aws

管理ガイド

Amazon WorkSpaces

Amazon WorkSpaces: 管理ガイド

Table of Contents

とは WorkSpaces 1
クライアントアプリケーションを使用した接続 3
自分の Windows デスクトップライセンスを使用する 4
Microsoft を使用するための前提条件 BYOL 4
でサポートされている Windows バージョン BYOL 7
BYOL に対するアカウントの適格性を判断する 8
適格な WorkSpaces アカウントの BYOL を有効にする 9
VM がBYOL要件を満たしていることを確認する 11
一般的なエラーメッセージとその解決策 13
SysPrep エラーメッセージとエラー修正のリスト 18
VM を仮想化環境からエクスポートする 20
VM をイメージとして Amazon にインポートする EC2 20
Microsoft Office をBYOLイメージに追加する 21
Microsoft Office のバージョン間で移行する 26
WorkSpaces コンソールを使用してBYOLイメージを作成する 28
のBYOLイメージからカスタムバンドルを作成する WorkSpaces 30
BYOL イメージを使用する専用ディレクトリを作成する WorkSpaces 30
を起動する BYOL WorkSpaces 31
BYOL イメージのアップロードと作成に関する動画 33
のBYOLアカウントをリンクする WorkSpaces 33
WorkSpaces Personal の使用と管理 35
WorkSpaces Personal のオプション 36
WorkSpaces Personal の使用を開始する 36
を作成する WorkSpace 46
に接続する WorkSpace 49
次のステップ 50
ネットワークプロトコルとアクセス 51
Amazon のプロトコル WorkSpaces 51
VPC の要件 53
AWS Global Accelerator (AGA) 59
WorkSpaces のアベイラビリティーゾーン 61
IP アドレスとポートの要件 63
ネットワークの要件 148
信頼されたデバイス 151

SAML 2.0 統合 154
Microsoft Entra ID へのアクセス 179
スマートカード認証 183
インターネットアクセス 194
セキュリティグループ 196
IP アクセスコントロールグループ 197
PCoIP ゼロクライアント 200
Chromebook 用の Android の設定 201
Web Access を設定する 202
FIPS エンドポイントの暗号化を設定する 207
Linux SSHの接続を有効にする WorkSpaces 209
必須の設定とサービスコンポーネント 215
のディレクトリを管理する WorkSpaces 222
既存の AWS Directory Service ディレクトリを登録する 224
組織単位を選択する 226
自動パブリック IP アドレスを設定する 227
デバイスのアクセスコントロール 228
ローカル管理者の許可を管理する 228
AD Connector アカウント (AD Connector) を更新する 229
多要素認証 (AD Connector) 229
ディレクトリを作成する 230
のDNSサーバーを更新する WorkSpaces 255
ディレクトリを削除する 263
AWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする 265
ディレクトリ管理を設定する 267
ユーザーの管理 270
ユーザーの管理 270
ユーザー WorkSpaces 用に複数の を作成する 272
WorkSpaces へのユーザーログイン方法をカスタマイズする 273
ユーザーを対象とした WorkSpaces の自己管理機能を有効にする 276
Amazon Connect オーディオ最適化を有効にする 279
診断ログのアップロードを有効にする 282
WorkSpaces 個人用の管理 283
Windows の管理 WorkSpaces 285
Amazon Linux を管理する WorkSpaces 332
Ubuntu を管理する WorkSpaces 341

Rocky Linux を管理する WorkSpaces 349
Red Hat Enterprise Linux を管理する WorkSpaces 356
リアルタイム通信用に最適化する 362
実行モードを管理する 372
アプリケーションの管理 375
の変更 WorkSpace 382
ブランドのカスタマイズ 389
リソースのタグ付け 397
メンテナンス 399
暗号化済み WorkSpaces 401
WorkSpace の再起動 411
の再構築 WorkSpace 412
の復元 WorkSpace 415
Microsoft 365 BYOL 416
Windows BYOL WorkSpaces のアップグレード 420
の移行 WorkSpace 429
WorkSpace の削除 438
バンドルとイメージ 439
バンドルオプション 442
カスタムイメージとカスタムバンドルを作成する 447
カスタムバンドルを更新する 469
カスタムイメージのコピー 470
カスタムイメージを共有/共有解除する 473
カスタムバンドルまたはイメージを削除する 476
WorkSpaces Personal のモニタリング 477
CloudWatch 自動ダッシュボードによるモニタリング 479
CloudWatch メトリクスを使用したモニタリング 481
Amazon を使用したモニタリング EventBridge 493
スマートカードユーザーの AWS サインインイベントを理解する 497
カスタム CloudWatch ダッシュボードを作成する 503
ビジネス継続性 509
クロスリージョンリダイレクト 510
マルチリージョンレジリエンス 528
トラブルシューティング 537
高度なログ記録の有効化 537
固有の問題のトラブルシューティング 542

リリースノート 574
WorkSpaces プールの使用と管理 582
サポートされるリージョンとアベイラビリティーゾーン 582
ディレクトリを管理する 585
2.0 SAML を設定し、プールディレクトリを作成する 586
ディレクトリの詳細を更新する 605
WorkSpaces プールディレクトリの登録を解除する 608
ネットワークとアクセス 609
インターネットアクセス 609
VPC の要件 611
Amazon S3 VPCエンドポイント 624
への接続 VPC 626
ユーザー接続 628
WorkSpaces プールを作成する 631
WorkSpaces プールの管理 634
実行モード 634
バンドル 634
プールの変更 635
プールを削除する 636
WorkSpaces プールの Auto Scaling 636
アクティブディレクトリの使用 648
アクティブディレクトリドメイン 649
開始する前に 650
証明書ベースの認証 652
管理 659
詳細情報 666
バンドルとイメージ 666
バンドルオプション 668
カスタムイメージとカスタムバンドルを作成する 672
カスタムイメージとカスタムバンドルの管理 688
セッションスクリプトを使用してエクスペリエンスを管理する 689
WorkSpaces Pools のモニタリング 699
WorkSpaces Pools のメトリクスとディメンション 700
永続的ストレージを管理する 702
ホームフォルダを管理する 702
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 709

アプリケーション設定の永続化の仕組み 710
アプリケーション設定の永続化を有効にする 712
ユーザーのアプリケーション設定VHDsの を管理する 714
トラブルシューティング通知コード 721
セキュリティ 725
データ保護 726
保管中の暗号化 727
転送中の暗号化 727
Identity and Access Management 727
ポリシーの例 729
IAM ポリシーで WorkSpaces リソースを指定する 736
workspaces_DefaultRole Role を作成する 742
AmazonWorkSpacesPCAAccess サービスロールを作成する 743
AWS の マネージドポリシー WorkSpaces 744
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 752
コンプライアンス検証 757
耐障害性 758
インフラストラクチャセキュリティ 758
ネットワークの隔離 759
物理ホストでの分離 759
企業ユーザーの承認 759
VPC インターフェイスエンドポイントを介した Amazon WorkSpaces API リクエストの実行 760
Amazon のVPCエンドポイントポリシーを作成する WorkSpaces 761
プライベートネットワークを に接続する VPC 763
更新管理 763
クォータ 764
WorkSpaces クライアントのサポート終了 770
サポートされていないクライアントバージョン 776
EOL FAQs 777
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EOL。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? 777
サポートされている EOLで に到達したバージョンの WorkSpaces クライアントを使用できますか WorkSpace? 777
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EOL。これに関する問題を引き続き報告できますか? 777

に達したオペレーティングシステムでサポートされている WorkSpaces クライアントバージョンを使用していますEOL。これに関する問題を引き続き報告できますか? 777
拡張機能SDKデベロッパーガイド 778
ドキュメント履歴 779
以前の更新 787
..... dccxci

Amazon とは WorkSpaces

Amazon WorkSpaces では、 と呼ばれる仮想クラウドベースのデスクトップをユーザーWorkSpaces向けにプロビジョニングできます。これらのデスクトップは、Microsoft Windows、Amazon Linux 2、Ubuntu Linux、Rocky Linux、または Red Hat Enterprise Linux を実行できます。 WorkSpaces により、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が不要になります。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、組織やユーザーのニーズに応じて、 WorkSpaces 個人用プールと WorkSpaces プールを選択できます。

- WorkSpaces Personal - 専用の高度にパーソナライズされたデスクトップを必要とするユーザー向けにカスタマイズされた永続的な仮想デスクトップが必要な場合は、 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 WorkSpace で を作成する」を参照してください。
- WorkSpaces プール - エフェメラルインフラストラクチャでホストされている高度にキュレートされたデスクトップ環境にアクセスする必要があるユーザー向けにカスタマイズされた、非永続的な仮想デスクトップには WorkSpaces プールを選択します。詳細については、「 WorkSpaces プールの管理」を参照してください。

WorkSpaces デスクトップはさまざまな方法で設定できます。

- ハードウェア設定、ソフトウェア設定、および AWS リージョンの範囲から選択します。詳細については、「Amazon WorkSpaces Bundles」および「」を参照してくださいthe section called “カスタムイメージとカスタムバンドルを作成する”。
- 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 が Windows 10 または 11 を実行している場合は、 WorkSpaces を Microsoft Entra ID に結合して、ユーザーが既存の Entra ID 認証情報を使用して Microsoft 365 Apps for enterprise にシームレスにアクセスできるようにします。 WorkSpaces を Intune に登録して、Intune を使用し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 を使用して専用の 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 Microsoft Active Directory を作成するか、 WorkSpaces をオンプレミスの Active Directory に接続して、ユーザーが既存の認証情報を使用して企業リソースにシームレスにアクセスできるようにします。詳細については、「the section called “のディレクトリを管理する WorkSpaces”」を参照してください。
- オンプレミスデスクトップの管理に使用する WorkSpaces のと同じツールを使用して を管理します。
- セキュリティを強化するには、多要素認証 (MFA) を使用します。
- 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 にアクセスするために使用できる IP アドレスを選択します WorkSpaces。
- 月額または時間単位の請求を選択します WorkSpaces。詳細については、WorkSpaces 料金を参照してください。

の使用の詳細については WorkSpaces、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 をデプロイするためのベストプラクティス WorkSpaces
- Amazon WorkSpaces FAQs
- WorkSpaces 料金の詳細と例については、WorkSpaces 「 料金表」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。

で独自の Windows デスクトップライセンスを使用する WorkSpaces

Microsoft とのライセンス契約で許可されている場合は、Windows 10 または 11 デスクトップを に持ち込んでデプロイできます WorkSpaces。これを行うには、Bring Your Own License (BYOL) を有効にし、以下の要件を満たす Windows 10 または 11 ライセンスを提供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BYOL WorkSpaces内のお客様専用のハードウェアで 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 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 の累積更新プログラムまたはセキュリティ更新プログラムは、 WorkSpaces イメージ作成プロセスでサポートされています。

Amazon BYOLで Microsoft を使用するための前提条件 WorkSpaces

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。
- バンドル (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および 以外のバンドル GraphicsPro) を使用する場合は non-GPU-enabled、リージョン WorkSpaces ごとに 100 以上を使用することを確認します。これらの 100 は、 AlwaysOn と の任意の組み合わせに WorkSpaces することができます AutoStop WorkSpaces。専用ハードウェア WorkSpaces で を実行するには、リージョン WorkSpaces あたり 100 個以上を使用する必要があります。Microsoft のライセンス要件に準拠するには、専用ハードウェア WorkSpaces で を実行する必要があります。専用ハードウェアは AWS 側でプロビジョニングされるため、 はデフォルトのテナンシーを維持VPCできます。

GPU対応 (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro) バンドルを使用する場合は、リージョン WorkSpaces で 1 か月あたり最低 4 AlwaysOn 個または 20 AutoStop GPU個を専用ハードウェアで実行することを確認します。

Note

- GraphicsPro バンドルは end-of-life 2025 年 10 月 31 日に終了します。2 GraphicsPro WorkSpaces 025 年 10 月 31 日より前に 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、「Personal WorkSpace で を移行する WorkSpaces」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。を WorkSpaces Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。
- グラフィックスと GraphicsPro バンドルは、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、および GraphicsPro バンドルは、アフリカ (ケープタウン) リージョンおよびイスラエル (テルアビブ) リージョンでは利用できません。
- をアフリカ (ケープタウン) リージョン WorkSpaces で実行するには、アフリカ (ケープタウン) リージョン WorkSpaces で最低 400 を実行する必要があります。
- Windows 11 バンドルは DCV用に作成できます WorkSpaces。Windows 11 バンドルは、 WorkSpaces Core を使用するパートナープロトコルでもサポートされています。
- Windows 11 では、グラフィックスと GraphicsPro バンドルはサポートされていません。
- 値バンドルは Windows 11 および WorkSpaces プールでは使用できません。既存の値バンドル WorkSpaces の移行の詳細については、「」を参照してくださいPersonal WorkSpace で を移行する WorkSpaces 。
- 最高のビデオ会議エクスペリエンスを得るには、Power または PowerPro バンドルを使用することをお勧めします。
- Windows 11 では、Unified Extensible Firmware Interface (UEFI) ブートモードが機能する必要があります。VM を正常にインポートUEFIするには、オプションの `--boot-mode`パラメータを として指定してください。

- WorkSpaces は、/16 IP アドレス範囲内の管理インターフェイスを使用できます。管理インターフェイスは、インタラクティブストリーミングに使用される安全な WorkSpaces 管理ネットワークに接続されます。これにより、 WorkSpaces は を管理できます WorkSpaces。詳細については、「ネットワークインターフェイス」を参照してください。この目的のために、次の IP アドレス範囲のうち少なくとも 1 つから /16 ネットマスクを予約する必要があります。
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

  > **Note**
  >
  > - WorkSpaces サービスを採用すると、使用可能な管理インターフェイスの IP アドレス範囲が頻繁に変更されます。現在使用可能な範囲を確認するには、 list-available-management-cidr-ranges AWS Command Line Interface （ AWS CLI) コマンドを実行します。
  > - 選択した /16 CIDRブロックに加えて、54.239.224.0/20 の 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。

- の Microsoft Windows および Microsoft Office のKMSアクティベーションに必要な管理インターフェイスポートが開いていることを確認しますBYOL WorkSpaces。詳細については、「管理インターフェイスポート」を参照してください。
- サポートされている 64 ビットバージョンの Windows を実行する仮想マシン (VM) があります。サポートされているバージョンのリストについては、このトピックの でサポートされている Windows バージョン BYOL 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 (GPOs) 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、 を通じ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GPOsでき、デフォルトのユーザープロファイルに対して行われたカスタマイズよりもエラーが発生しにくいためです。
  - イメージを共有する前に、ローカル管理者アクセス権を持つ WorkSpaces_BYOL アカウントを作成する必要があります。このアカウントのパスワードは後で必要になる可能性があるため、メモしておいてください。
  - VM は、最大サイズが 70 GB、空き容量が 10 GB 以上の 1 つのボリューム上にあることが必要です。BYOL イメージの Microsoft Office もサブスクライブする場合は、VM は最大サイズが 70 GB、空き容量が 20 GB 以上の 1 つのボリューム上にある必要があります。ルートボリューム DISKがある は 70GB 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。
- BYOL で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Amazon の Windows VM が Microsoft WorkSpaces の要件を満たしていることを確認します。 BYOL。
- `%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**
>
> - ではBYOL AutoStop WorkSpaces、多数の同時ログインにより、 が利用可能 WorkSpaces になるまでの時間が大幅に長くなる可能性があります。多数のユーザーがBYOL AutoStop WorkSpaces 同時に にログインすることが予想される場合は、アカウントマネージャーにアドバイスを求めてください。
> - 暗号化AMIsはインポートプロセスではサポートされていません。の作成に使用したインスタンスを無効にし、EBS暗号化EC2AMIします。暗号化は、最終的な WorkSpaces がプロビジョニングされた後に有効にできます。

でサポートされている Windows バージョン BYOL

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、使用している AWS リージョンで利用可能なすべてのコンピューティングタイプをサポートしています WorkSpaces。Microsoft でサポートされなくなった Windows のバージョンは動作する保証はなく、 AWS サポートでもサポートされません。

> **Note**
>
> BYOL 現時点では、Windows 10 N および Windows 11 N バージョンは ではサポートされていません。

WorkSpaces アカウントが Microsoft BYOL に適格であ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 AWS アカウントの CIDR 範囲と BYOL 設定を別の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ために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 API 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、「のBYOLアカウントをリンクする WorkSpaces」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/ 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。使用を開始するには、AWS アカウントマネージャーまたは営業担当者にお問い合わせいただくか、AWS Support センターにお問い合わせください。担当者が BYOL 適格性を検証します。

   BYOL 適格性を判断するには、お客様から特定の情報を担当者にご提供いただく必要があります。例えば、次の質問への回答を求められる場合があります。

   - 前述の BYOL 要件を確認して承諾しましたか?
   - アカウントを BYOL 対応とする必要がある AWS リージョンはどこですか?
   - デプロイする予定の BYOL WorkSpaces は AWS リージョンごとにいくつありますか?
   - 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 対応となっている他の 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 API 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。

Amazon WorkSpaces コンソールを使用して適格な WorkSpaces アカウントの BYOL を有効にする

「WorkSpaces アカウントが Microsoft BYOL に適格であ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/ 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、「WorkSpaces アカウントが Microsoft BYOL に適格であ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、続行する前に AWS アカウントマネージャーまたは営業担当者に連絡するか、 AWS Supportセンターに連絡してください。
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。

