキャパシティーをプロビジョニングする作業を進めます。それまでの間、他の AZ を使用してサブネットを変更するか別のサブネットを WorkSpaces Pools に関連付けてください。

解決方法: Amazon EC2 で十分なキャパシティーが確保されるか、ディレクトリ上の他の AZ のサブネットに更新されるまで待ちます。

INVALID_CUSTOMER_SUBNET_CIDR_BLOCK

メッセージ: サブネットに、使用できない CIDR 範囲が使用されています。現在の /18 の範囲外にサブネットを更新してください。

解決方法: EC2 で十分なキャパシティーが確保されるか、ディレクトリ上の他の AZ のサブネットに更新されるまで待ちます。

# Amazon WorkSpaces に関するセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とお客様の間で共有される責任です。責任共有モデルではこれをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 は、お客様が安全に使用できるサービスも提供します。AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。WorkSpaces に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、WorkSpaces 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。

内容

# Amazon WorkSpaces におけるデータ保護

Amazon WorkSpaces でのデータ保護には、 AWS 責任共有モデルが適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、AWS CLIまたは SDK を使用して WorkSpaces 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 タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

WorkSpaces および FIPS エンドポイント暗号化の詳細については、「 WorkSpaces Personal で FedRAMP 認証または DoD SRG コンプライアンスを設定する 」を参照してください。

## 保管中の暗号化

AWS KMS キーを使用して WorkSpaces のストレージボリュームを暗号化できます AWS Key Management Service。詳細については、「WorkSpaces Personal の暗号化された WorkSpaces」を参照してください。

暗号化されたボリュームで WorkSpaces を作成すると、WorkSpaces は Amazon Elastic Block Store (Amazon EBS) を使用してこ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」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、PCoIP セキュリティ設定の構成Windows WorkSpaces のグループポリシー設定を使用するか、PCoIP セキュリティ設定()`pcoip-agent.conf`ファイルを Amazon Linux WorkSpaces 用にダウンロードします。

Amazon WorkSpaces のグループポリシー管理の詳細については、PCoIP セキュリティ設定を構成するがWorkSpaces Personal で Windows WorkSpaces を管理する。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 WorkSpaces で PCoIP エージェントの動作を制御するおよび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。

DCV では、転送中のストリーミングおよび制御データは、UDP トラフィックには TLS 1.3 暗号化を、TCP トラフィックには 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。

> **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。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center :

  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「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって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します。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) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当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 ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) 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。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

IAM の追加リソースは次のとおりです。

- 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。
- 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の詳細については、「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」を参照してください。
- 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。

内容



## 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。

例 1: WorkSpaces Personal および WorkSpaces Pools タスクを実行するためのアクセス許可を付与する

次のポリシーステートメントは、WorkSpaces Personal と WorkSpaces Pools のタスクを実行するアクセス許可を IAM ユーザーに付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
```

```
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "secretsmanager:ListSecrets",
                "tag:GetResources",
                "sso-directory:SearchUsers",
                "sso:CreateApplication",
                "sso:DeleteApplication",
                "sso:DescribeApplication",
                "sso:DescribeInstance",
                "sso:GetApplicationGrant",
                "sso:ListInstances",
                "sso:PutApplicationAssignment",
                "sso:PutApplicationAssignmentConfiguration",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

例 2: WorkSpaces Personal タスクを実行するためのアクセス許可を付与する

次のポリシーステートメントは、すべての WorkSpaces Personal タスクを実行するアクセス許可を IAM ユーザーに付与します。

Amazon WorkSpaces は API `Action`およびコマンドラインツールを使用する際に および `Resource`要素を完全にサポートしていますが、 から Amazon WorkSpaces を使用するには AWS Management Console、IAM ユーザーに以下のアクションとリソースに対するアクセス許可が必要です。

- 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",
        "secretsmanager:ListSecrets",
        "sso-directory:SearchUsers",
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationGrant",
        "sso:ListInstances",
        "sso:PutApplicationAssignment",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

例 3: WorkSpaces Pools タスクを実行するためのアクセス許可を付与する

次のポリシーステートメントは、すべての WorkSpaces Pools タスクを実行するアクセス許可を IAM ユーザーに付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:CreateSecurityGroup",
```

```
                "ec2:CreateTags",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "secretsmanager:ListSecrets",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-role/workspaces.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_WorkSpacesPool",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "workspaces.application-
autoscaling.amazonaws.com"
                }
            }
        }
    ]
}
```

例 4: 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": [
                "ds:*",
                "workspaces:*",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:ModifyImageAttribute",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "kms:ListAliases",
```

```
                "kms:ListKeys"
            ],
            "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。

WorkSpace プールの ARN

WorkSpace プールの ARN には、次の例に示す構文があります。

```
arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier
```

region

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 ) 。

workspacespool_identifier

WorkSpace プールの 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:workspacespool/workspacespool_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、クイックセットアップによって、または を使用して WorkSpace を起動する場合に作成され AWS Management Console、ユーザーに代わって特定の AWS リソースにアクセスするアクセス許可を Amazon WorkSpaces に付与します。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. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
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] (次のステップ: 許可) を選択します。
8. アクセス許可ポリシーのアタッチページで、 AWS 管理ポリシー AmazonWorkSpacesServiceAccess、AmazonWorkSpacesSelfServiceAccess、および AmazonWorkSpacesPoolServiceAccess を選択します。これらのマネージドポリシーの詳細については、「AWS WorkSpaces の マネージドポリシー」を参照してください。
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、 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 AWS Management Console、ユーザーに代わって AWS Private CA リソースにアクセスするアクセス許可を Amazon WorkSpaces に付与します。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。

を使用して AmazonWorkSpacesPCAAccess サービスロールを作成するには AWS CLI

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、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
```

## AWS WorkSpaces の マネージドポリシー

AWS 管理ポリシーを使用すると、ユーザー、グループ、ロールにアクセス許可を追加する方が、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 管理ポリシーを使用して、すぐに開始できます。これらのポリシーは一般的なユースケースを対象としており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

AWS サービスは、 AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスは、新しい機能をサポートするために、 AWS 管理ポリシーに追加のアクセス許可を追加する場合があります。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。サービスは、新機能が起動されたとき、または新しいオペレーションが利用可能になったときに、 AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 ReadOnlyAccess AWS マネージドポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新しい機能を起動する場合、 AWS は新たなオペ

レーションとリソース用に、読み取り専用の許可を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドのジョブ機能のAWS 管理ポリシーを参照してください。

## AWS マネージドポリシー: 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 Personal および WorkSpaces Pools 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": [
        {
            "Sid": "AmazonWorkSpacesAdmin",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaceImage",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspacesPool",
                "workspaces:CreateStandbyWorkspaces",
                "workspaces:DeleteTags",
                "workspaces:DeregisterWorkspaceDirectory",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesPools",
                "workspaces:DescribeWorkspacesPoolSessions",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:ModifyStreamingProperties",
                "workspaces:ModifyWorkspaceCreationProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:RebootWorkspaces",
```

```
                "workspaces:RebuildWorkspaces",
                "workspaces:RegisterWorkspaceDirectory",
                "workspaces:RestoreWorkspace",
                "workspaces:StartWorkspaces",
                "workspaces:StartWorkspacesPool",
                "workspaces:StopWorkspaces",
                "workspaces:StopWorkspacesPool",
                "workspaces:TerminateWorkspaces",
                "workspaces:TerminateWorkspacesPool",
                "workspaces:TerminateWorkspacesPoolSession",
                "workspaces:UpdateWorkspacesPool"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS マネージドポリシー: AmazonWorkspacesPCAAccess

この管理ポリシーは、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の 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 マネージドポリシー: 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 マネージドポリシー: 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": "*"
        }
    ]
}
```

## AWS マネージドポリシー: AmazonWorkSpacesPoolServiceAccess

このポリシーは workspaces_DefaultRole で使用されます。WorkSpaces はこれを使用して、WorkSpaces Pools の顧客 AWS アカウントの必要なリソースにアクセスします。詳細については、「workspaces_DefaultRole ロールを作成する」を参照してください。以下のアクセス許可が提供されます。

- ec2 - WorkSpaces Pools に関連付けられた VPC、サブネット、アベイラビリティーゾーン、セキュリティグループ、ルートテーブルなどの Amazon EC2 リソースを管理するためのアクセスを許可します。
- s3 - ログ、アプリケーション設定、ホームフォルダ機能に必要な Amazon S3 バケットでアクションを実行するためのアクセスを許可します。

### Commercial AWS リージョン

次のポリシー JSON が商用に適用されます AWS リージョン。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

### AWS GovCloud (US) Regions

次のポリシー JSON は、商用の AWS GovCloud (US) Regionsに適用されます。

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