Amazon の Windows VM が Microsoft WorkSpaces の要件を満たしていることを確認します。 BYOL

「」の手順に従って アカウントBYOLで を有効にした後Amazon WorkSpaces コンソールを使用して適格な WorkSpaces アカウントの BYOL を有効にする、VM が の要件を満たしていることを確認する必要がありますBYOL。そのためには、以下の手順を実行して Checker PowerShell スクリプトをダウンロードして実行します WorkSpaces BYOL。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**
>
> VM は、 で使用する前にすべてのテストに合格する必要がありますBYOL。

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、最新の Windows セキュリティ更新プログラムが VM にインストールされていることを確認します。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。

BYOL Checker スクリプトを実行するには、以下の手順を実行します。

BYOL Checker スクリプトを実行するには

1. Windows デスクトップから Windows を開きます PowerShell。Windows 開始ボタンを選択し、Windows PowerShell を右クリックして、管理者として実行を選択します。デバイスに変更

PowerShell を加えるかどうかを選択するようにユーザーアカウントコントロールから求められた場合は、はいを選択します。

2. PowerShell コマンドプロンプトで、BYOLChecker スクリプトがあ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 PowerShell の実行ポリシーを更新します。これにより、BYOLChecker スクリプトは次のことを実行できます。

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. PowerShell 実行ポリシーを変更するかどうかを確認するプロンプトが表示されたら、「はいA」と「すべて」と指定します。

5. Checker BYOL スクリプトを実行するには、次のコマンドを入力します。

   ```
   .\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 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。ステータスが のテストではFAILED、Info を選択して、障害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 のステータスが表示された場合はWARNING、すべての警告を修正する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は、 BYOLPrevalidationlog*YYYY-MM-DD_HHmmss*.txtと の 2 つのログファイルを生成しますImageInfo.text。これらのファイルは、BYOLChecker 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チェッカー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 が成功すると、ステップ 12 でエクスポートした VM を Amazon Elastic Compute Cloud (Amazon) にインポートできますEC2。

    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。次に、BYOLChecker スクリプトを再実行して、問題が解決されたことを確認します。

    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。 PowerShell コマンドレットを使用して AppX `Remove-AppxPackage` パッケージを削除します。

14. ステップ 12 でエクスポートした VM を Amazon にインポートしますEC2。

一般的なエラーメッセージとその解決策

BYOL import は、アクティブな Microsoft Office がインストールされた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 インポートには、 PCoIP エージェントの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 エージェントをアンインストールする方法については、「Teradici Software PCoIP Client for Mac のアンインストール」を参照してください。

BYOL インポートでは、Windows 更新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 import では、Automount 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 import では、 WorkSpaces_BYOL アカウントを有効にする必要があります

WorkSpaces_BYOL アカウントを有効にする必要があります。詳細については、「Amazon WorkSpaces コンソールBYOLを使用してアカウントBYOLで を有効にする」を参照してください。

BYOL import では、ネットワークインターフェイス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。

を使用するように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DHCP。詳細については、TCP「/IP 設定を変更する」を参照してください。

BYOL インポートには、ローカルディスクに 20 GB を超える容量が必要です。

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 インポートには、1 つのローカルドライブを持つシステムが必要です。他に、ローカルドライブ、リムーバブルドライブ、またはネットワークドライブがあります。

イメージのインポートに使用される には WorkSpace 、C および D ドライブのみ存在できます。仮想ドライブを含め他のすべてのドライブを削除します。

BYOL 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 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 デバイス管理FAQ」を参照してください。

BYOL 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 デバイス管理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が無効になっている必要があります。

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 インポートには、VMwareツールのないシステムが必要です。

VMWare ツール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、「Fusion (1014522) でのVMwareツールVMwareのアンインストールと手動インストール」を参照してください。

BYOL 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 インポートでは、ローカルドライブのパーティションが 2 つ未満です。さらに、すべての Windows 10 パーティションをMBRパーティション化し、すべての Windows 11 パーティションをGPTパーティション化する必要があります。

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 import では、再起動が必要な保留中のすべての更新が完了している必要があります。

すべての更新プログラムをインストールし、オペレーティングシステムを再起動します。

BYOL インポートでは、 AutoLogon が無効になっている必要があります。

AutoLogon レジストリを無効にするには：

1. Windows キー + R を押して、コマンドプロンプトに `Regedit.exe` を入力します。

2. HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon まで下にスクロールします。
3. DontDisplayLastUserName に値を追加します。
4. [タイプ] に REG_SZ を入力します。
5. [値] に「0」と入力します。

> **Note**
>
> - 値 DontDisplayLastUserName は、ログオンダイアログボックスに、PC に最後にログオンしたユーザーのユーザー名を表示するかどうかを決定します。
> - この値はデフォルトでは存在しません。存在する場合は、 に設定する必要があります。0設定されていない場合DefaultUser、 の値は消去され、失敗 AutoLogon します。

BYOL インポートを有効にする**RealTimeIsUniversal**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 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 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、「 でサポートされている Windows バージョンBYOL」を参照してください。

BYOL インポートには、再調整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 import 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 import では、システムにウイルス対策がインストールされていない必要があります。

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。を実行してBYOLChecker、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 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 にはレガシー BIOS BootMode を使用する必要があります。詳細については、「ブートモード」を参照してください。

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

予約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.`

SysPrep エラーメッセージとエラー修正のリスト

AMI インポートする には 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AMIする では、リザーブドストレージ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
```

AMI インポートする には、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。を実行してBYOLChecker、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、「Amazon の Windows VM が Microsoft WorkSpaces の要件を満たしていることを確認します。 BYOL」を参照してください。

中にインポートAMIする に不明なエラーが発生しましたAMI SysPrep。

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

Amazon の仮想化環境から VM をエクスポートする WorkSpaces

「」の手順に従って VM が Microsoft BYOL要件を満たしていることを確認したらAmazon の Windows VM が Microsoft WorkSpaces の要件を満たしていることを確認します。 BYOL、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、 で使用できる BYOL のイメージを作成するために必要です WorkSpaces。

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) 、Trusted Platform Module (TPM) 2.0、および Secure Boot サポートの新しいハードウェア要件が設定されます。Windows 11 のインポートに固有の VM Import/Export では、Microsoft キーと Nitro を使用して UEFI Secure Boot が自動的に有効になりますTPM。詳細については、「VM Import/Export AWS を使用して Windows 11 イメージを に持ち込む」を参照してください。

のイメージを作成する準備EC2として、VM をBYOLイメージとして Amazon にインポートする WorkSpaces

「Amazon の仮想化環境から VM をエクスポートする WorkSpaces」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オプトインしている場合は、VM をインポートする前にそのオプションの選択を解除する必要があります。

VM を Amazon マシンイメージ () EC2 として Amazon にインポートしますAMI。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 EC2APIリファレンスImportImage」の「」を参照してください。

詳細については、VM Import/Export ユーザーガイドのイメージとして VM をインポートするを参照してください。

Amazon のBYOLイメージに Microsoft Office を追加する WorkSpaces

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イメージにプリインストールされ、このイメージから起動 WorkSpaces するすべての に含まれます。

> **Note**
>
> - を使用した Graphics.g4dn および GraphicsPro.g4dn BYOLイメージは、Office 2019 のみPCoIPをサポートします。Office 2016 はサポートしていません。
> - を使用した Graphics.g4dn および GraphicsPro.g4dn BYOLイメージは、 を通じて OfficeバンドルDCV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 料金」を参照してください。

> **Important**
>
> - BYOL イメージの作成に使用している VM に Microsoft Office が既にインストールされている場合は、Office をサブスクライブする場合は、そのイメージを 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 でブラウザベースのアプリケーションとデスクトップアプリケーションの両方に独自の Microsoft 365 ライセンスを持ち込むには WorkSpaces、BYOLイメージの取り込みプロセスが完了したらBYOL、イメージに Microsoft 365 アプリケーションをインストールします。

> **Note**
>
> Graphics.g4dn および GraphicsPro.g4dn BYOLイメージは Office 2019 のみをサポートし、Office 2016 はサポートしていません。

Office にサブスクライブすることを選択した場合、BYOLイメージの取り込みプロセスには最低 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、「」を参照してください WorkSpaces コンソールを使用してBYOLイメージを作成する。

オフィスの言語設定

Office サブスクリプションに使用される言語は、BYOLイメージの取り込みを実行している AWS リージョンに基づいて選択されます。例えば、アジアパシフィック (東京) リージョンでBYOLイメージの取り込みを実行している場合、Office サブスクリプションの言語は日本語になります。

デフォルトでは、頻繁に使用する Office 言語パックがいくつかインストールされます WorkSpaces。目的の言語パックがインストールされていない場合は、Microsoft から追加の言語パックをダウンロードできます。詳細については、Microsoft のドキュメントの「 Office 用言語アクセサリパック」を参照してください。

Office の言語を変更するには、いくつかのオプションがあります。

オプション 1: 個々のユーザーが Office の言語設定をカスタマイズできるようにする

個々のユーザーは、それぞれの Office 言語設定を調整できます WorkSpaces。詳細については、Microsoft ドキュメントの「Office で編集言語または作成言語を追加する、または言語の基本設定を設定する」を参照してください。

オプション 2: GPO管理テンプレート (.admx/.adml) を使用して、すべての WorkSpaces ユーザーにデフォルトの Office 言語設定を適用する

グループポリシーオブジェクト (GPO) 設定を使用して、 WorkSpaces ユーザーにデフォルトの Office 言語設定を適用できます。

> **Note**
>
> WorkSpaces ユーザーは、 を通じて適用される言語設定を上書きすることはできません GPO。

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 ドキュメントの「Customize language setup and settings for Office」を参照してください。Office 2016 と Office 2019 では、同じGPO設定 (Office 2016 のラベル付き) が使用されます。

を使用するにはGPOs、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 を操作する方法についてはGPOs、「」を参照してくださいWorkSpaces Personal で Active Directory 管理ツールを設定する。

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、 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 ファイル`office16.admx`と `office16.adml` ファイルを追加する必要があります。(`office16.admx` および `office16.adml` ファイルは、Office 2016 と Office 2019 の両方に適用されます)。`.admx` および `.adml` ファイルの操作の詳細については、Microsoft のドキュメントの「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。 WorkSpaces ディレクトリ管理 WorkSpace またはディレクトリに参加している 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 またはディレクトリに参加している WorkSpaces Amazon EC2インスタンスで、Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します`\\example.com`。
3. SYSVOL フォルダを開きます。
4. *FQDN* という名前のフォルダを開きます。
5. Policies フォルダを開きます。今、`\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies` に入っているはずです。
6. まだ存在しない場合は、PolicyDefinitions という名前のフォルダを作成します。
7. PolicyDefinitions フォルダを開きます。
8. office16.admx ファイルを `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions` フォルダにコピーします。
9. PolicyDefinitions フォルダに en-US という名前のフォルダを作成します。
10. en-US フォルダを開きます。
11. office16.adml ファイルを `\\`*FQDN*`\SYSVOL\`*FQDN*`\Policies\PolicyDefinitions\en-US` フォルダにコピーします。

Office のGPO言語設定を構成するには

1. ディレクトリ管理 WorkSpace またはディレクトリに参加している Amazon EC2インスタンスで WorkSpaces 、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト (フォレスト:) ***FQDN***を展開します。
3. [ドメイン] を展開します。
4. を展開します FQDN (例: `example.com`) 。
5. を選択しFQDN、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GPOで を作成するを選択し、ここでリンクします。
6. に という名前を付けます GPO (例: **`Office`**) 。
7. を選択しGPO、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いて編集を選択します。

8. グループポリシー管理エディタで、ローカルコンピュータ、Microsoft Office 2016、および言語設定から取得したユーザー設定、ポリシー、管理テンプレートポリシー定義 (ファイル) を選択します。 ADMX

   > **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)。ユーザー設定、ポリシーでローカルコンピュータから取得した管理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、`office16.admx`および `office16.adml` ファイルはドメインコントローラーに正しくインストールされません。

9. [言語設定] で、次の設定で使用する言語を指定します。各設定を [有効] に設定し、[オプション] で目的の言語を選択します。[OK] を選択して各設定を保存します。

   - [表示言語] > [ヘルプを表示]
   - [表示言語] > [メニューとダイアログボックスを表示]
   - [編集言語] > [主要編集言語]

10. 終了したら、グループポリシー管理ツールを閉じます。
11. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションの再開後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

オプション 3: の Office 言語レジストリ設定を更新する WorkSpaces

レジストリを使用して Office の言語設定を設定するには、次のレジストリ設定を更新します。

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\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 () を持つDWORDキー値を追加しますLCID。たとえば、英語 (米国) LCIDの は 1033 です。LCIDs は 10 進値であるため、DWORD値の Base オプションを 10 進数に設定する必要があります。Office のリストについてはLCIDs、Microsoft OptionState ドキュメントの「Office 2016 の言語識別子と ID 値」を参照してください。

これらのレジストリ設定は、GPO設定またはログオンスクリプト WorkSpaces を使用して に適用できます。

Office の言語設定の操作の詳細については、Microsoft のドキュメントの「Office の言語設定と設定をカスタマイズする」を参照してください。

既存の に Office を追加する BYOL WorkSpaces

また、次の手順BYOL WorkSpaces を実行して、Office へのサブスクリプションを既存の 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 にインストールして設定できます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace - Office がインストールされたBYOLバンドルをインストールしたら、WorkSpaces 移行機能を使用して、Office にサブスクライブしているBYOLバンドルBYOL WorkSpaces に既存の を移行できます。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。

> **Note**
>
> アプリケーション管理オプションは、Microsoft Office 2021 および Microsoft Visual Studio 2022、Microsoft Visio 2021、Microsoft Project 2021 などの他のアプリケーションを にインストールするために使用できます WorkSpaces。に Microsoft Office 2016 または 2019 をインストールするには WorkSpaces、 を使用しますPersonal WorkSpace で を移行する WorkSpaces 。

Microsoft Office のバージョン間で移行する

Microsoft Office の 1 つのバージョンを別のバージョンに移行する際には、次のオプションがあります。

- アプリケーションの管理 (推奨) – 元の Office バージョンをアンインストールし、Office 2021 および Microsoft Visual Studio 2022、Microsoft Visio 2021、Microsoft Project 2021 などの他のアプリケーションを既存の にインストールできます WorkSpaces。例えば、Microsoft Office 2019 から Microsoft Office 2021 に移行するには、アプリケーションの管理ワークフローを使用して Microsoft Office 2019 をアンインストールし、Microsoft Office 2021 をインストールします。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace – Microsoft Office 2016 から Microsoft Office 2019 または Microsoft Office 2019 から Microsoft Office 2016 に移行するには、移行先の Office のバージョンにサブスクライブされているBYOLバンドルを作成する必要があります。次に、 WorkSpaces 移行機能を使用して、Office にサブスクライブBYOL WorkSpaces している既存の を、移行先の Office にサブスクライブしているBYOLバンドルに移行します。例えば、Microsoft Office 2016 から Microsoft Office 2019 に移行するには、Microsoft Office 2019 にサブスクライブされているBYOLバンドルを作成します。次に、 WorkSpaces 移行機能を使用して、Office 2016 にサブスクライブBYOL WorkSpaces されている既存の を、Office 2019 にサブスクライブされているBYOLバンドルに移行します。詳細については、「 の移行 WorkSpace」を参照してください。

これらのオプションを使用して、 を介して Microsoft Office にサブスクライブ WorkSpaces されている AWS を Microsoft 365 アプリケーションに移行できます。ただし、アプリケーションの管理は、から Microsoft Office をアンインストールすることに限定されます WorkSpace。Microsoft 365 アプリケーションを にインストールするには、独自のツールとインストーラーを導入する必要があります WorkSpaces。

> **Note**
>
> 管理アプリケーションを使用すると、 に Microsoft Office、Microsoft Visio、または MicrosoftProject 2021 をインストールまたはアンインストールできます WorkSpaces。Microsoft Office 2016 または 2019 バージョンでは、 からのみ削除できます WorkSpaces。に Microsoft Office 2016 または 2019 をインストールするには WorkSpaces、を移行します WorkSpace。

移行プロセスの詳細については、Personal WorkSpace で を移行する WorkSpaces 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 Microsoft Visio や Microsoft Project などの他のアプリケーションを からアンインストールできます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。
- の移行 WorkSpace - Office にサブスクライブされていないBYOLバンドルを作成できます。次に、 WorkSpaces 移行機能を使用して、既存の を Office BYOL WorkSpaces 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、「Personal WorkSpace で を移行する WorkSpaces 」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 更新の一部として含まれます。すべてのセキュリティパッチと更新を最新の状態に保つために、BYOLベースイメージを定期的に更新することをお勧めします。

WorkSpaces コンソールを使用してBYOLイメージを作成する

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

> **Note**
>
> この手順を実行するには、以下を実行する AWS Identity and Access Management （ IAM) アクセス許可があることを確認します。
>
> - を呼び出します WorkSpaces **`ImportWorkspaceImage`**。
> - BYOL イメージの作成に使用する Amazon EC2イメージEC2**`DescribeImages`**で Amazon を呼び出します。
> - BYOL イメージの作成に使用する Amazon EC2イメージEC2**`ModifyImageAttribute`**で Amazon を呼び出します。Amazon EC2イメージの起動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全体で共有可能である必要があります。
>
> に固有のIAMポリシーの例についてはBYOL WorkSpaces、「」を参照してくださいの Identity and Access Management WorkSpaces。アクセスIAM許可の使用の詳細については、「 IAMユーザーガイド」の「 IAMユーザーのアクセス許可の変更」を参照してください。