```
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
```

```
}
```

## AWS 管理ポリシーに対する WorkSpaces 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 “AmazonWorkSpacesPoolServiceAcces” - 新しいポリシーを追加しました | Amazon EC2 VPC や関連リソースを表示するためのアクセスを許可し、WorkSpaces Pools の Amazon S3 バケットを表示および管理するためのアクセスを許可する、新しいマネージドポリシーが WorkSpaces に追加されました。 | 2024 年 6 月 24 日 |
| the section called “AmazonWorkSpacesAdmin” – ポリシーを更新 | Amazon WorkSpacesAdmin マネージドポリシーに WorkSpaces Pools のリソース管理用のアクションがいくつか追加され、管理者がアクセスできるようになりました。 | 2024 年 6 月 24 日 |
| the section called “AmazonWorkSpacesAdmin” – ポリシーを更新 | 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 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 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 AWS のためのプライベート CA を管理するacm-pcaアクセス許可を付与する新しい管理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 |

# ストリーミングインスタンスでの WorkSpaces とスクリプトへのアクセス

WorkSpaces ストリーミングインスタンスで実行されるアプリケーションとスクリプトは、 AWS API リクエストに AWS 認証情報を含める必要があります。IAM ロールを作成して、これらの認証情報を管理できます。IAM ロールは、 AWS リソースへのアクセスに使用できる一連のアクセス許可を指定します。ただし、このロールは 1 人のユーザーに一意に関連付けられるわけではありません。代わりに、それを必要とするすべてのユーザーが引き受けることができます。

IAM ロールを WorkSpaces ストリーミングインスタンスに適用できます。ストリーミングインスタンスがロールに切り替える (引き受ける) と、ロールは一時的なセキュリティ認証情報を提供します。アプリケーションまたはスクリプトはこれらの認証情報を使用して、ストリーミングインスタンスで API アクションおよび管理タスクを実行します。WorkSpaces は、一時的な認証情報スイッチを管理します。

内容

- WorkSpaces ストリーミングインスタンスで IAM ロールを使用するためのベストプラクティス
- WorkSpaces ストリーミングインスタンスで使用するために既存の IAM ロールを設定する
- WorkSpaces ストリーミングインスタンスで使用する IAM ロールを作成する方法
- WorkSpaces ストリーミングインスタンスで IAM ロールを使用する方法

## WorkSpaces ストリーミングインスタンスで IAM ロールを使用するためのベストプラクティス

WorkSpaces ストリーミングインスタンスで IAM ロールを使用する場合は、以下のプラクティスに従うことをお勧めします。

- AWS API アクションとリソースに付与するアクセス許可を制限します。

  IAM ポリシーを作成し、WorkSpaces ストリーミングインスタンスに関連付けられた IAM ロールにアタッチするときは、最小特権の原則に従います。 AWS API アクションまたはリソースへのアクセスを必要とするアプリケーションまたはスクリプトを使用する場合は、必要な特定のアクションとリソースを決定します。次に、アプリケーションまたはスクリプトがこれらのアクションのみを実行できるようにするポリシーを作成します。詳細については、「IAM ユーザーガイド」の「Grant Least Privilege」(最小権限を付与する) を参照してください。
- WorkSpaces リソースごとに IAM ロールを作成します。

  WorkSpaces リソースごとに一意の IAM ロールを作成することは、最小特権の原則に従うプラクティスです。これにより、他のリソースに影響を与えることなく、リソースのアクセス許可を変更することもできます。
- 認証情報を使用できる場所を制限します。

  IAM ポリシーでは、IAM ロールを使用してリソースにアクセスするための条件を定義できます。たとえば、リクエスト元の IP アドレスの範囲を指定する条件を含めることができます。これにより、認証情報が環境外で使用されなくなります。詳細については、IAM ユーザーガイドの「追加セキュリティに対するポリシー条件を使用する」を参照してください。

## WorkSpaces ストリーミングインスタンスで使用するために既存の IAM ロールを設定する

このトピックでは、既存の IAM ロールを WorkSpaces で使用できるように設定する方法について説明します。

前提条件

WorkSpaces で使用する IAM ロールは、次の前提条件を満たしている必要があります。

- IAM ロールは、WorkSpace ストリーミングインスタンスと同じ Amazon Web Services アカウントに存在する必要があります。

- IAM ロールをサービスロールにすることはできません。
- IAM ロールにアタッチされた信頼関係ポリシーには、プリンシパルとして WorkSpaces サービスが含まれている必要があります。プリンシパルは、アクションを実行してリソースにアクセスできる AWS のエンティティです。ポリシーには `sts:AssumeRole` アクションも含める必要があります。このポリシー設定は、WorkSpaces を信頼されたエンティティとして定義します。

- IAM ロールを WorkSpaces に適用する場合、2019 年 9 月 3 日以降にリリースされたバージョンの WorkSpaces エージェントを WorkSpaces で実行する必要があります。IAM ロールを WorkSpaces に適用する場合、同じ日付以降にリリースされたバージョンのエージェントを用いるイメージを WorkSpaces で使用する必要があります。