イメージから Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または GraphicsPro バンドルを作成するには、 AWS Support センターに連絡して、アカウントを許可リストに追加してもらいます。アカウントが許可リストに登録されたら、 import-workspace-image コマンドを使用して AWS CLI Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または GraphicsPro 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [Images] を選択します。
3. BYOL イメージの作成 を選択します。
4. 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コンソールリンクを選択し、前のセクション () で説明したようにインポートした Amazon EC2イメージを選択しますのイメージを作成する準備EC2として、VM をBYOL イメージとして Amazon にインポートする WorkSpaces。イメージ名は で始まり、 の識別子が`ami-`続く必要があります AMI (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に応じて、適切なバンドルタイプ (通常、Graphics.g4dn、Graphics、または のいずれかGraphicsPro) PCoIPを選択しますDCV。GraphicsPro.g4dn バンドルを作成する場合は、Graphics.g4dn を選択します。バンドル (Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または 以外のバンドル GraphicsPro) の場合は non-GPU-enabled、Regular を選択します。

     Note
     - GraphicsPro イメージは、 PCoIPプロトコルに対してのみ作成できます。
     - Windows 11 イメージは、 DCVプロトコルに対してのみ作成できます。
     - Windows 11 では、グラフィックスと GraphicsPro イメージはサポートされていません。

- (オプション) [Select applications] (アプリケーションの選択) で、購読する Microsoft Office のバージョンを選択します。詳細については、「Amazon のBYOLイメージに Microsoft Office を追加する WorkSpaces」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. 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 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。

のBYOLイメージからカスタムバンドルを作成する WorkSpaces

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

BYOL イメージを使用する専用ディレクトリを作成する WorkSpaces

BYOL イメージを使用するには WorkSpaces、この目的のためにディレクトリを作成する必要があります。

のディレクトリを作成するには WorkSpaces、「」を参照してください WorkSpaces Personal のディレクトリを作成する。ディレクトリを作成するときは、必ず専有を有効にする WorkSpacesを選択してください。

専用ハードウェアで実行 WorkSpaces されない の AWS Managed Microsoft AD ディレクトリまたは AD Connector ディレクトリをすでに登録している場合は、この目的のために新しい AWS Managed Microsoft AD ディレクトリまたは AD Connector ディレクトリを設定できます。ディレクトリを登録解除し、専用ディレクトリとして再度登録することもできます WorkSpaces。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。

を起動する BYOL WorkSpaces

WorkSpaces 「」の手順に従って専用ディレクトリを登録したら 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 and WorkSpaces Pool を起動できます。

Personal を起動する BYOL WorkSpaces

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

BYOL WorkSpaces プールを起動する

WorkSpaces プールを起動するには、個人用を起動し WorkSpace、その個人用のイメージを作成してから WorkSpace、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 プールのイメージを作成するには

1. WorkSpaces プールに使用するBYOLイメージ WorkSpace で個人用 を起動します。WorkSpaces Personal を起動する方法については、「」を参照してください WorkSpaces Personal WorkSpace で を作成する。
2. 個人用にログイン WorkSpace し、すべての Windows 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。
3. Amazon EC2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、「 の最新バージョンをインストールするEC2Config」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、「 の最新バージョンをインストールするEC2Launch」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. を再起動します WorkSpace。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 プールのイメージの作成を開始する前に、次の操作を行う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、「」を参照してください WorkSpaces Personal 用のカスタム WorkSpaces イメージとバンドルを作成する。

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. すべてのテストがイメージチェッカーに合格したら、 WorkSpaces コンソールに戻ります。
10. ナビゲーションペインで、Personal WorkSpacesを選択します。BYOL 個人を選択し WorkSpaces、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。

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

BYOL イメージのアップロードと作成に関する動画

BYOL イメージのアップロードのデモンストレーションについては、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デモンストレーションについては、次の動画をご覧ください。

のBYOLアカウントをリンクする WorkSpaces

BYOL リンクを使用してアカウントをリンクし、BYOL設定を共有できます。 BYOL設定には、アカウントで使用されるCIDR範囲と、Windows ライセンス WorkSpaces での作成に使用するイメージが含まれます。リンクされ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**
>
> APIs BYOLアカウントリンクの は、 では使用できません AWS GovCloud (US) Region。

> **Note**
>
> にリンクする 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. 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 CreateAccountLinkInvitationAPI。
2. を使用して、ターゲットアカウントからの保留中のリンクを受け入れます AcceptAccountLinkInvitationAPI。
3. GetAccountLink または を使用して、リンクが確立されていることを確認しますListAccountLinksAPI。

WorkSpaces Personal の使用と管理

WorkSpaces Personal 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、専用にプロビジョニングされた高度にパーソナライズされたデスクトップを必要とするユーザー向けにカスタマイズされた永続的な仮想デスクトップを提供します。

各 WorkSpace は、仮想プライベートクラウド (VPC) と、 WorkSpaces および ユーザーの情報を保存および管理するためのディレクトリに関連付けられています。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 サービスによって管理されるか AWS Directory Service、または AWS Managed Microsoft AD とも呼ばれる 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。

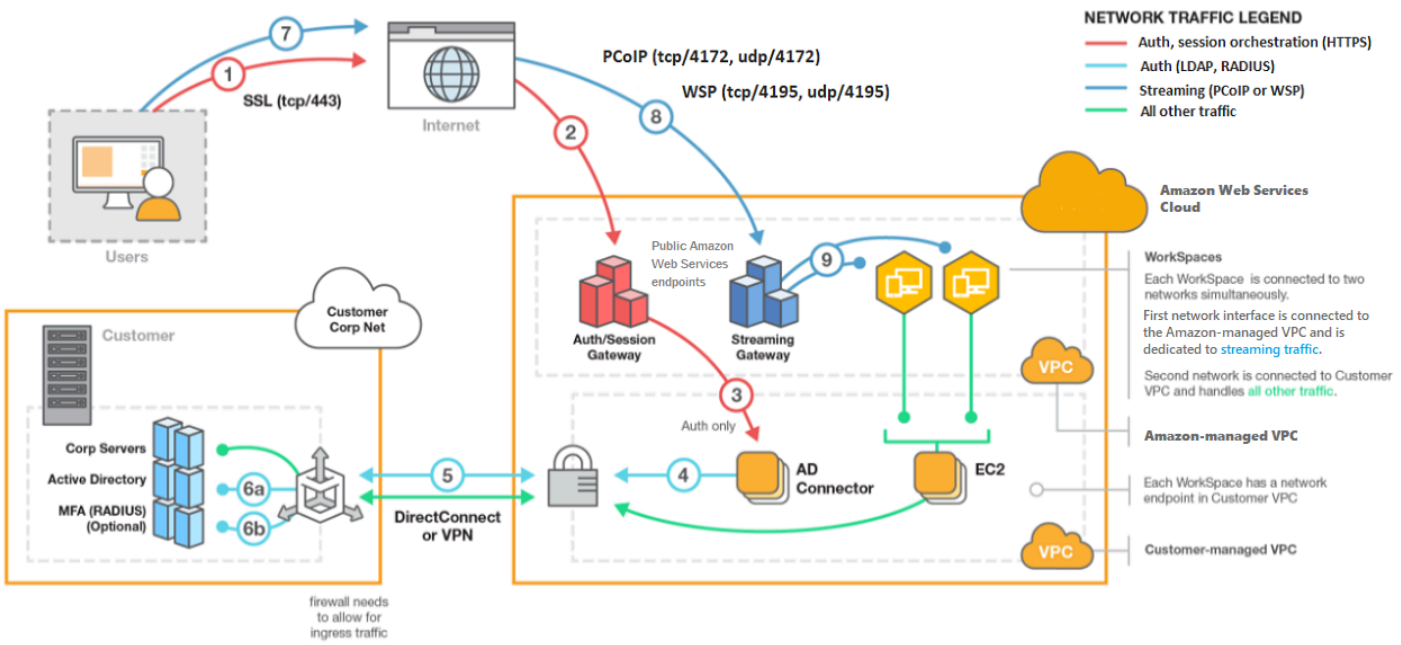
WorkSpaces は、IAMIdentity Center (Amazon が管理するディレクトリ用 WorkSpaces) 、Simple AD、AD Connector、または AWS Managed Microsoft AD ディレクトリを使用してユーザーを認証します。ユーザーは、サポートされているデバイスからクライアントアプリケーション WorkSpaces を使用するか、Windows の場合はウェブブラウザを使用して WorkSpacesにアクセスし、ディレクトリ認証情報を使用してログインします。ログイン情報は認証ゲートウェイに送信され、認証ゲートウェイはトラフィックを の デ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

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

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

次の図は、AD Connector WorkSpaces を使用する のアーキテクチャを示しています。

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 で 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
- AWS Managed Microsoft AD ディレクトリと WorkSpaces Personal のオンプレミスドメインの間に信頼関係を作成する
- WorkSpaces Personal を使用して専用の 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

初めて WorkSpaces 使用するユーザーとして、クイックセットアップまたは高度なセットアップで WorkSpaces Personal をセットアップできます。以下のチュートリアルでは、 WorkSpaces および WorkSpaceを使用して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 AWS Directory Service。

> **Note**
>
> WorkSpaces プールの使用を開始するには、「」を参照してください2.0 SAML を設定し、WorkSpaces プールディレクトリを作成する。

WorkSpaces 個人用のクイックセットアップ

このチュートリアルでは、 WorkSpaces および を使用して、 と呼ばれる仮想クラウドベースの Microsoft Windows、Amazon Linux 2、Ubuntu Linux、Rocky LinuxWorkSpace、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、クイックセットアップオプションを使用して を起動します WorkSpace。このオプションは、 を起動したことがない場合にのみ使用できます WorkSpace。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**
>
> このクイックセットアップオプションとチュートリアルは WorkSpaces プール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
- Quick Setup の機能
- ステップ 1: を起動する WorkSpace
- ステップ 2: WorkSpace に接続する
- ステップ 3: クリーンアップする (オプション)
- 次のステップ

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。

- を作成または管理する AWS アカウントが必要です WorkSpace。ユーザーは、 に接続して使用するために AWS アカウントを必要としません WorkSpaces。
- 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、 のリージョンを選択します WorkSpaces。サポートされているリージョンの詳細については、WorkSpaces AWS 「リージョン別の料金表」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。

- を起動するときは WorkSpace、 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 Bundles」と「Amazon WorkSpaces 料金表」を参照してください。
- を起動するときは WorkSpace、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。
- を起動するときは WorkSpace、ユーザー名や E メールアドレスなど、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。 WorkSpaces および ユーザーに関する情報は、 ディレクトリに保存されます。詳細については、「the section called “のディレクトリを管理する WorkSpaces”」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。VPC 代わりに既存の を使用する場合は、 に記載されている要件を満たしていることを確認しVPC WorkSpaces 個人用の を設定する、 に記載されているチュートリアルのいずれかの手順に従います WorkSpaces Personal のディレクトリを作成する。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。
- で Simple AD ディレクトリを設定しVPC、Amazon で有効にします WorkDocs。この Simple AD ディレクトリは、ユーザーと WorkSpace 情報を保存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。
- を作成します WorkSpaces。各 WorkSpace は、インターネットアクセスを提供するパブリック IP アドレスを受け取ります。実行モードは です AlwaysOn。詳細については、「 WorkSpaces Personal で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。

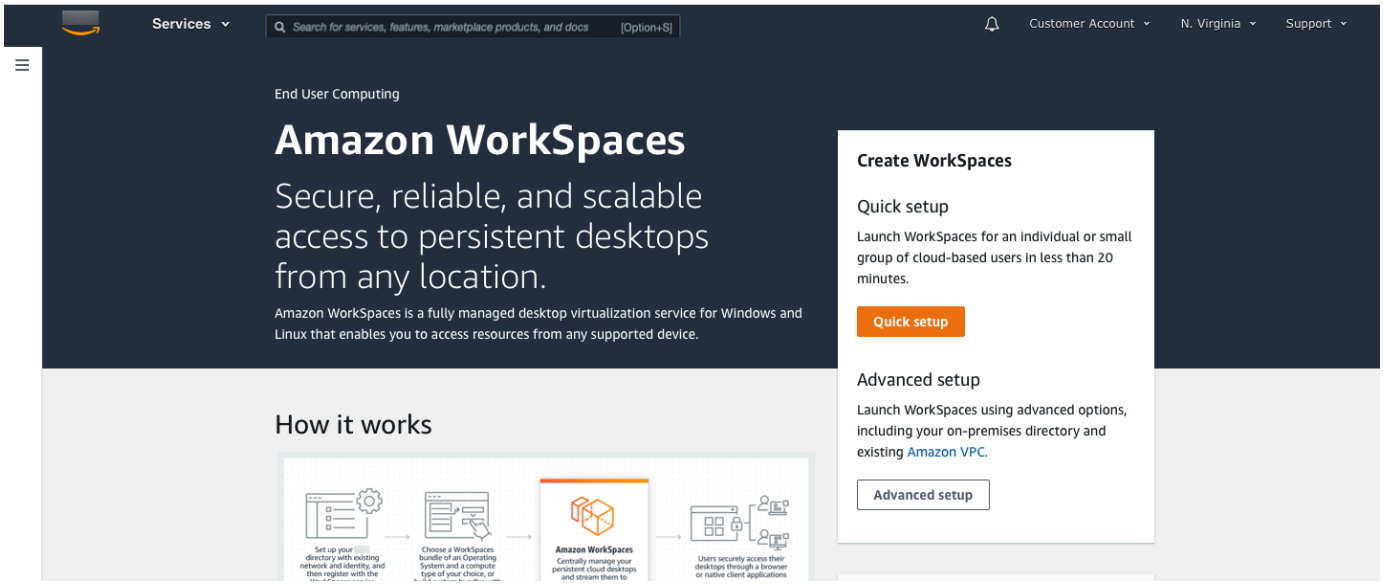
† クイックセットアップによって最初に AWS アカウント 作成されるのは管理者 です AWS アカウント。 WorkSpaces コンソール AWS アカウント から更新することはできません。このアカウントの情報は、他の誰とも共有しないでください。他のユーザーに使用を招待するには WorkSpaces、新しいユーザーを作成します AWS アカウント 。

ステップ 1: を起動する WorkSpace

クイックセットアップを使用すると、最初の を数分 WorkSpace で起動できます。

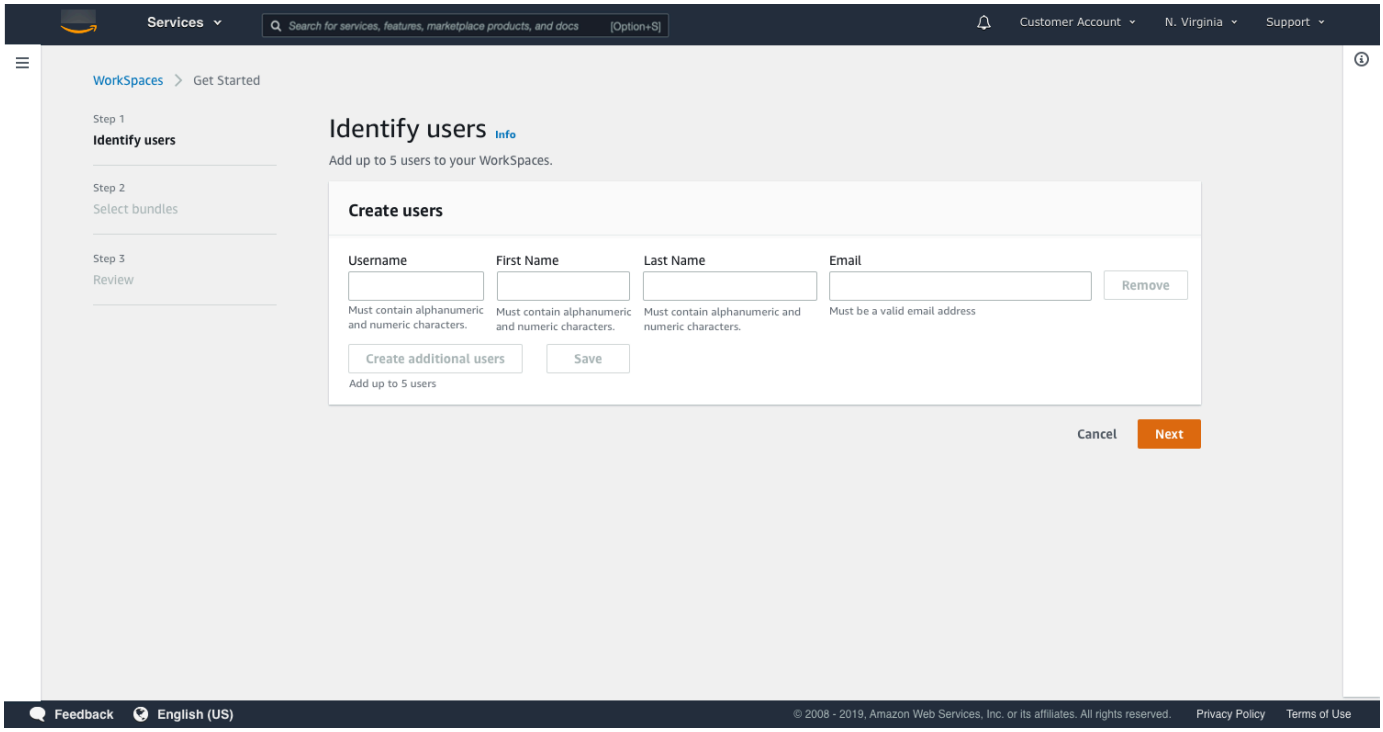
を起動するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. [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 WorkSpace で をすでに起動しているか、クイックセットアップをサポートするリージョンの 1 つを使用していません。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。