WorkSpaces サービスプリンシパルが既存の IAM ロールを引き受けるようにするには

以下のステップを実行するには、IAM ロールを一覧表示および更新するために必要なアクセス許可を持つ IAM ユーザーとしてアカウントにサインインする必要があります。必要なアクセス許可がない場合は、お客様の Amazon Web Services アカウント管理者に対し、アカウントでこれらのステップを実行するか、必要なアクセス許可をお客様に付与するかのどちらかを依頼します。

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) を選択します。
3. アカウントのロールの一覧で、変更するロールの名前を選択します。
4. [Trust relationships] タブを選択し、続いて [Edit trust relationship] を選択します。
5. [Policy Document (ポリシードキュメント)]で、信頼関係ポリシーに `workspaces.amazonaws.com` サービスプリンシパルの `sts:AssumeRole` アクションが含まれていることを確認します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

6. 信頼ポリシーの編集を完了したら、[信頼ポリシーの更新] を選択して変更を保存します。
7. 選択した IAM ロールが WorkSpaces コンソールに表示されます。このロールは、ストリーミングインスタンスで API アクションおよび管理タスクを実行するアクセス許可をアプリケーションとスクリプトに付与します。

## WorkSpaces ストリーミングインスタンスで使用する IAM ロールを作成する方法

このトピックでは、WorkSpaces で使用する新しい IAM ロールを作成する方法について説明します。

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. 信頼できるエンティティの種類の選択 で、AWS サービス を選択します。
4. AWS サービスのリストから WorkSpaces を選択します。
5. 「ユースケースの選択」のWorkSpaces — WorkSpaces インスタンスがユーザーに代わって AWS サービスを呼び出すことを許可します」が既に選択されています。[Next: Permissions] (次へ: アクセス許可) を選択します。
6. 可能な場合は、アクセス許可ポリシーとして使用するポリシーを選択するか、[ポリシーの作成] を選択して新しいブラウザタブを開き、新しいポリシーをゼロから作成します。詳細については、IAM ユーザーガイドの「IAM ポリシーの作成 (コンソール)」のステップ 4 を参照してください。

   ポリシーを作成したら、そのタブを閉じて元のタブに戻ります。WorkSpaces に割り当てるアクセス許可ポリシーの横にあるチェックボックスをオンにします。
7. (オプション) アクセス許可の境界を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。詳細については、IAM ユーザーガイドの「IAM エンティティのアクセス許可境界」を参照してください。
8. [Next: Tags] (次へ: タグ) を選択します。オプションで、タグをキーと値のペアとしてアタッチできます。詳細については、IAM ユーザーガイドの「IAM リソースのタグ付け」を参照してください。
9. [次へ: レビュー] を選択します。

10. [Role name] (ロール名) に、Amazon Web Services アカウント内で一意のロール名を入力します。他の AWS リソースがロールを参照する可能性があるため、ロールの作成後にロールの名前を編集することはできません。
11. [ロールの説明] に、デフォルトのロールの説明をそのまま使用するか、新しいロールの説明を入力します。
12. ロールを確認したら、[ロールを作成] を選択します。

## WorkSpaces ストリーミングインスタンスで IAM ロールを使用する方法

IAM ロールを作成したら、WorkSpaces を起動するときにロールを WorkSpaces に適用できます。既存の WorkSpaces に IAM ロールを適用することもできます。

IAM ロールを WorkSpaces に適用すると、WorkSpaces は一時的な認証情報を取得し、インスタンスに workspaces_machine_role 認証情報プロファイルを作成します。一時的な認証情報は 1 時間有効で、新しい認証情報は 1 時間ごとに取得されます。以前の認証情報は失効しないため、有効である限り使用できます。認証情報プロファイルを使用して、選択した言語で コマンドラインインターフェイス (AWS CLI)、 AWS Tools for PowerShell、または AWS SDK を使用して AWS プログラムで AWS サービスを呼び出すことができます。

API コールを行う場合、認証情報プロファイルとして workspaces_machine_role を指定します。それ以外の場合、アクセス許可が不十分なため、オペレーションは失敗します。

ストリーミングインスタンスがプロビジョニングされている間、WorkSpaces は指定されたロールを引き受けます。WorkSpaces は AWS 、API コール用に VPC にアタッチされた Elastic Network Interface を使用するため、アプリケーションまたはスクリプトは、 AWS API コールを行う前に Elastic Network Interface が使用可能になるまで待機する必要があります。Elastic Network Interface が使用可能になる前に API 呼び出しが行われると、呼び出しは失敗します。

以下の例では、workspaces_machine_role 認証情報プロファイルを使用して、ストリーミングインスタンス (EC2 インスタンス) を記述し、Boto クライアントを作成する方法を示します。Boto は、Amazon Web Services (AWS) SDK for Python です。

CLI を使用してストリーミングインスタンス (EC2 インスタンス) AWS を記述する