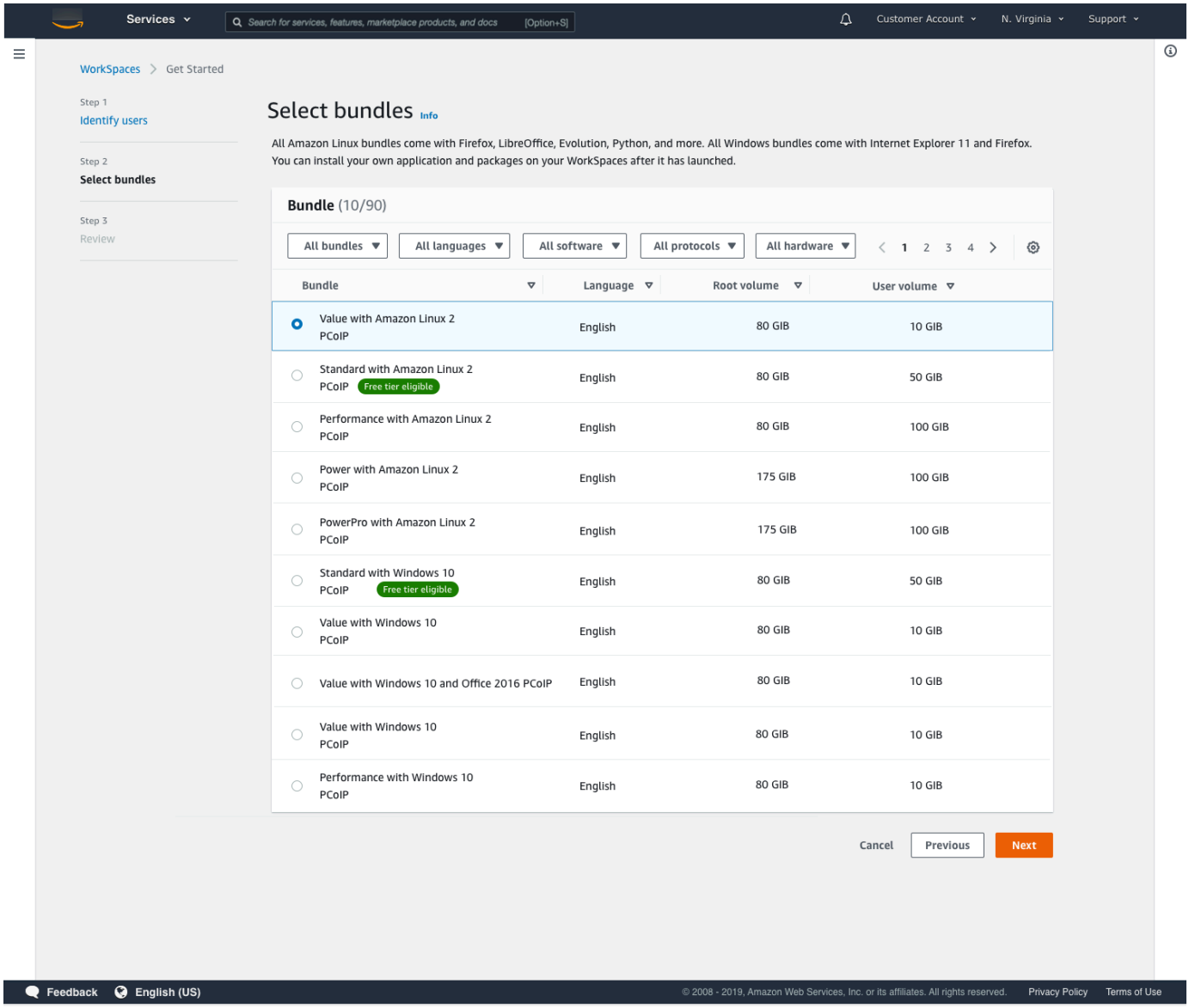


3. [Identify users] (ユーザーの識別) に [Username] (ユーザー名) と [First Name] (名前) を入力します。[Last Name] (姓) および [Emai] (E メール)。次いで、[次へ] を選択します。

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



4. バンドルでは、適切なプロトコル (または) を持つユーザーのバンドル (PCoIPハードウェアとソフトウェア) を選択しますDCV。Amazon で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。



5. 情報を確認します。次に [作成] WorkSpace を選択します。
6. の起動 WorkSpace には約 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 になったらACTIVE、左側のナビゲーションペインWorkSpacesで を選択して起動プロセスの進行 WorkSpace状況をモニタリングできます。の初期ステータスは WorkSpace ですPENDING。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

招待メールを受信したら、選択したクライアント WorkSpace を使用して に接続できます。サインインすると、クライアントに WorkSpaceデスクトップが表示されます。

に接続するには WorkSpace

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。への接続に必要なため、指定したパスワードを覚えておいてください WorkSpace。

   > **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WorkSpaces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「クライアント」を確認し、次のいずれかを実行します。

   - 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、クライアントアプリケーションをまだインストールしていない場合は、https://clients.amazonworkspaces.com/ を開いて、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。

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

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。

マルチモニターの設定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の詳細については、WorkSpaces 「Amazon ユーザーガイド」の「クライアントと周辺機器のサポート」を参照してください。 WorkSpaces

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 WorkSpace 作成した を使い終わったら、削除できます。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、 で無料で使用できます WorkSpaces。Simple AD ディレクトリで 30 日間連続して使用 WorkSpaces されていない場合、このディレクトリは Amazon で使用するために自動的に登録解除され WorkSpaces、AWS Directory Service 料金条件に従ってこのディレクトリに対して課金されます。
> 空のディレクトリを削除するには、 WorkSpaces Personal の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すると、 WorkSpaces の使用を再開するときに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

WorkSpace 先ほど作成した 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、 からカスタムバンドルを作成できます WorkSpace。また、 と WorkSpaces ディレクトリに対して WorkSpaces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 用のカスタム WorkSpaces イメージとバンドルを作成する
- WorkSpaces 個人用の管理
- WorkSpaces Personal のディレクトリを管理する

追加の を作成するには WorkSpaces、次のいずれかを実行します。

- クイックセットアップで作成された VPCと Simple AD ディレクトリを引き続き使用する場合は、「Simple AD WorkSpace の使用 WorkSpaces 」チュートリアルの WorkSpaces Personal WorkSpace で を作成する「」セクションの手順に従って、追加のユーザーを追加できます。
- 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。

マルチモニターの設定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の詳細については、WorkSpaces 「Amazon ユーザーガイド」の「クライアントと周辺機器のサポート」を参照してください。 WorkSpaces

WorkSpaces 個人用の高度なセットアップの使用を開始する

このチュートリアルでは、 WorkSpaces および を使用して、 と呼ばれる仮想クラウドベースの Microsoft Windows、Amazon Linux、Ubuntu LinuxWorkSpace、または Red Hat Enterprise Linux デスクトップ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、高度なセットアップオプションを使用して を起動します WorkSpace。

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

タスク

- [開始する前に]
- の詳細設定を使用した の起動 WorkSpace

[開始する前に]

開始する前に、 を作成または管理するために使用できる AWS アカウントがあることを確認してください WorkSpace。ユーザーは、 に接続して使用するために AWS アカウントを必要としません WorkSpaces。

以下の概念を確認してから作業を進めてください。

- を起動するときは WorkSpace、 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 Bundles」を参照してください。
- を起動するときは WorkSpace、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。
- を起動するときは WorkSpace、ユーザー名や E メールアドレスなど、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。 WorkSpaces および ユーザーに関する情報は、 ディレクトリに保存されます。詳細については、「the section called “のディレクトリを管理する WorkSpaces”」を参照してください。

の詳細設定を使用した の起動 WorkSpace

詳細設定を使用して を起動するには WorkSpace：

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. 次のいずれかのディレクトリタイプを選択してから、[Next] (次へ) をクリックします。
   - AWS Managed Microsoft AD
   - Simple AD
   - AD Connector
3. ディレクトリ情報の入力
4. 2 つの異なるアベイラビリティーゾーンVPCから 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VPCで を設定する」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 WorkSpace で を作成する

WorkSpaces では、 と呼ばれる、ユーザー向けの仮想クラウドベースの Windows および Linux デスクトップをプロビジョニングできますWorkSpaces。

個人用を作成する前に WorkSpace、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 ID ソースとして使用する専用ディレクトリを (IAM Identity Center を介して) 作成します。ディレクトリ WorkSpaces 内の は、ネイティブの Entra ID 結合であり、Microsoft Windows Autopilot ユーザー駆動モードを介して 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 Bring Your Own Licenses Personal のみをサポートしています WorkSpaces。

- 任意の ID プロバイダーを ID ソースとして使用する専用ディレクトリを (IAM Identity Center を介して) 作成します。ディレクトリ WorkSpaces 内の は、ネイティブの Entra ID 結合であり、Microsoft Windows Autopilot ユーザー駆動モードを介して 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 Bring Your Own Licenses Personal のみをサポートしています WorkSpaces。

ディレクトリを作成したので、個人用を作成する準備が整いました WorkSpace。

個人を作成するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. 起動 WorkSpaces、個人用 を選択します。
4. 作成 WorkSpacesを選択します。
5. オンボーディング (オプション) で、ユースケースに基づいてレコメンデーションオプションを選択して、 WorkSpace 使用する のタイプに関するレコメンデーションを取得できます。個人用の使用がわかっている場合は、このステップをスキップできます WorkSpaces。
6. Next. WorkSpaces registers your AD Connector を選択します。
7. 設定 WorkSpaces で、次の詳細を入力します。

    - バンドル で、使用するバンドルタイプを以下から選択します WorkSpaces。
        - ベース WorkSpaces バンドルを使用する - ドロップダウンからバンドルのいずれかを選択します。選択したバンドルタイプの詳細を確認するには、[バンドルの詳細] を選択します。プールに提供されるバンドルを比較するには、[すべてのバンドルを比較] を選択します。
        - 独自のカスタムまたはBYOLバンドルを使用する - 以前に作成したバンドルを選択します。カスタムバンドルを作成するには、「WorkSpaces Personal 用のカスタム 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 Bundles」を参照してください。バンドルの仕様、推奨用途、料金の詳細については、「Amazon WorkSpaces の料金」を参照してください。

- 実行モードでは、以下から選択して、個人の WorkSpace即時可用性とその支払い方法 (月単位または時間単位) を設定します。
  - AlwaysOn — の無制限の使用に対して月額料金を請求します WorkSpaces。このモードは、プライマリデスクトップとして WorkSpace フルタイムを使用するユーザーに最適です。
  - AutoStop — 時間単位の請求。このモードでは、指定した切断期間が経過すると が WorkSpaces 停止し、アプリケーションとデータの状態が保存されます。
- [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 WorkSpaces を実行して、個人用にプロビジョニングするディレクトリからユーザーを選択します。

     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. 作成 を選択します WorkSpaces。の初期ステータスは WorkSpace ですPENDING。作成が完了すると、ステータスは AVAILABLEになり、ユーザーに指定した E メールアドレスに招待が送信されます。
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

に接続する WorkSpace

選択したクライアント WorkSpace を使用して に接続できます。サインインすると、クライアントに WorkSpace デスクトップが表示されます。

に接続するには WorkSpace

1. 招待メールでリンクを開きます。
2. 各WorkSpaces 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「クライアント」を確認し、次のいずれかを実行します。
   - 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、クライアントアプリケーションがまだインストールされていない場合は、https://clients.amazonworkspaces.com/ を開いて、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。

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

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。（ WorkSpaces クライアントアプリケーションのログイン画面のパスワードを忘れた場合？ オプションは使用できません。）ユーザーパスワードをリセットする方法については、WorkSpaces 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

WorkSpace 先ほど作成した 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、 からカスタムバンドルを作成できます WorkSpace。また、 WorkSpaces と 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。の使用が終了したら WorkSpace、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 用のカスタム WorkSpaces イメージとバンドルを作成する
- WorkSpaces 個人用の管理
- WorkSpaces Personal のディレクトリを管理する
- WorkSpaces Personal で WorkSpace を削除する

マルチモニターの設定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の詳細については、WorkSpaces 「Amazon ユーザーガイド」の「クライアントと周辺機器のサポート」を参照してください。 WorkSpaces

WorkSpaces Personal のネットワークプロトコルとアクセス

WorkSpace 管理者は、プロトコルから始めてネットワーク WorkSpaces とアクセスを管理する方法を理解する必要があります。

WorkSpaces Personal のプロトコル

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

要件

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

ホストエージェントの要件:

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

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

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、世界中の距離 WorkSpaces にわたって にアクセスするユーザーや、信頼できないネットワークを使用しているユーザーがいます。

- ユーザーがスマートカードで認証したり、セッション内でスマートカードを使用したりする必要がある場合。
- セッション内でウェブカメラサポート機能が必要な場合。
- Windows Server 2022 搭載 WorkSpaces バンドルで Web Access を使用する必要がある場合。
- Ubuntu を使用する必要がある場合 WorkSpaces。
- Windows 11 を使用する必要がある場合BYOL WorkSpaces。
- Windows または Ubuntu GPUベースのバンドル (Graphics.g4dn および GraphicsPro.g4dn) を使用する必要がある場合。
- ユーザーが、 YubiKey や Windows Hello などの WebAuthn 認証プログラムを使用してセッション内の認証を行う必要がある場合。

PCoIP を使用する場合

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

> **Note**
>
> - ディレクトリには、 PCoIPと を混在DCV WorkSpaces させることができます。
> - ユーザーは、2 つの WorkSpaces が別々のディレクトリにあるDCV WorkSpace 限り、 PCoIPと の両方を持つことができます。同じユーザーが同じディレクトリDCV WorkSpace に PCoIPと を持つことはできません。ユーザー用に複数の を作成する方法の詳細については、 WorkSpaces 「」を参照してください WorkSpaces Personal でユーザー WorkSpaces 用に複数の を作成する。
> - 2 つのプロトコル WorkSpace 間で を移行するには、 の再構築が必要な WorkSpaces 移行機能を使用します WorkSpace。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。

- WorkSpace がPCoIPバンドルで作成された場合は、ルートボリュームを維持しながら、再ビルドを必要とせずに 2 つのプロトコル間で移行するようにストリーミングプロトコルを変更できます。詳細については、「プロトコルの変更」を参照してください。
- ビデオ会議を最大限に活用するには、Power または PowerPro バンドルのみを使用することをお勧めします。

以下のトピックでは、 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。

VPC WorkSpaces 個人用の を設定する

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

の 2 つのプライベートサブネット WorkSpaces とパブリックサブネットのNATゲートウェイVPCを持つ を作成できます。または、 用に 2 つのパブリックサブネットVPCを持つ を作成し WorkSpaces 、それぞれにパブリック IP アドレスまたは Elastic IP アドレスを関連付けることができます WorkSpace。