```
aws ec2 describe-instances --region us-east-1 --profile workspaces_machine_role
```

AWS Tools for PowerShell を使用してストリーミングインスタンス (EC2 インスタンス) を記述する

AWS Tools for PowerShell バージョン 3.3.563.1 以降、Amazon Web Services SDK for .NET バージョン 3.3.103.22 以降を使用する必要があります。 AWS Tools for PowerShell と Amazon Web Services SDK for .NET を含む AWS Tools for Windows インストーラは、AWS Tools for PowerShell ウェブサイトからダウンロードできます。

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

AWS SDK for Python を使用した Boto クライアントの作成

```
session = boto3.Session(profile_name=workspaces_machine_role')
```

# 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、複数の 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 AWS コンプライアンスを評価します。これらのプログラムには、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AWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。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。

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

WorkSpaces および FedRAMP の詳細については、「 WorkSpaces Personal で FedRAMP 認証または DoD SRG コンプライアンスを設定する 」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＆コンプライアンスクイックリファレンスガイド」 – 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手順が記載されています。
- アマゾン ウェブ サービスでの HIPAA セキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と場所に適用される場合があります。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – AWS Configは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

## Amazon WorkSpaces の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。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が高く、フォールトトレラントで、スケーラブルです。

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 が利用できないときに WorkSpaces ユーザーを別の AWS リージョンの代替 WorkSpaces にリダイレクトする機能です。詳細については、「WorkSpaces Personal のクロスリージョンリダイレクト」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 がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で 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 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

## ネットワークの隔離

Virtual Private Cloud (VPC) は、 AWS クラウド内の論理的に隔離された独自のエリア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、「WorkSpaces Personal 用に VPC を設定する」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、「WorkSpaces Personal で信頼されたデバイス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 Personal 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場合、VPC と Amazon WorkSpaces API エンドポイント間の通信は、 AWS ネットワーク内で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、「WorkSpaces Personal の IP アドレスとポートの要件」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、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 接続なしで、VPC を Amazon WorkSpaces API エンドポイントに直接接続します。VPC のインスタンスは、パブリック IP アドレスがなくても 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て、 または AWS Command Line Interface （ AWS CLI) コマンドを使用して AWS Management Console Amazon WorkSpaces に接続できます。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、Amazon VPC と Amazon Amazon WorkSpaces の両方が利用可能なすべての AWS リージョンで VPC エンドポイントをサポートします。 https://docs.aws.amazon.com/general/latest/gr/rande.html#vpc_regionAmazon WorkSpaces では、すべてのパブリック APIを VPC 内に配置します。

詳細については AWS PrivateLink、 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**
>
> を使用する Amazon WorkSpaces API エンドポイント AWS PrivateLink は、連邦情報処理規格 (FIPS) Amazon WorkSpaces API エンドポイントではサポートされていません。

## 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。
- 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 内のインスタンスから接続するか、AWS Virtual Private Network （ AWS VPN) または 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 AWS Direct Connect。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。詳細については AWS Direct Connect、「 AWS Direct Connect ユーザーガイド」の「接続の作成」を参照してください。