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

内容

- 要件
- プライベートサブネットとNATゲートウェイVPCを使用して を設定する
- パブリックサブネットVPCを使用して を設定する

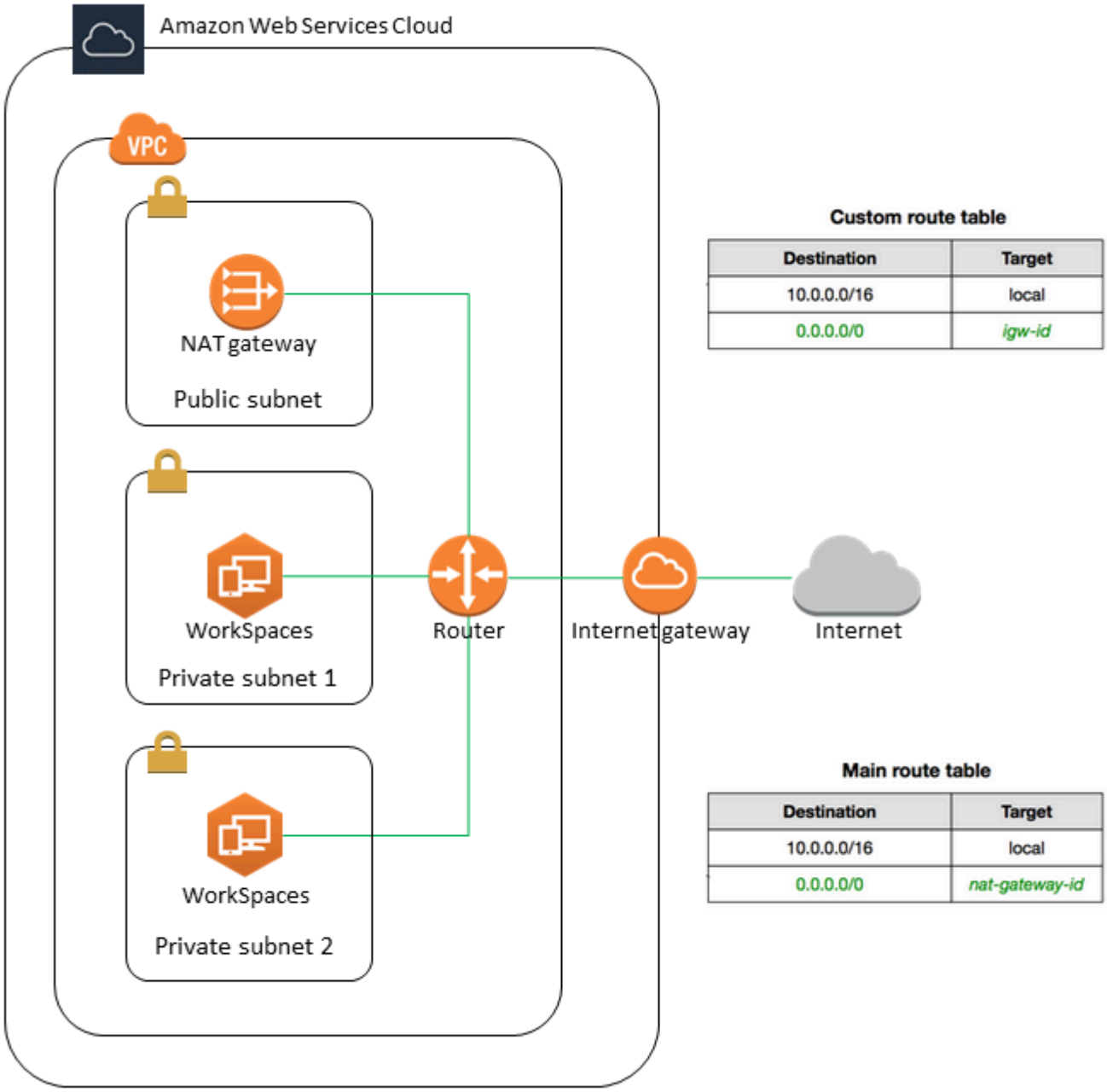
要件

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

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

プライベートサブネットとNATゲートウェイVPCを使用して 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VPCで を設定することをお勧めします。プライベートサブネットで WorkSpaces を起動するようにディレクトリを設定します。プライベートサブネット WorkSpaces で へのインターネットアクセスを提供するには、パブリックサブネットでNATゲートウェイを設定します。



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

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. [作成]VPC を選択します。
3. 作成するリソースで、 VPC などを選択します。
4. 名前タグの自動生成には、 の名前を入力しますVPC。

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. カスタマイズAZs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. NAT ゲートウェイの場合は、AZ ごとに 1 を選択します。
7. [作成]VPC を選択します。

IPv6 CIDR ブロック

IPv6 CIDR ブロックを VPCおよび 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、Graphics バンドルを使用することはできません。(ただし、Graphics.g4dn、GraphicsPro.g4dn、および GraphicsPro バンドルを使用できます)。この制限は、 をサポートしてい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IPv6。

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

デフォルトでは、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VPCを使用して を設定する

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

タスク

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

ステップ 1: を作成する VPC

次のように 1 つのパブリックサブネットVPCを持つ を作成します。

VPC を作成するには

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. [作成]VPC を選択します。
3. 作成するリソースで、 VPC などを選択します。
4. 名前タグの自動生成には、 の名前を入力しますVPC。
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. カスタマイズAZs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. [作成]VPC を選択します。

IPv6 CIDR ブロック

IPv6 CIDR ブロックを VPCおよび 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、Graphics バンドルを使用することはできません。(ただし、 GraphicsPro バンドルは使用できます)。この制限は、 をサポートしてい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IPv6。

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

デフォルトでは、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サブネットを選択します。サブネットを選択し、[アクション]、[自動割り当て IP 設定の変更] の順に選択します。

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

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

にパブリック IP アドレス WorkSpace を手動で割り当てるには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. の行を展開 WorkSpace し (矢印アイコンを選択) 、WorkSpace IP の値を書き留めます。これは、 のプライマリプライベート IP アドレスです WorkSpace。
4. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
5. ナビゲーションペインで、Elastic IPsを選択します。使用可能な Elastic IP アドレスがない場合は、Elastic IP アドレスの割り当て を選択し、Amazon のIPv4アドレスプールまたはカスタマー所有のIPv4アドレスプールを選択してから、割り当て を選択します。新しい IP アドレスを書き留めます。
6. ナビゲーションペインで、[ネットワークインターフェイス] を選択します。
7. のネットワークインターフェイスを選択します WorkSpace。のネットワークインターフェイスを検索するには WorkSpace、検索ボックスに WorkSpace IP 値 (前に書き留めた値) を入力し、Enter キーを押します。WorkSpace IP 値は、ネットワークインターフェイスのプライマリプライベートIPv4アドレスと一致します。ネットワークインターフェイスの VPC ID は、 の ID と一致することに注意してください WorkSpaces VPC。
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。

Personal の AWS Global Accelerator (AGA) WorkSpaces を設定する

AWS Global Accelerator (AGA) は、 WorkSpaces ディレクトリレベルまたは個々の WorkSpaces 実行中のDCVプロトコルで有効にできます。有利な場合、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に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、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。この WorkSpaces サービスはAGA使用状況を完全に管理し、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
- 制限
- アウトバウンドデータの制限
- WorkSpaces ディレクトリAGAの を有効にする
- 個々の AGAに対して を有効にする WorkSpaces

要件

- WorkSpaces は、専用の AWS Global Accelerator (AGA) エンドポイントのパブリックIPv4アドレスの範囲を使用します。 WorkSpaces を介して 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設定してくださいAGA。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 経由でルーティングされませんAGA。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。
- WorkSpaces を介して にアクセスするにはAGA、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

- は AGAに対してDCV WorkSpaces のみ有効にできます。AGA WorkSpaces ディレクトリレベルで を有効にすると、 ディレクトリDCV WorkSpaces の 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 WorkSpaces 内の) AGAに対して を有効にすることはできません。ディレクトリAGAの 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

以下は、 WorkSpaces バンドルに適用されるデータボリュームの制限です。

- 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、 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 WorkSpaces。制限を超えると、 WorkSpaces サービスはAGA使用量を制限し、 WorkSpaces トラフィックを AGA case-by-caseからルーティングする可能性があります。

WorkSpaces ディレクトリAGAの を有効にする

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

ディレクトリAGAに対して を有効にするには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリ ID 列で、AGA設定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スクロールし、編集を選択します。
5. 有効 AGA (自動 ） を選択します。
6. デフォルトでは、 TCPで常に AGA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AGAに基づいて、 TCPまたは UDP がで使用されているかどうかを判断します。
7. [Save] を選択します。

WorkSpaces ディレクトリAGAに対して を有効にした後、 ディレクトリDCV WorkSpaces で、次のセッションから開始するストリーミングAGAに を使用します。再起動は必要ありません。

個々の AGAに対して を有効にする WorkSpaces

個々の AGAの設定を設定できます。これにより WorkSpaces、 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 AGAに対して を有効にするには WorkSpaces

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces、Personal を選択します。
3. WorkSpace ID 列で、AGA設定 WorkSpace する の WorkSpace ID を選択します。
4. WorkSpaces 詳細ページで、 AWS Global Accelerator (AGA) 設定セクションまでスクロールし、編集を選択します。
5. これの設定を手動で上書きAGAするを選択します WorkSpace。
6. 有効 AGA (自動) を選択します。
7. デフォルトでは、 TCPで常に AGA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AGAに基づいて、 TCPまたは UDP がで使用されているかどうかを判断します。
8. [Save] 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複数のアベイラビリティーゾーンに分散されるようにするために、アベイラビリティーゾーンは各 AWS アカウントの名前に個別にマッピングされます。例えば、AWS アカウントのアベイラビリティーゾーン us-east-1a の場所は、別の AWS アカウントの us-east-1a の場所と異なる可能性があります。

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

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
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

リージョン名	リージョンコード	サポートされる AZ ID
欧州 (アイルランド)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
欧州 (ロンドン)	eu-west-2	euw2-az2, euw2-az3
南米 (サンパウロ)	sa-east-1	sae1-az1, sae1-az3
アフリカ (ケープタウン)	af-south-1	afs1-az1, afs1-az2, afs1-az3
イスラエル (テルアビブ)	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
AWS GovCloud (米国西部)	us-gov-west-1	usgw1-az1 , usgw1-az2 , usgw1-az3
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

に接続するには WorkSpaces、 WorkSpaces クライアントが接続されているネットワークで、さまざまな AWS のサービス (サブセットにグループ化) の IP アドレス範囲に対して特定のポートが開いている必要があります。これらのアドレス範囲は AWS リージョン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 をデプロイするためのベストプラクティス WorkSpaces」を参照してください。

クライアントアプリケーションのポート

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

ポート 53 (UDP)

このポートはサーバーへのアクセスに使用されますDNS。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 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 および 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。
- があるリージョンのAMAZONサブセット WorkSpace 。
- 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 および TCP)

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

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

ポート 4195 (UDP および TCP)

このポートは、 の WorkSpace デスクトップおよびヘルスチェックのストリーミングに使用されますDCV WorkSpaces。このポートは、 があるリージョンのDCVゲートウェイ IP アドレス

範囲とヘルスチェックサーバーに対して開いている必要があります WorkSpace 。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。

ではDCV WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) はポート 4195 TCP トラフィックのHTTPプロキシサーバーの使用をサポートしていますが、プロキシの使用は推奨されません。 の復TLS号化と検査はサポートされていません。詳細については、「Windows WorkSpaces、Amazon Linux WorkSpaces、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。
- プロキシサーバー関数はUDPトラフィックではサポートされていません。プロキシサーバーを使用することを選択した場合、クライアントアプリケーションが Amazon WorkSpaces サービスに対して行うAPI呼び出しもプロキシされます。API 呼び出し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 のみを許可する場合TCP、 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 には、次のポートへのアウトバウンドアクセスが必要です。

ポート 53 (UDP)

このポートはサーバーへのアクセスに使用されますDNS。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 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 および TCP)

このポートは、 への初期接続に使用されhttps://clients.amazonworkspaces.com、その後 に切り替わりますHTTPS。 WorkSpace が属するリージョンのEC2サブセット内のすべての IP アドレス範囲に対して開いている必要があります。

ポート 443 (UDP および TCP)

このポートは、 を使用した登録と認証に使用されますHTTPS。 WorkSpace が属するリージョンのEC2サブセット内のすべての IP アドレス範囲に対して開かれている必要があります。

ポート 4195 (UDP および TCP)

用に WorkSpaces 設定された の場合DCV、このポートは WorkSpaces デスクトップトラフィックのストリーミングに使用されます。このポートは、DCVゲートウェイ IP アドレス範囲に対して開いている必要があります。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 ウェブアクセスは、ポート 4195 TCPトラフィックの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 のみを許可する場合TCP、 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、ウェブブラウザはトラフィックのストリーミングに使用する高範囲のソースポートをランダムに選択します。 WorkSpaces ウェブアクセスは、ブラウザが選択するポートを制御できません。このポートへのリターントラフィックが許可されていることを確認する必要があります。

許可リストに追加するドメインと IP アドレス

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

許可リストに追加するドメインと IP アドレス

カテゴリ	ドメインまたは IP アドレス
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	• https://d2td7dqidlhjx7.cloudfront.net/ • AWS GovCloud （ 米国西部) リージョンの場合 : https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/WorkSpacesAppCastx64.xml
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com

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

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

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

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

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

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

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

カテゴリ	ドメインまたは IP アドレス
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 • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin.amazonaws-us-gov.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン) (AWS GovCloud 米国西部) および AWS GovCloud (米国東部) リージョンの場合 : https://login.us-gov-home.awsapps.com/directory/<directory id>/ (<directory id> はお客様のドメインです)

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

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

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

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

カテゴリ	ドメインまたは IP アドレス
WorkSpaces SAML シングルサインオンのエンドポイント (SSO)	ドメイン: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.us-west-2.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.af-south-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.il-central-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/ハートビートのレポート

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/ハートビートのレポート • https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/ハートビートのレポート • https://euc-sso-sm-fips.us-gov-east-1.amazonaws.com/v1/ハートビートのレポート

の許可リストに追加するドメインと IP アドレス PCoIP

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

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

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

の許可リストに追加するドメインと IP アドレス DCV

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

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

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

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

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

PCoIP ゲートウェイサーバー

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

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

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

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

DCV ゲートウェイサーバー

Important

2020 年 6 月以降、 はポート 4172 ではなくポート 4195 経由で のデスクトップセッションをクライアントDCV WorkSpacesに WorkSpaces ストリーミングします。を使用する場合はDCV WorkSpaces、ポート 4195 がトラフィックに対して開いていることを確認してください。

Note

以下の IP アドレス範囲の一部はBYOL WorkSpaces 、プール以外の ではサポートされていない場合があります。

WorkSpaces は、DCVゲートウェイサーバーに少数の Amazon EC2パブリックIPv4アドレスを使用します。これにより、 にアクセスするデバイスに対して、よりきめ細かなファイアウォールポリシーを設定できます WorkSpaces。 は、専用の AWS Global Accelerator (AGA) エンドポイントに別のパブリックIPv4アドレス範囲 WorkSpaces を使用します。AGA で 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 WorkSpaces。現時点では、 WorkSpaces クライアントは接続オプションとしてIPv6アドレスをサポートしていないことに注意してください。

リージョン	パブリック IP アドレス範囲
米国東部 (バージニア北部)	• 3.227.4.0/22

リージョン	パブリック IP アドレス範囲
	• 44.209.84.0/22 • 93.77.138.0/24 (AGA エンドポイント) • 93.77.139.0/24 (AGA エンドポイント)
米国東部 (オハイオ)	• 3.146.84.0/22 • 93.77.130.0/24 (AGA エンドポイント) • 93.77.131.0/24 (AGA エンドポイント)
米国西部 (オレゴン)	• 34.223.96.0/22 • 93.77.148.0/24 (AGA エンドポイント) • 93.77.149.0/24 (AGA エンドポイント)
アジアパシフィック (ムンバイ)	• 65.1.156.0/22 • 93.77.142.0/24 (AGA エンドポイント) • 93.77.143.0/24 (AGA エンドポイント)
アジアパシフィック (ソウル)	• 3.35.160.0/22 • 93.77.156.0/24 (AGA エンドポイント) • 93.77.157.0/24 (AGA エンドポイント)
アジアパシフィック (シンガポール)	• 13.212.132.0/22 • 93.77.158.0/24 (AGA エンドポイント) • 93.77.159.0/24 (AGA エンドポイント)
アジアパシフィック (シドニー)	• 3.25.248.0/22 • 93.77.150.0/24 (AGA エンドポイント) • 93.77.151.0/24 (AGA エンドポイント)
アジアパシフィック (東京)	• 3.114.164.0/22 • 93.77.134.0/24 (AGA エンドポイント) • 93.77.135.0/24 (AGA エンドポイント)

リージョン	パブリック IP アドレス範囲
カナダ (中部)	• 3.97.20.0/22 • 93.77.128.0/24 (AGA エンドポイント) • 93.77.129.0/24 (AGA エンドポイント)
欧州 (フランクフルト)	• 18.192.216.0/22 • 93.77.154.0/24 (AGA エンドポイント) • 93.77.155.0/24 (AGA エンドポイント)
欧州 (アイルランド)	• 3.248.176.0/22 • 93.77.132.0/24 (AGA エンドポイント) • 93.77.133.0/24 (AGA エンドポイント)
欧州 (ロンドン)	• 18.134.68.0/22 • 93.77.140.0/24 (AGA エンドポイント) • 93.77.141.0/24 (AGA エンドポイント)
欧州 (パリ)	• 51.44.72.0/22 • 93.77.144.0/24 (AGA エンドポイント) • 93.77.145.0/24 (AGA エンドポイント)
南米 (サンパウロ)	• 15.228.64.0/22 • 93.77.146.0/24 (AGA エンドポイント) • 93.77.147.0/24 (AGA エンドポイント)
アフリカ (ケープタウン)	• 13.246.108.0/22 • 93.77.136.0/24 (AGA エンドポイント) • 93.77.137.0/24 (AGA エンドポイント)
イスラエル (テルアビブ)	• 51.17.72.0/22 • 93.77.152.0/24 (AGA エンドポイント) • 93.77.153.0/24 (AGA エンドポイント)

リージョン	パブリック IP アドレス範囲
AWS GovCloud（米国西部）	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud（米国東部）	18.254.148.0/22

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。これらのドメインは、WorkSpaces クライアントアプリケーションがサービスにアクセスできる WorkSpace DCVように、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 • （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 • （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

リージョン	分野
欧州 (アイルランド)	*.prod.eu-west-1.highlander.aws.a2z.com
欧州 (ロンドン)	*.prod.eu-west-2.highlander.aws.a2z.com
南米 (サンパウロ)	*.prod.sa-east-1.highlander.aws.a2z.com
アフリカ (ケープタウン)	*.prod.af-south-1.highlander.aws.a2z.com
イスラエル (テルアビブ)	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud （米国西部）	• *.prod.us-gov-west-1.highlander.aws.a2z.com • （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 • （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 には、次のネットワークインターフェイスがあります。

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

WorkSpaces は、 WorkSpaces が作成されるリージョンに応じて、さまざまなアドレス範囲から管理ネットワークインターフェイスの IP アドレスを選択します。ディレクトリが登録されると、 はVPCCIDRと のルートテーブルを WorkSpaces テストVPCして、これらのアドレス範囲が競合を引き起こすかどうかを判断します。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。ディレクトリの登録VPC後に のルートテーブルを変更すると、競合が発生する可能性があります。