# WorkSpaces に関する更新管理

定期的に WorkSpaces のオペレーティングシステムやアプリケーションに対してパッチ処理、更新、および保護を行うことをお勧めします。WorkSpaces は、通常のメンテナンス期間中に WorkSpaces によって更新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、「WorkSpaces Personal のメンテナンス」を参照してください。

WorkSpaces 上のアプリケーションについては、提供されている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プログラム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。

# Amazon WorkSpaces のクォータ

Amazon WorkSpaces は、WorkSpaces、イメージ、バンドル、ディレクトリ、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は次のとおりです。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 | 引き上げ可能 |
| --- | --- | --- | --- |
| WorkSpaces | 1 | 現在のリージョン内のこのアカウントの WorkSpaces の最大数。 | はい |
| Graphics WorkSpaces | 0 | 現在のリージョン内のこのアカウントの Graphics WorkSpaces の最大数。<br><br>**Note**<br>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。それまでに WorkSpaces | はい |

| リソース | デフォルト | 説明 | 引き上げ可能 |
| --- | --- | --- | --- |
| | | 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、「WorkSpaces Personal で WorkSpace を移行する」を参照してください。 | |
| GeneralPurpose.4xlarge WorkSpaces | 1 | このアカウントの現在のリージョンにおける GeneralPurpose.4xlarge WorkSpaces の最大数。 | はい |
| GeneralPurpose.8xlarge WorkSpaces | 1 | このアカウントの現在のリージョンにおける GeneralPurpose.8xlarge WorkSpaces の最大数。 | はい |
| Graphics.g4dn WorkSpaces | 0 | 現在のリージョン内のこのアカウントの Graphics.g4dn WorkSpaces の最大数です。 | はい |

| リソース | デフォルト | 説明 | 引き上げ可能 |
| --- | --- | --- | --- |
| GraphicsPro WorkSpaces | 0 | 現在のリージョン内のこのアカウントの GraphicsPro WorkSpaces の最大数です。(GraphicsPro end-of-lifeになります。 他のサポートされているバンドルを置き換えとして使用することを検討してください）。 | はい |
| GraphicsPro.g4dn WorkSpaces | 0 | 現在のリージョン内のこのアカウントの GraphicsPro.g4dn WorkSpaces の最大数です。 | はい |
| スタンバイ WorkSpaces | 5 | 現在のリージョン内のこのアカウントの WorkSpaces の最大数。 | はい |
| 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 |

| リソース | デフォルト | 説明 | 引き上げ可能 |
| --- | --- | --- | --- |
| 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 | 現在のリージョンにおいて、このアカウントで Amazon WorkSpaces 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 |
| 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 |

| リソース | デフォルト | 説明 | 引き上げ可能 |
| --- | --- | --- | --- |
| WorkSpaces Pools | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools の最大数。 | はい |
| WorkSpaces Pools の汎用 Value ストリーミングインスタンス | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる汎用 Value ストリーミングインスタンスの最大数。 | はい |
| WorkSpaces Pools の汎用 Standard ストリーミングインスタンス | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる汎用 Standard ストリーミングインスタンスの最大数。 | はい |
| WorkSpaces Pools の汎用 Performance ストリーミングインスタンス | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる汎用 Performance ストリーミングインスタンスの最大数。 | はい |
| WorkSpaces Pools の汎用 Power ストリーミングインスタンス | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる汎用 Power ストリーミングインスタンスの最大数。 | はい |

| リソース | デフォルト | 説明 | 引き上げ可能 |
| --- | --- | --- | --- |
| WorkSpaces Pools の汎用 PowerPro ストリーミングインスタンス | 10 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる汎用 PowerPro ストリーミングインスタンスの最大数。 | はい |
| WorkSpaces Pools のグラフィックス Graphics.g4dn xlarge ストリーミングインスタンス | 0 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる Graphics.g4dn xlarge ストリーミングインスタンスの最大数。 | はい |
| WorkSpaces Pools のグラフィックス Graphics.g4dn 4xlarge ストリーミングインスタンス | 0 | 現在のリージョン内のこのアカウントの WorkSpaces Pools で使用できる Graphics.g4dn 4xlarge ストリーミングインスタンスの最大数。 | はい |