Warning

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

管理インターフェイスの IP 範囲

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

Note

- Bring Your Own License (BYOL) Windows を使用している場合 WorkSpaces、次の表の IP アドレス範囲は適用されません。代わりに、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PCoIPBYOL WorkSpaces を使用します。DCV BYOL Windows では WorkSpaces、54.239.224.0/20 と 10.0.0.0/8 の両方の IP アドレス範囲がすべての AWS リージョンに適用されます。(これらの IP アドレス範囲は、 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) BYOL WorkSpaces。
- パブリックバンドルからDCV WorkSpaces 作成された 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 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、198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (ムンバイ)	PCoIP/WSP: 192.168.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (ソウル)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (シンガポール)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (シドニー)	PCoIP/WSP: 172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 WSP: 10.0.0.0/8
アジアパシフィック (東京)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
カナダ (中部)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8
欧州 (フランクフルト)	PCoIP/WSP: 198.19.0.0/16 WSP: 10.0.0.0/8

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

管理インターフェイスポート

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

- ポート 4172 TCPへのインバウンド。これは、PCoIPプロトコルでのストリーミング接続の確立に使用されます。
- ポート 4172 UDPへのインバウンド。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 TCPのインバウンド。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 TCPのインバウンド。これは、 の管理と設定に使用されます WorkSpace。
- ポート 8201-8250 TCPのインバウンド。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 UDPのインバウンド。このポートは、ストリーミング接続の確立と、DCVプロトコルでのストリーミングユーザー入力に使用されます。
- ポート 8443 および 9997 TCPでのアウトバウンド。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 UDPでのアウトバウンド。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 UDPでのアウトバウンド。これはストリーミングに使用されます。ファイアウォールがステートフルフィルタリングを使用している場合、リターン通信用に一時ポート 50002 が自動的に開放されます。ファイアウォールがステートレスフィルタリングを使用する場合には、リターン通信用に一時ポート 49152 ~ 65535 を開放する必要があります。
- 管理インターフェイスの IP 範囲に定義されているように、ポート 80 TCPでのアウトバウンドは、EC2メタデータサービスにアクセスするために IP アドレス 169.254.169.254 に行われます。に割り当てられたHTTPプロキシは、169.254.169.254 も除外 WorkSpaces する必要があります。
- ポート 1688 TCPで IP アドレス 169.254.169.250 および 169.254.169.251 にアウトバウンドし、パブリックバンドルに基づく Workspace の Microsoft KMS for Windows アクティベーションへのアクセスを許可します。Bring-Your-Own-License (BYOL) Windows を使用している場合は WorkSpaces、Windows アクティベーションのために独自のKMSサーバーへのアクセスを許可する必要があります。
- の Microsoft KMS for Office アクティベーションへのアクセスを許可するため、ポート 1688 TCP で IP アドレス 54.239.236.220 にアウトバウンドしますBYOL WorkSpaces。

  いずれかの WorkSpaces パブリックバンドルで Office を使用している場合、Microsoft KMS for Office のアクティベーションの IP アドレスは異なります。その IP アドレスを確認するには、 の管理インターフェイスの IP アドレスを見つけ WorkSpace、最後の 2 つのオクテットを に置き換えます`64.250`。例えば、管理インターフェイスの IP アドレスが 192.168.3.5 の場合、Microsoft KMS Office アクティベーションの IP アドレスは 192.168.64.250 です。
- WorkSpace ホストがプロキシサーバーを使用するように設定されている場合DCV WorkSpaces の IP アドレス 127.0.0.2 TCPへのアウトバウンド。
- ループバックアドレス 127.0.01 から発信される通信。

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

プライマリインターフェイスポート

ディレクトリのタイプにかかわらず、すべて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を開く必要があります WorkSpaces。

- インターネット接続の場合、次のポートはすべての送信先へのアウトバウンドで、 からのインバウンドである必要があります WorkSpaces VPC。インターネットにアクセス WorkSpaces できるようにするには、 のセキュリティグループにこれらを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、 とディレクトリコントローラーの間で WorkSpaces VPC次のポートが開いている必要があります。Simple AD ディレクトリの場合、 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 ディレクトリの場合、これらのポートVPCを開くには、 のデフォルトのセキュリティグループを調整する必要がある場合があります。
  - TCP/UDP53 - 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/UDP445 - SMB
  - TCP/UDP 636 - LDAPS (LDAP over TLS/SSL)
  - TCP 1024-65535 - の動的ポート RPC

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

リージョンごとの IP アドレスとポートの要件

米国東部 (バージニア北部)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.us-east-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-east-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID>

カテゴリ	詳細
	お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 米国東部 (バージニア北部) — https://d32i4gd7pg4909.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.us-east-1.signin.aws
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.us-east-1.amazonaws.com • 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: https://workspaces.us-east-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.us-east-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-iad.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
DCV ゲートウェイサーバーの IP アドレス範囲	• 3.227.4.0/22 • 44.209.84.0/22
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 • WSP: 10.0.0.0/8

米国西部 (オレゴン)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.us-west-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.us-west-2.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック:

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 米国西部 (オレゴン) — https://d18af777lco7lp.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.us-west-2.signin.aws
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.us-west-2.amazonaws.com • 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: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.us-west-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-pdx.amazonworkspaces.com
ヘルスチェック IP アドレス	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 35.80.88.0 - 35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
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 • WSP: 10.0.0.0/8

アジアパシフィック (ムンバイ)

許可リストに追加するドメインと IP アドレス

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

カテゴリ	詳細
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (ムンバイ) — https://d78hovzzqqtsb.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-south-1.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-south-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-south-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	Web Access は現在、アジアパシフィック (ムンバイ) リージョンではご利用いただけません。
ヘルスチェックホスト名	drp-bom.amazonworkspaces.com
ヘルスチェック IP アドレス	• 13.127.57.82 • 13.234.250.73
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	13.126.243.0 - 13.126.243.255
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 • 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 以降および 2.0 以降の WorkSpaces クライアントアプリケーション用)	https://device-metrics-us-2.amazon.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-northeast-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-northeast-2.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (ソウル) — https://dtyv4uwoh7ynt.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-northeast-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-northeast-2.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-northeast-2.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.ap-northeast-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-icn.amazonworkspaces.com
ヘルスチェック IP アドレス	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
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 • 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 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-southeast-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン： https://ws-client-service.ap-southeast-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定:

カテゴリ	詳細
	• https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (シンガポール) — https://d3qzmd7y07pz0i.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-southeast-1.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-southeast-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-southeast-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.ap-southeast-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-sin.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
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 • WSP: 10.0.0.0/8

アジアパシフィック (シドニー)

許可リストに追加するドメインと IP アドレス

カテゴリ	詳細
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
クライアントの自動更新	https://d2td7dqidlhjx7.cloudfront.net/
接続の確認	https://connectivity.amazonworkspaces.com/
クライアントメトリクス (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ap-southeast-2.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ap-southeast-2.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック:

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (シドニー) — https://dwcpoxuuza83q.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
セッション前のスマートカード認証エンドポイント	https://smartcard.ap-southeast-2.signin.aws
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-southeast-2.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • 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: • https://skylight-cm.ap-southeast-2.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.ap-southeast-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-syd.amazonworkspaces.com
ヘルスチェック IP アドレス	• 3.24.11.127 • 13.237.232.125
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
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、198.19.0.0/16 • WSP: 10.0.0.0/8

アジアパシフィック (東京)

許可リストに追加するドメインと IP アドレス

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

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

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アジアパシフィック (東京) — https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

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 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ap-northeast-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ap-northeast-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ap-northeast-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.ap-northeast-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-nrt.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.178.102.247 • 54.64.174.128
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
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 • 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 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.ca-central-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.ca-central-1.amazonaws.com
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace : • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • カナダ (中部) — https://d2wfbsypmqjmog.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.ca-central-1.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.ca-central-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.ca-central-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.ca-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-yul.amazonworkspaces.com
ヘルスチェック IP アドレス	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
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 • WSP: 10.0.0.0/8

欧州 (フランクフルト)

許可リストに追加するドメインと IP アドレス

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

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 欧州 (フランクフルト) — https://d1whcm49570jjw.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-central-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • 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: • https://skylight-cm.eu-central-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.eu-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-fra.amazonworkspaces.com
ヘルスチェック IP アドレス	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
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 • 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 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://skylight-client-ds.eu-west-1.amazonaws.com
Dynamic Messaging Service (3.0 以降の WorkSpaces クライアントアプリケーション用)	ドメイン: https://ws-client-service.eu-west-1.amazonaws.com

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 欧州 (アイルランド) — https://d3pgffbf39h4k4.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

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 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-west-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.eu-west-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.eu-west-1.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.eu-west-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-dub.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
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、198.19.0.0/16 • WSP: 10.0.0.0/8

欧州 (ロンドン)

許可リストに追加するドメインと IP アドレス

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

カテゴリ	詳細
	お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル : • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル : • 欧州 (ロンドン) — https://d16q6638mh01s7.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.eu-west-2.amazonaws.com

カテゴリ	詳細
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.eu-west-2.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.eu-west-2.amazonaws.com
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.eu-west-2.rdn.amazonaws.com
ヘルスチェックホスト名	drp-lhr.amazonworkspaces.com
ヘルスチェック IP アドレス	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
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 • WSP: 10.0.0.0/8

南米 (サンパウロ)

許可リストに追加するドメインと IP アドレス

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

カテゴリ	詳細
	• https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • 南米 (サンパウロ) — https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.sa-east-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.sa-east-1.amazonaws.com

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

アフリカ (ケープタウン)

許可リストに追加するドメインと IP アドレス

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

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

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory ID> CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • アフリカ (ケープタウン); — https://di5ygl2cs0mrh.cloudfront.net/
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	詳細
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.af-south-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.af-south-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.af-south-1.amazonaws.com
ヘルスチェックホスト名	drp-cpt.amazonworkspaces.com
ヘルスチェック IP アドレス	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 13.246.120.0 - 13.246.123.255
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 • WSP: 10.0.0.0/8

イスラエル (テルアビブ)

許可リストに追加するドメインと IP アドレス

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

カテゴリ	詳細
	• CSS ログインページをスタイル設定する ファイル： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript ログインページの ファイル： • イスラエル (テルアビブ) —
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://<directory id>.awsapps.com/ (<directory id> はお客様のドメイン)
WS ブローカー	ドメイン: • https://ws-broker-service.il-central-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.il-central-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.il-central-1.amazonaws.com

カテゴリ	詳細
のウェブアクセスTURNサーバー PCoIP	サーバー: • turn:*.il-central-1.rdn.amazonaws.com
ヘルスチェックホスト名	drp-tlv.amazonworkspaces.com
ヘルスチェック IP アドレス	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 51.17.28.0-51.17.31.255
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
管理インターフェイスの IP アドレス範囲	• 198.19.0.0/16 • WSP: 10.0.0.0/8

AWS GovCloud（米国西部) リージョン

許可リストに追加するドメインと IP アドレス

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

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

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<ディレクトリ ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://s3.amazonaws.com/workspaces-client-assets/prod/pdt/<ディレクトリ ID> CSS ログインページをスタイル設定する ファイル： • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript ログインページの ファイル： • 該当しない
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

カテゴリ	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.signin.amazonaws-us-gov.com
登録の依存関係 (ウェブアクセスと Teradici PCoIP ゼロクライアントの場合)	https://s3.amazonaws.com
ユーザーログインページ	https://login.us-gov-home.awsapps.com/directory/<directory id>/ (<directory id> はお客様のドメインです)
WS ブローカー	ドメイン: • https://ws-broker-service.us-gov-west-1.amazonaws.com • https://ws-broker-service-fips.us-gov-west-1.amazonaws.com
WorkSpaces API エンドポイント	ドメイン: • https://workspaces.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com
セッションブローカー (PCM)	ドメイン: • https://skylight-cm.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com
ヘルスチェックホスト名	drp-pdt.amazonworkspaces.com

カテゴリ	詳細
ヘルスチェック IP アドレス	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 52.61.193.0 - 52.61.193.255
DCV ゲートウェイサーバーの IP アドレス範囲	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
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 • 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/

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

カテゴリ	詳細
ディレクトリ設定	にログインする前に、クライアントからカスタマーディレクトリへの認証 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<region>/<directory ID> MacOS クライアントからの接続: • https://d32i4gd7pg4909.cloudfront.net/ お客様のディレクトリ設定: • https://s3.amazonaws.com/workspaces-client-properties/prod/osu/<ディレクトリ ID> お客様のディレクトリレベルの共同ブランド化に使用されるログインページのグラフィック: • https://s3.amazonaws.com/workspaces-client-assets/prod/osu/<ディレクトリ ID> CSS ログインページをスタイル設定する ファイル： • https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css JavaScript ログインページの ファイル： • 該当しない
Forrester Log Service	https://fls-na.amazon.com/
ヘルスチェック (DRP) サーバー	ヘルスチェックサーバー

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

カテゴリ	詳細
PCoIP ゲートウェイサーバーのパブリック IP アドレス範囲	• 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
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 • WSP: 10.0.0.0/8

WorkSpaces Personal のクライアントネットワーク要件

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 WorkSpaces を使用して に接続できます。または、ウェブブラウザを使用して、この形式のアクセス WorkSpaces をサポートする に接続することもできます。ウェブブラウザアクセス WorkSpaces をサポートする のリストについては、「どの Amazon WorkSpaces バンドルがウェブアクセスをサポートしていますか？」を参照してください。クライアントアクセス、Web アクセス、およびユーザーエクスペリエンスで。

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

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

ユーザーに の優れたエクスペリエンスを提供するには WorkSpaces、クライアントデバイスが次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。
- のパフォーマンスを最大限に高めるにはPCoIP、クライアントのネットワークから があるリージョンへのラウンドトリップ時間 (RTT) が 100 ミリ秒未満 WorkSpaces である必要があります。RTT が 100 ミリ秒から 200 ミリ秒の間であれば、ユーザーは にアクセスできますが WorkSpace、パフォーマンスは影響を受けます。RTT が 200 ミリ秒から 375 ミリ秒の間であれば、パフォーマンスが低下します。が 375 ミリ秒RTTを超えると、 WorkSpaces クライアント接続は終了します。

  のパフォーマンスを最大限に高めるにはDCV、クライアントのネットワークRTTから があるWorkSpaces リージョンまでの が 250 ミリ秒未満である必要があります。RTT が 250 ミリ秒から 400 ミリ秒の間であれば、ユーザーは にアクセスできますが WorkSpace、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RTTに 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) WorkSpaces を介して にアクセスする場合、接続は 1200 バイト以上の最大送信単位 (MTU) をサポートする必要があります。

  > **Note**
  >
  > 仮想プライベートクラウド () VPNに接続された WorkSpaces 経由で にアクセスすることはできませんVPC。を使用して にアクセスするには WorkSpaces VPN、「」で説明されているように、インターネット接続 (VPNのパブリック IP アドレス経由) が必要です WorkSpaces Personal の IP アドレスとポートの要件。

- クライアントは、 サービスと Amazon Simple Storage Service (Amazon S3) によってホストされる WorkSpaces リソースHTTPSにアクセスする必要があります。クライアントは、アプリケーションレベルでプロキシリダイレクトをサポートしていません。 HTTPSへのアクセスは、ユーザーが登録を正常に完了して にアクセスできるようにするために必要です WorkSpaces。

- 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、 のPCoIPプロトコルバンドルを使用する必要があります WorkSpaces。Teradici でネットワークタイムプロトコル (NTP) も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。
- 3.0 以降のクライアントで Amazon のシングルサインオン (SSO) を使用している場合は WorkDocs、 AWS Directory Service 管理ガイドの「シングルサインオン」の手順に従う必要があります。

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

3.0 以上のクライアントのネットワーク要件を確認するには

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

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

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

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

1. WorkSpaces クライアントを開きます。クライアントを初めて開いた場合は、招待メールで受け取った登録コードを入力するよう求められます。

2. クライアントアプリケーションの右下隅にある [Network (ネットワーク)] を選択します。クライアントアプリケーションによって、ネットワーク接続、ポート、ラウンドトリップ時間がテストされ、これらのテストの結果がレポートされます。
3. [Dismiss] を選択してサインインページに戻ります。

WorkSpaces Personal の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 WorkSpaces 任意のデバイスから にアクセスできます。会社が企業データへのアクセスを信頼できるデバイス (マネージドデバイスとも呼ばれます) に制限している場合、有効な証明書を使用して信頼できるデバイス WorkSpaces へのアクセスを制限できます。

> **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 を介して WorkSpaces Personal ディレクトリが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、 は証明書ベースの認証 WorkSpaces を使用して、デバイスが信頼されているかどうかを判断します。 WorkSpaces クライアントアプリケーションは、デバイスが信頼されていることを検証できない場合、デバイスから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、 は両方をクライアントに WorkSpaces 提示し、クライアントはいずれかのルート証明書に連鎖する最初の有効な一致証明書を見つけます。

Supported Clients (サポートされるクライアント)

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

> **Important**
>
> この機能は次のクライアントではサポートされていません。
>
> - WorkSpaces Linux または 用の クライアントアプリケーション iPad

- Teradici 、 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むが、これに限定されないサードパーティーPCoIPRDPクライアント。

> **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、、CRT、CERTまたは PEM形式の Base64-encodedされた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 では RSA、 SHA256では ECDSA、 SHA384 では ECDSA、または SHA512では をお勧めしますECDSA。
- macOS の場合、デバイス証明書がシステムキーチェーンにある場合は、 WorkSpaces クライアントアプリケーションがそれらの証明書にアクセスすることを許可することをお勧めします。それ以

外の場合は、ユーザーがログインまたは再接続するときに、キーチェーンの資格情報を入力する必要があります。

ステップ 2: クライアント証明書を信頼されたデバイスにデプロイする

ユーザーの信頼されたデバイスで、デバイス証明書から信頼されたルート証明書認証へのチェーン内の、すべての証明書を含む証明書バンドルをインストールする必要があります。任意のソリューションを使用して、System Center Configuration Manager (SCCM) やモバイルデバイス管理 () などの証明書をクライアントデバイスのフリートにインストールできますMDM。SCCM および MDMは、オプションでセキュリティ体制評価を実行して、デバイスがアクセスする企業ポリシーを満たしているかどうかを判断できることに注意してください WorkSpaces。

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

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

ステップ 3: 制限を設定する

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

制限を設定するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Access Control Options] を展開します。
5. 「各デバイスタイプ」で、 にアクセスできるデバイスを指定し WorkSpaces、「信頼できるデバイス」を選択します。

6. 最大 2 つのルート証明書をインポートします。各ルート証明書について、次の操作を行います。

   a. [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にアクセス権があるかどうかを指定します WorkSpaces。

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

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

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

8. [Update and Exit] を選択します。

2.0 SAML を WorkSpaces Personal と統合する

> **Note**
>
> SAML 2.0 は、Simple AD、AD Connector、 AWS および Managed Microsoft AD ディレクトリ AWS Directory Service を含む を介して WorkSpaces 個人用ディレクトリが管理されている場合にのみ使用できます。この機能は、Amazon によって管理されるディレクトリには適用されません。通常 WorkSpaces、Amazon は 2.0 フェデレーションの代わりに IAM Identity Center SAML をユーザー認証に使用します。

デスクトップセッション認証 WorkSpaces 用に SAML 2.0 を 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ます。IdP を使用してユーザーを認証することで WorkSpaces、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 WorkSpaces することで を保護できます。

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 ウェブアクセス、および 2.0 ID プロバイダー (IdP) SAML 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たとき。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 によって開始されたとき。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 2.0 アプリケーションに対して WorkSpaces SAML承認されます。ユーザーは、WorkSpace 2.0 認証が有効になっているディレクトリに`user`ユーザー名 の SAML 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 開始フローにより、ユーザーは登録コードを入力することなく、 WorkSpaces クライアントアプリケーションをデバイスに自動的に WorkSpaces 登録できます。ユーザーは IdP 実行フロー WorkSpaces を使用して に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発信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 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. これで WorkSpaces クライアントアプリケーションが登録され、ユーザーはサインインを続けるをクリックして引き続きサインイン WorkSpaces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 実行型ウェブアクセスフローを使用すると、ユーザーは登録コードを入力することなく、ウェブブラウザ WorkSpaces から を自動的に WorkSpaces 登録できます。ユーザーは IdP 実行フロー WorkSpaces を使用して にサインインしません。 WorkSpaces 認証は Web Access から発信する必要があります。

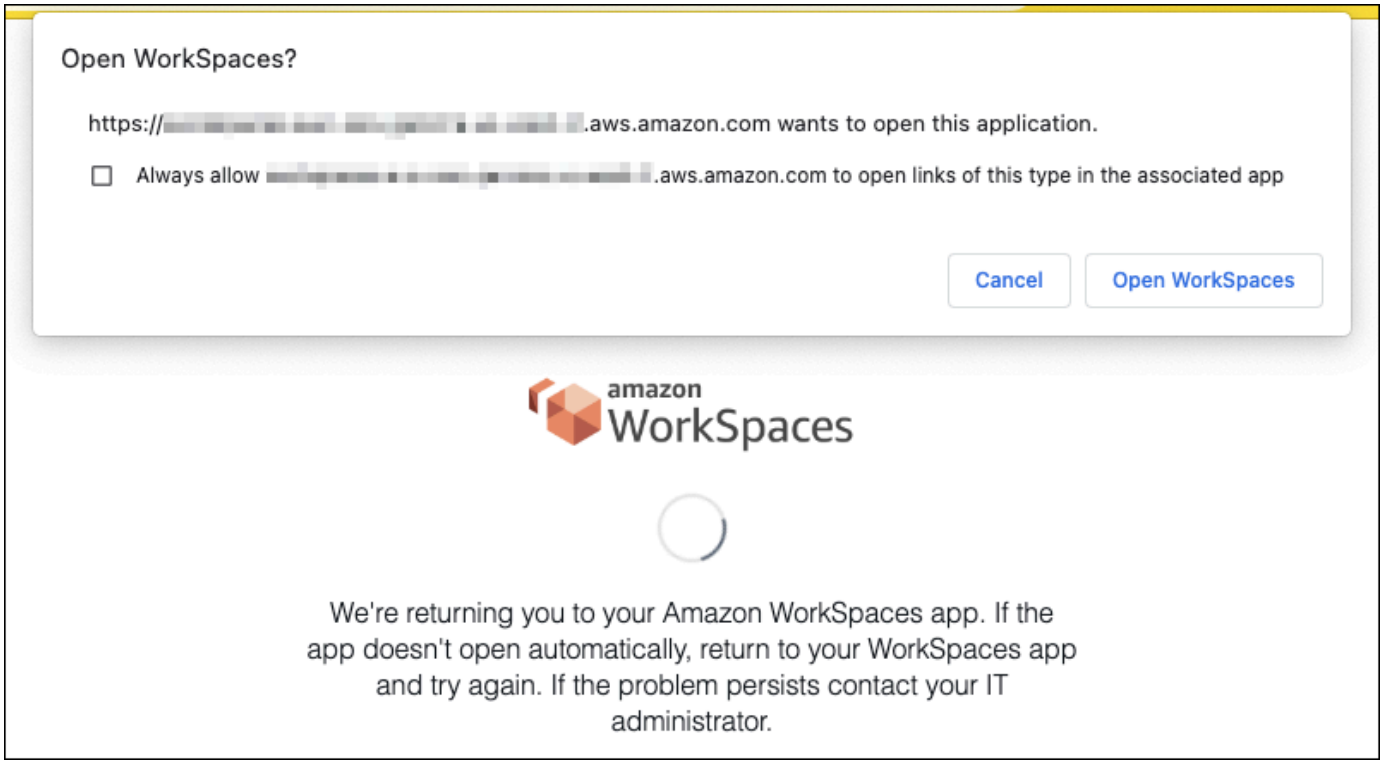
1. ユーザーはウェブブラウザを使用して、IdP にサインインします。
2. IdP にサインインすると、ユーザーは IdP ユーザーポータルから WorkSpaces アプリケーションをクリックします。
3. ユーザーはブラウザでこのページにリダイレクトされます。開くには WorkSpaces、ブラウザ WorkSpaces で Amazon を選択します。

4. WorkSpaces クライアントアプリケーションが登録され、ユーザーは WorkSpaces Web Access を通じて引き続きサインインできます。

WorkSpaces クライアント開始フロー

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 WorkSpaces した後に にサインインできます。

1. ユーザーは 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) 、「サインインを続ける WorkSpaces」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、 へのサインインを完了します WorkSpace。 WorkSpaces ユーザー名は IdP 2SAML.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します。
5. ユーザーは にサインインします WorkSpace。

WorkSpaces ウェブアクセス開始フロー

ウェブアクセス開始フローでは、ユーザーは IdP にサインイン WorkSpaces した後に にサインインできます。

1. ユーザーが WorkSpaces ウェブアクセスを起動し、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、ログインをクリックします WorkSpaces。
4. WorkSpace. WorkSpaces usernames へのサインインを完了するために WorkSpaces クライアントアプリケーションにリダイレクトされたユーザーは、IdP 2SAML.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します。

5. ユーザーは にサインインします WorkSpace。

WorkSpaces Personal SAML 用に 2.0 をセットアップする

2SAML.0 を使用して ID フェデレーションを設定することで、2.0 ID プロバイダー (IdP) の認証情報と認証方法を使用して、 WorkSpaces ユーザーの WorkSpaces クライアントアプリケーション登録と SAML へのサインインを有効にします。2SAML.0 を使用して 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を使用して IdP URLを設定し、 を有効にします AWS。これにより、フェデレーティッドユーザーに WorkSpaces ディレクトリへのアクセスが許可されます。リレーステートは、 WorkSpaces正常にサインインした後にユーザーが転送されるディレクトリエンドポイントです AWS。

内容

- 要件
- 前提条件
- ステップ 1: で SAML ID プロバイダーを作成する AWS IAM
- ステップ 2: 2.0 SAML フェデレーションIAMロールを作成する
- ステップ 3: IAMロールにインラインポリシーを埋め込む
- ステップ 4: 2.0 ID SAML プロバイダーを設定する
- 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
- 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
- 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

要件

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

  - アジアパシフィック (シンガポール) リージョン
  - アジアパシフィック (シドニー) リージョン
  - アジアパシフィック (東京) リージョン
  - カナダ (中部) リージョン
  - Europe (Frankfurt) Region
  - 欧州 (アイルランド) リージョン
  - 欧州 (ロンドン) リージョン
  - 南米 (サンパウロ) リージョン
  - イスラエル (テルアビブ) リージョン
  - AWS GovCloud （ 米国西部 ）
  - AWS GovCloud （ 米国東部 ）
- で SAML2.0 認証を使用するには WorkSpaces、IdP はディープリンクターゲットリソースまたはリレーステートエンドポイント SSOで開始された未承諾 IdP をサポートする必要がありますURL。の例 IdPs には、ADFS、Azure AD、"" Single Sign-On、Okta PingFederate、 などがありますPingOne。詳細については、IdP のユーザードキュメントを参照してください。
- SAML 2.0 認証は Simple AD を使用して WorkSpaces 起動された で機能しますが、Simple AD は 2.0 SAML と統合されないため、これは推奨されません IdPs。
- SAML 2.0 認証は、次の WorkSpaces クライアントでサポートされています。他のクライアントバージョンは 2.0 SAML 認証ではサポートされていません。Amazon WorkSpaces Client Downloads を開いて最新バージョンを検索します。
  - 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

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

、Azure ADADFS、シングルサインオン、Okta OneLogin、 PingFederate および for Enterprise step-by-step WorkSpaces を使用して SAML 2.0 を と統合する手順については、「Amazon WorkSpaces SAML Authentication Implementation Guide PingOne 」を参照してください。

前提条件

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

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

ステップ 1: で SAML ID プロバイダーを作成する AWS IAM

まず、 で SAML IdP を作成します AWS IAM。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 (Amazon Web Services マネジメントコンソール)」を参照してください。 (米国西部) および AWS GovCloud （ AWS GovCloud 米国東部)

SAML IdPs での の操作については、AWS 「 Identity and Access Management」を参照してください。

ステップ 2: 2.0 SAML フェデレーションIAMロールを作成する

次に、2.0 SAML 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。

IdP の SAML IAMロールを作成するには

1. https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
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、SAML2.0 フェデレーションを選択します。
4. Provider で、作成した SAML IdP SAMLを選択します。

   > **Important**
   >
   > 2 つの SAML 2.0 アクセス方法、プログラムによるアクセスのみを許可する方法、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アクセスを許可する方法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、永続の 値を持つ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 が永続的である場合、IdP は特定のユーザーからのすべてのSAMLリクエストで NameID 要素に同じ一意の値を送信します。SAML:sub_type アサーションの詳細については、「アクセスに SAMLベースのフェデレーションを使用する」の「 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。 SAML API AWS
7. 2.0 SAML の信頼情報を確認し、正しい信頼されたエンティティと条件を確認し、次へ: 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. sts:TagSession permission を新しいIAMロールの信頼ポリシーに追加します。詳細については、「AWS STSでのセッションタグの受け渡し」を参照してください。新しいIAMロールの詳細で、信頼関係タブを選択し、信頼関係の編集*を選択します。信頼関係ポリシーの編集エディタが開いたら、次のように sts:TagSession* アクセス許可を追加します。

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

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

ステップ 3: IAMロールにインラインポリシーを埋め込む

次に、作成したロールにインライン IAM ポリシーを埋め込みます。インラインポリシーを埋め込むと、ポリシーのアクセス許可が、間違ったプリンシパルエンティティにアタッチされることを回避で

きます。インラインポリシーは、フェデレーティッドユーザーに WorkSpaces ディレクトリへのアクセスを提供します。

> **Important**
>
> IAM ソース IP AWS に基づいて へのアクセスを管理する ポリシーは、`workspaces:Stream`アクションではサポートされていません。の IP アクセスコントロールを管理するには WorkSpaces、IP アクセスコントロールグループを使用します。さらに、2.0 SAML 認証を使用する場合、2.0 IdP SAML から IP アクセスコントロールポリシーを使用できる場合は、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、アクセス許可タブを選択し、ロールのアクセス許可ポリシーに必要なアクセス許可を追加します。[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ポリシーをコピーしてJSONウィンドウに貼り付けます。次に、 AWS リージョンコード、アカウント ID、ディレクトリ ID を入力してリソースを変更します。次のポリシーでは、 `"Action": "workspaces:Stream"`は WorkSpaces 、 ディレクトリ内のデスクトップセッションに接続するためのアクセス許可を WorkSpaces ユーザーに付与するアクションです。

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

をディレクトリが存在する AWS リージョンREGION-CODEに置き換えます WorkSpaces。を、 WorkSpaces マネジメントコンソールにある WorkSpaces ディレクトリ ID DIRECTORY-IDに置き換えます。 AWS GovCloud （ 米国西部) または AWS GovCloud （ 米国東部) のリソースの場合は、 に次の形式を使用しますARN。 `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: 2.0 ID SAML プロバイダーを設定する

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

IdP でこの更新がまだ設定されていない場合には、IdP から提供されるドキュメントでメタデータを更新する方法に関する情報を確認します。一部のプロバイダーでは、 と入力するオプションが提供されておりURL、IdP が ファイルを取得してインストールします。それ以外の場合は、 からファイルをダウンロードしURL、ローカルファイルとして指定する必要があります。

> **Important**
>
> 現時点では、IdP で設定したアプリケーションへのアクセス WorkSpacesを IdP のユーザーに許可することもできます。ディレクトリの WorkSpaces アプリケーションへのアクセスが許可されているユーザーには、自動的に WorkSpace が作成されません。同様に、 が WorkSpace 作成されたユーザーには、 WorkSpaces アプリケーションへのアクセスは自動的に許可されません。2.0 認証を使用して SAML に WorkSpace 正常に接続するには、ユーザーが IdP によって承認され、 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 が認証レスポンスの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 – サインインしているユーザーの一意の識別子。値は WorkSpaces ユーザー名と一致する必要があり、通常は Active Directory ユーザーの sAMAccountName 属性です。
- SAML サブジェクトタイプ (値を に設定`persistent`) – IdP が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する`persistent`ように 値を設定します。 ステップ 2: SAML2.0 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`persistent`、SAMLsub_type が 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てください。
- **Attribute Name** 属性が に設定された 要素 **https://aws.amazon.com/SAML/Attributes/Role** – この要素には、ユーザーが IdP によってマッピングされるIAMロールと SAML IdP を一覧表示する 1 つ以上の`AttributeValue`要素が含まれています。ロールと IdP は、カンマで区切られた のペアとして指定されますARNs。予期される値の例は `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME` です。
- **Attribute Name** 属性が に設定された 要素 **https://aws.amazon.com/SAML/Attributes/RoleSessionName** – この要素には、 に発行される AWS 一時的な認証情報の識別子を提供する`AttributeValue`要素が 1 つ含まれていますSSO。`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 () です UPN。ユーザーの表示名のように、スペースを含む値とすることはできません。
- **Attribute** 要素 (**Name** 属性を **https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email** に設定) – この要素には、ユーザーの E メールアドレスを指定する `AttributeValue` 要素が含まれます。値は、 WorkSpaces ディレクトリで定義されている WorkSpaces ユーザーの E メールアドレスと一致する必要があります。タグ値には、文字、数字、スペース、および特殊文字 (_ . : / = + - @) の組み合わせを含めることができます。詳細については、「 IAMユーザーガイド」の「 IAMおよび でのタグ付けのルール AWS STS」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 Name** 属性が **https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid** (オプション) に設定された 要素 – 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) を提供する `AttributeValue` 要素が 1 つ含まれています。このパラメータを証明書ベースの認証で使用すると、Active Directory ユーザーへの強力なマッピングが可能になります。詳細については、「証明書ベースの認証」を参照してください。
- **Attribute** 要素 (**Name** 属性を **https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName** に設定) (オプション) — この要素には、代替ユーザー名形式を指定する `AttributeValue` 要素が 1 つ含まれています。 WorkSpaces クライアントを使用してログイン`username@corp.example.com`するために `corp\username`、、 などのユーザー名形式を必要とするユースケースがある場合は`corp.example.com\username`、この属性を使用します。タグのキーと値には、文字、数字、スペース、特殊文字 (_ : / . + = @ -) の任意の組み合わせを使用できます。詳細については、「 IAMユーザーガイド」の「 IAMおよび でのタグ付けのルール AWS STS」を参照してください。`corp\username` または `corp.example.com\username`形式を取得するには、SAMLアサーションで \ を / に置き換えます。
- **AttributeName** 属性が Attributes/PrincipalTag:Domain (オプション) に設定された https://aws.amazon.com/SAML/要素 – この要素には、サインインするユーザーに Active Directory のDNS 完全修飾ドメイン名 (FQDN) を提供する 1 つの `AttributeValue`要素が含まれています。このパラメータは、ユーザーの Active Directory `userPrincipalName` に代替サフィックスが含まれている場合に、証明書ベースの認証で使用されます。値は、サブドメインを含め、`domain.com` で指定する必要があります。
- **Attribute Name** 属性が Attributes/SessionDuration (オプション) に設定された https://aws.amazon.com/SAML/要素 – この要素には、ユーザーのフェデレーティッドストリーミングセッションが再認証が必要になる前にアクティブのままになる最大時間を指定する `AttributeValue` 要素が 1 つ含まれています。デフォルト値は 3600 秒 (60 分) です。詳細については、`SAMLSessionDurationAttribute`「」を参照してください。