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 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、WorkSpaces Personal および WorkSpaces Pools の WorkSpaces WorkSpaces クライアントの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、技術ガイダンス、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。技術ガイダンスフェーズで修正が必要な場合、 はその修正を今後の公開バージョンリリース用に AWS スケジュールします。修正に関連する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できます。

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。終了日を過ぎると、それ以上のサポートやメンテナンスは提供されません。 は互換性の問題のテスト AWS を停止します。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。

> **Important**
>
> 次のバージョンのサポートは 2025 年 3 月 31 日までに終了します。サービスの中断を避けるため、サポート対象のクライアントバージョンが EOL になる前に必ずアップグレードしてください。
>
> - Windows 3.x、4.x、および 5.0 ~ 5.22.0
> - Ubuntu 20.04 用の Linux 4.x、2023.x、および 2024 年 0 月 5 日
> - Ubuntu 22.04 用の Linux 2023.x および 2024.0 ~ 2024.5

- macOS 3.x、4.x、および 5.1 ~ 5.22.0
- Android 3.x、4.x、および 5.0.0

| 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 | メモ |
|---|---|---|---|---|
| 5.22.1 以降 | 2024 年 9 月 3 日 | | | サポート |
| 5.0 ~ 5.22.0 | 2022 年 6 月 2 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| 4.x | 2021 年 6 月 30 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| 3.x | 2019 年 11 月 25 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| Ubuntu 22.04 では 2024.6 以降 | 2024 年 9 月 6 日 | | | サポート |
| Ubuntu 20.04 の場合は 2024.6 以降 | 2024 年 9 月 6 日 | | | サポート |
| Ubuntu 22.04 の場合、2024 年 0 月 5 日 | 2024 年 2 月 1 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| Ubuntu 20.04 の場合は 2024.0 ~ 2024.5 | 2023 年 8 月 24 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| Ubuntu 22.04 用の 2023.x | 2023 年 8 月 24 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| Ubuntu 20.04 用の 2023.x | 2023 年 8 月 24 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアン |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| | | | | トバージョンにアップグレードしてください。 |
| Ubuntu 20.04 用の 4.x | 2022 年 10 月 27 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| 5.22.1 以降 | 2024 年 9 月 3 日 | | | サポート |
| 5.1 ~ 5.22.0 | 2022 年 6 月 30 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| 4.x | 2021 年 8 月 5 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| 3.x | 2019 年 11 月 25 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| 2.x | 2019 | | | サポート |

| 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 | メモ |
| --- | --- | --- | --- | --- |
| 5.0.1 以降 | 2024 年 11 月 6 日 | | | サポート |
| 5.0.0 | 2024 年 2 月 26 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |
| 4.x | 2022 年 5 月 12 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンに |

| 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 | メモ |
|---|---|---|---|---|
| | | | | アップグレードしてください。 |
| 3.x | 2021 年 6 月 30 日 | 2024 年 11 月 21 日 | 2025 年 3 月 31 日 | このバージョンが終了日に達する前に、必ず最新のクライアントバージョンにアップグレードしてください。 |

| 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 |
| 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バージョン

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 | 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 | 5.10 | 2023 年 6 月 19 日 | 2023 年 10 月 1 日 | 2023 年 10 月 1 日 | サポートされていません |
| Windows | 5.9 | 2023 年 5 月 9 日 | 2023 年 10 月 1 日 | 2023 年 10 月 1 日 | サポートされていません |
| Windows | 2.x | 2018 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |
| Ubuntu | 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 | サポートされていません |
| Ubuntu | 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 | サポートされていません |
| macOS | 2.x | 2019 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |
| macOS | 1.x | 2018 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |
| iPad | 1.x | 2018 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |
| Android | 2.x | 2019 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |
| Android | 1.x | 2018 | 2023 年 3 月 31 日 | 2023 年 8 月 31 日 | サポートされていません |

# 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?

技術支援とソフトウェア更新は、EOL に達したオペレーティングシステムでは利用できなくなり、EOL に達したオペレーティングシステムを使用する WorkSpaces クライアントではサポート AWS されません。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。

# DCV でサポートされている SDK 拡張機能

DCV は、幅広いワークロードとユースケースで 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。Amazon 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のために、DCV WorkSpaces のエクスペリエンスを以下のようにカスタマイズできます。

- 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。

Amazon DCV 拡張機能 SDK の使用を開始するには、Amazon 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 Amazon DCV 拡張機能 SDK の GitHub リポジトリにあります。また、Amazon DCV 拡張機能 SDK サンプル GitHub リポジトリで、SDK の統合例を確認することもできます。

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 – DCV
- WorkSpaces Windows クライアント – Windows: 5.9.0.4110 以降。

> **Note**
>
> WorkSpaces Android クライアント、iOS クライアント、Web Access は、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 |
| --- | --- | --- |
| 実行モード | WorkSpaces Pools の実行モードによって、即時の可用性と支払い方法が決まります。WorkSpaces Pools を作成するときに、2 つの実行モードから選択できます。 | 2025 年 5 月 15 日 |
| Microsoft Entra ID ディレクトリ | IAM Identity Center と WorkSpaces 間のクロスリージョン統合がサポートされています。 | 2025 年 2 月 27 日 |
| Microsoft Entra ID ディレクトリ | 専用の Microsoft Entra ID ディレクトリを作成できます。 | 2024 年 8 月 26 日 |
| Microsoft Visual Studio | アプリケーションの管理で Microsoft Visual Studio バンドルがサポートされます。 | 2024 年 8 月 1 日 |
| Amazon DCV WebRTC リダイレクト拡張機能 | Amazon DCV WebRTC リダイレクト拡張機能をインストールして、WebRTC リダイレクトを使用できます。 | 2024 年 8 月 1 日 |
| WorkSpaces Pools が で利用可能になりました AWS GovCloud (US) Region | WorkSpaces Pools では、一時的なインフラストラクチャでホストされている高度に選別されたデスクトップ環境への | 2024 年 7 月 23 日 |

| | | |
|---|---|---|
| | オンデマンドアクセスを必要とするユーザーに向けて、カスタマイズされた非永続的な仮想デスクトップを提供します。 | |
| WorkSpaces Pools の提供開始 | WorkSpaces Pools では、一時的なインフラストラクチャでホストされている高度に選別されたデスクトップ環境へのオンデマンドアクセスを必要とするユーザーに向けて、カスタマイズされた非永続的な仮想デスクトップを提供します。 | 2024 年 6 月 27 日 |
| AmazonWorkSpacesAdmin マネージドポリシーの更新と新しい AmazonWorkSpacesPoolServiceAccess マネージドポリシー | WorkSpaces の AmazonWorkSpacesAdmin マネージドポリシーが更新され、新しい AmazonWorkSpacesPoolServiceAccess マネージドポリシーが追加されました。 | 2024 年 6 月 27 日 |
| 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 |
| DCV でサポートされている SDK 拡張機能 | Amazon DCV 拡張機能 SDK を使用することで、デベロッパーはエンドユーザーのために、DCV WorkSpaces の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 |

| | | |
|---|---|---|
| DCV ホストエージェントバージョン | DCV のバージョン情報。 | 2023 年 5 月 8 日 |
| Amazon WorkSpaces が AWS GovCloud (米国東部) で利用可能に | Amazon WorkSpaces は、AWS GovCloud (米国東部) で利用できます。 | 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 DCV を使用してシームレスにリダ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。 | 2021 年 4 月 5 日 |
| 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。スマートカードサポートは、DCV を使用して WorkSpaces で利用できます。 | 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 |
| スマートカード | Amazon WorkSpaces は、AWS GovCloud (米国西部) リージョンの Windows および Linux WorkSpaces でセッション前 (ログイン) およびセッション内スマートカード認証をサポートするようになりました。 | 2020 年 12 月 1 日 |
| DCV | Graphics と GraphicsPro を除くすべてのバンドルタイプの、ライセンス付属 (Windows Server 2016) の WorkSpaces と BYOL Windows 10 ベースの WorkSpaces の両方で、DCV が利用可能になりました。DCV 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 |
| 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場合、VPC と Amazon WorkSpaces API エンドポイント間の通信は、 AWS ネットワーク内で完全かつ安全に行われます。 | 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 Microsoft Active Directory ドメインの間に信頼関係を確立し、オンプレミスドメインのユーザーに 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。