> **Note**
>
> `SessionDuration` はオプションの属性ですが、SAMLレスポンスに含めることをお勧めします。この属性を指定しない場合、セッション期間はデフォルト値の 3600 秒 (60 分) に設定されます。 WorkSpaces デスクトップセッションは、セッション期間が終了すると切断されます。

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

ステップ 6: フェデレーションのリレーステートを設定する

次に、IdP を使用して、 WorkSpaces ディレクトリリレーステート 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URL。による認証に成功すると AWS、ユーザーは認証SAMLレスポンスでリレーステートとして定義された WorkSpaces ディレクトリエンドポイントに誘導されます。

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

オプションで、クロスリージョンリダイレクトを使用している場合は WorkSpaces、登録コードをプライマリリージョンとフェイルオーバーリージョンのディレクトリに関連付けられた完全修飾ドメイン名 (FQDN) に置き換えることができます。詳細については、「Amazon のクロスリージョンリダイレクト WorkSpaces」を参照してください。クロスリージョンリダイレクトと 2.0 SAML 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 認証で有効にし、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 が正しくFQDN設定され、フェイルオーバーイベント中にユーザーが認証できるようになります。

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

2.0 認証が WorkSpaces SAML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

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-east-1.aws.amazon.com
米国西部 (オレゴン) リージョン	• workspaces.euc-sso.us-west-2.aws.amazon.com • （FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
アフリカ (ケープタウン) リージョン	workspaces.euc-sso.af-south-1.aws.amazon.com
アジアパシフィック (ムンバイ) リージョン	workspaces.euc-sso.ap-south-1.aws.amazon.com
アジアパシフィック (ソウル) リージョン	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
アジアパシフィック (シンガポール) リージョン	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
アジアパシフィック (シドニー) リージョン	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
アジアパシフィック (東京) リージョン	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
カナダ (中部) リージョン	workspaces.euc-sso.ca-central-1.aws.amazon.com
欧州 (フランクフルト) リージョン	workspaces.euc-sso.eu-central-1.aws.amazon.com
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

リージョン	リレーステートのエンドポイント
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-1amazonaws-us-gov..com • （FIPS) workspaces.euc-sso-fips.us-gov-west-1amazonaws-us-gov..com **Note** 詳細については、 AWS GovCloud （米国) 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-1amazonaws-us-gov..com • （FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** 詳細については、 AWS GovCloud （米国) 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) が開始するフローでは、2.0 SAML 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、 の後にリレーステート のweb最後に URLnativeまたは を指定します&client=。パラメータがリレーステート で指定されている場合URL、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 コンソールを使用して、 WorkSpaces ディレクトリで SAML 2.0 認証を有効にできます。

2.0 SAML との統合を有効にするには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. のディレクトリ ID を選択します WorkSpaces。
4. [Authentication] (認証) で、[Edit] (編集) を選択します。
5. 編集 SAML 2.0 ID プロバイダーを選択します。
6. 「Enable SAML 2.0 authentication」を確認します。
7. ユーザーアクセスURLと 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適用される値を入力します。IdP ディープリンクパラメータ名のデフォルト値は、このパラメータを省略するとRelayState「」になります。次の表に、アプリケーションのさまざまな ID プロバイダーに固有のユーザーアクセス名URLとパラメータ名を示します。

   許可リストに追加するドメインと IP アドレス

ID プロバイダー	パラメータ	ユーザーアクセス URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID=<relaying-party-uri>`
Azure AD	`RelayState`	`https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>`
Duo Single Sign-On	`RelayState`	`https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso`

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

ユーザーアクセスURLは通常、未承諾の IdP 開始 のプロバイダーによって定義されますSSO。ユーザーはこれをウェブブラウザURLに入力して、SAMLアプリケーションに直接フェデレーションできます。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、テストを選択します。現在のブラウザまたは別のブラウザのプライベートウィンドウURLにテストをコピーして貼り付け、現在の AWS 管理コンソールセッションを中断することなく SAML 2.0 ログオンをテストします。IdP 開始フローが開いたら、 WorkSpaces クライアントを登録できます。詳細に

ついては、「Identity provider (IdP)-initiated flow」(ID プロバイダー (IdP) を起点とするフロー) を参照してください。

8. フォールバック設定を管理するには、 をオンまたはオフにします。2SAML.0 をサポートしていないクライアントがログインできるようにします。この設定を有効にすると、ユーザーが 2SAML.0 をサポートしていないクライアントタイプまたはバージョン WorkSpaces を使用してへのアクセスを引き続き提供したり、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、 へのアクセスを提供したりできます。

   > **Note**
   >
   > この設定により、ユーザーは SAML 2.0 をバイパスし、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使用してログインできます。

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

   > **Note**
   >
   > PCoIP を使用した SAMLは、ウェブアクセスではサポートされていません。

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

証明書ベースの認証と WorkSpaces 個人

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

- 2.0 ID プロバイダーに依存してユーザーを認証し、Active Directory SAML のユーザーと一致する SAMLアサーションを提供します。
- 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。
- 2.0 ID SAML プロバイダーを使用してパスワードレス認証フローを有効にします。

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、ルートや下位 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CAs。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 ユーザーガイドをご参照ください。

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

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

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

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

前提条件

証明書ベースの認証を有効にする前に、次の手順を実行してください。

1. 証明書ベースの認証を使用するように WorkSpaces ディレクトリを SAML 2.0 統合で設定します。詳細については、「 WorkSpaces2.0 SAML との統合」を参照してください。
2. SAML アサーションで `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 アサーションで `ObjectSid` 属性を設定します。これは、Active Directory ユーザーへの強力なマッピングを行うためのオプションです。属性が SAML_Subject 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NameID。詳細については、SAML「認証レスポンスのアサーションを作成する」を参照してください。
4. 2.0 SAML 設定で使用されているIAMロール信頼ポリシーが存在しない場合は、sts:TagSession アクセス許可を追加します。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、「2SAML.0 フェデレーションIAMロールの作成」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。証明書ベースの認証を使用するには AWS Private CA 、 が必要です。詳細に

ついては、AWS Private CA「デプロイの計画」を参照し、ガイダンスに従って証明書ベースの認証用に CA を設定します。証明書ベースの認証のユースケースで最も一般的な 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エントリ用に設定された Amazon S3 バケットへの認証されていないアクセス、または CloudFrontパブリックアクセスをブロックしている場合は S3 バケットにアクセスできるディストリビューションが必要です。これらのオプションの詳細については、「証明書失効リストの計画 (CRL)」を参照してください。

6. プライベート CA に、EUC証明書ベースの認証で使用する CA `euc-private-ca`を指定する権限を持つキーをタグ付けします。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 を使用した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して、TCPポート 135 および 49152-65535 で証明書の自動登録を有効にすることです。さらに、実行中のEC2インスタンスは、ドメイン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を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 コンソールで、または SDKまたは を使用して CA を選択しCLI、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 を発行することもできます。詳細については、「設定手順」を参照してください。

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

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

> **Note**
>
> - Active Directory は、ドメインに参加している WorkSpaces デスクトップの信頼されたルート認証機関とエンタープライズNTAuthストアに CA を自動的に配布する必要があります。

証明書ベースの認証を有効にする

証明書ベースの認証を有効にするには、次の手順を実行します。

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

> **Note**
>
> 証明書ベースの認証で へのサインインが有効になっている場合 WorkSpaces、ディレクトリで有効になっていても、ユーザーは多要素認証 (MFA) を求められません。証明書ベースの認証を使用する場合、 は 2.0 ID SAML プロバイダーを通じて有効にMFAできます。詳細につ

いては AWS Directory Service MFA、「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

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

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

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

クロスアカウントPCA共有を有効にする

プライベート CA 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。

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

1. 集中型 AWS アカウントCBAで 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 個人」を参照してください。
2. 「 を使用してプライベート CA クロス AWS アカウントを共有する方法」のCBA手順に従って、 WorkSpaces リソースが使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 RAM ACM 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。Private CA は、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 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APIs。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 サービスロールで使用されるPCAテンプレートと一致します。
3. 共有が成功すると、リソースアカウントのプライベート 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、 WorkSpaces ディレクトリプロパティCBAで Private CA を ARN 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 の選択をサポートしていませんARNs。CLI コマンドの例：

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

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 を使用して専用の 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 にサインインした後、ユーザーは IdP ユーザーポータルから AWS IAM アイデンティティセンター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 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 にサインインした後、ユーザーは IdP ユーザーポータルから AWS IAM アイデンティティセンター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で 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

DCV バンドル WorkSpaces の Windows および Linux では、認証に共通アクセスカード (CAC) および個人 ID 検証 (PIV) スマートカードを使用できます。

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

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

内容

- 要件

- 制限
- ディレクトリ設定
- Windows のスマートカードを有効にする WorkSpaces
- Linux 用のスマートカードを有効にする WorkSpaces

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) 認証を使用して、ハードウェアまたはソフトウェアベースのスマートカード証明書を使用して Active Directory に対してユーザーを認証します。AD Connector およびオンプレミスのディレクトリを設定する方法の詳細については、ディレクトリ設定 を参照してください。
- Windows または Linux でスマートカードを使用するには WorkSpace、ユーザーは Amazon WorkSpaces Windows クライアントバージョン 3.1.1 以降または WorkSpaces macOS クライアントバージョン 3.1.5 以降を使用する必要があります。Windows および macOS クライアントで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」と、Microsoft ドキュメントの「証明書の要件」を参照してください。

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

  - 証明書の userPrincipalName （ UPN) フィールドの AD ユーザーの subjectAltName （ SAN ）。ユーザーのデフォルト に対してスマートカード証明書を発行することをお勧めしますUPN。
  - 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ステータスプロトコル (OCSP) が必要です。セッション内認証の場合、 OCSPが推奨されますが、必須ではありません。

制限

- 現在、スマートカード認証では、 WorkSpaces Windows クライアントアプリケーションバージョン 3.1.1 以降と macOS クライアントアプリケーションバージョン 3.1.5 以降のみがサポートされています。
- WorkSpaces Windows クライアントアプリケーション 3.1.1 以降では、クライアントが 64 ビットバージョンの Windows で実行されている場合にのみスマートカードがサポートされます。
- Ubuntu 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
- Linux または Windows でのセッション内認証とセッション前認証の場合 WorkSpaces、現在一度に許可されるスマートカードは 1 つだけです。
- 現在、セッション前認証において、スマートカード認証とサインイン認証の両方を同じディレクトリで有効にすることはサポートされていません。
- 現時点では、 CACおよび 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動作する可能性がありますが、 での使用は完全にテストされていませんDCV。

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ために 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では、Kerberos の制約付き委任 (KCD) が正しく機能する必要があります。 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 sAMAccountの名前と一致する必要があります。sAMAccount名前は 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 ディレクトリの設定に加えて、オンプレミス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を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 のスマートカードを有効にする WorkSpaces

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

Windows ロック画面を検出してセッションを切断するには

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

グループポリシー設定を使用して、Windows ロック画面が検出されたときに、セッションの切断を有効にできます。詳細については、「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 DCV」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のためのスマートカードの使用をサポートしていません。必要に応じて、グループポリシー設定 WorkSpaces を使用して、Windows のセッション内認証とセッション前認証を有効にできます。詳細については、「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 DCV」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ために AD Connector で mTLS 認証を有効にする」の指示に従ってください。

ユーザーがブラウザでスマートカードを使用できるようにするには

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

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

例えば、Windows 用 OpenSC の 64 ビットバージョンをインストールして PKCS #11 をサポートした後、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 のように PKCS #11 を識別するために使用する任意の値OpenSCで、 *PATH_TO_LIBRARY_FOR_DEVICE*は PKCS #11 モジュールへのパスです。このパスは、 などの DLL拡張子を持つライブラリを指す必要がありますC:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll。

```
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UPNの 。
- キーの使用に <EKU>msScLogin が含まれる複数の証明書を有していること。

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

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

Linux 用のスマートカードを有効にする WorkSpaces

> **Note**
>
> WorkSpaces の Linux には、DCV現在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。
> - で Linux に接続するには、 WorkSpaces Windows WorkSpaces クライアントアプリケーションを使用する必要がありますDCV。

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

ルート CA 証明書を取得するには

ルート CA 証明書は、いくつかの方法で取得できます。

- サードパーティーの証明機関によって運用されるルート CA 証明書を使用できます。
- 独自のルート CA 証明書を エクスポートするには、 `http://ip_address/certsrv`または のいずれかのウェブ登録サイトを使用します。ここで`http://fqdn/certsrv`、 *ip_address* と はルート証明書 CA サーバーの IP アドレスと完全修飾ドメイン名 (FQDN) *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。Open の詳細については SSL、www.openssl.org を参照してください。

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

Linux にルート CA 証明書を追加するには WorkSpaces

スマートカードの有効化を支援するために、Amazon Linux DCVバンドルに enable_smartcardスクリプトを追加しました。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 Network Security Services (NSS) データベースにインポートします。
- Pluggable Authentication pam_pkcs11 Module (PAM) 認証用の モジュールをインストールします。
- プロビジョニングpkinit中の WorkSpace の有効化を含むデフォルト設定を実行します。

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

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

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

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

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

   `auth` 行のコメントを解除した後、あるサービスについてスマートカード認証を使用できるようにするには、その行をリストに追加する必要があります。あるサービスににについてパスワード認証のみを使用するには、リストからそのサービスを削除する必要があります。
4. に追加のカスタマイズを実行します WorkSpace。例えば、システム全体のポリシーを追加して、ユーザーが Firefox でスマートカードを使用できるようにします。(Chrome ユーザーはクライアントでスマートカードを有効にする必要があります。 詳細については、「Amazon 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. からカスタム WorkSpace イメージとバンドルを作成します WorkSpace。
6. 新しいカスタムバンドルを使用して、ユーザーの WorkSpaces を起動します。

ユーザーが Firefox でスマートカードを使用できるようにするには

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

1. WorkSpace イメージの作成に WorkSpace 使用している で、 `policies.json`に という名前の新しいファイルを作成します`/usr/lib64/firefox/distribution/`。
2. JSON ファイルで、次の SecurityDevices ポリシーを追加します。ここで、*NAME_OF_DEVICE*はpkcsモジュールを識別するために使用する任意の値です。例えば、"0penSC" 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UPNの 。
- 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 を入力しますPIN。 は、スマートカード証明書stdoutのユーザー名を 形式でpklogin_finder出力します*NETBIOS**username*。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 (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。たとえば、DNSドメイン名が の場合example.com、NetBIOS ドメイン名は通常 ですEXAMPLE。DNS ドメイン名が の場合corp.example.com、NetBIOS ドメイン名は通常 ですCORP。

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 チケット付与チケット () を正常に取得する必要がありますTGT。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すると、 WorkSpace ユーザー名から Kerberos プリンシパル名へのマッピングで問題が発生する可能性が最も高くなります。[appdefaults]/pam/mappings ファイル内の /etc/krb5.conf セクションを確認してください。

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

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、VPC WorkSpaces 個人用の 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/ 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/ 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 アカウントあたり最大 100 の IP アクセスコントロールグループをリージョンごとに作成できます。ただし、1 つのディレクトリに関連付けることができるのは、最大 25 の IP アクセスコントロールグループのみです。

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

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

> **Note**
>
> - IP アクセスコントロールグループでは、NAT 用に動的 IP アドレスを使用することはできません。NAT を使用している場合は、動的 IP アドレスではなく静的 IP アドレスを使用するように設定します。WorkSpaces セッションの間、NAT がすべての UDP トラフィックを同じ静的 IP アドレス経由でルーティングするようにします。
> - IP アクセス制御グループは、ユーザーが WorkSpaces にストリーミングセッションを接続できる IP アドレスを制御します。ユーザーは、Amazon WorkSpaces パブリック API を使用して、任意の IP アドレスから再起動、再構築、シャットダウンなどの機能を実行できます。

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

IP アクセスコントロールグループを作成する

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

IP アクセスコントロールグループを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. [IP グループの作成] を選択します。

4. [IP グループの作成] ダイアログボックスで、グループ名と説明を入力し、[作成] を選択します。
5. グループを選択してから、[編集] を選択します。
6. 各 IP アドレスで、[Add Rule (ルールの追加)] を選択します。[Source (送信元)] に IP アドレスまたは IP アドレスの範囲を入力します。[説明] に説明を入力します。ルールの追加を完了したら、[保存] を選択します。

IP アクセスコントロールグループをディレクトリに関連付ける

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

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

IP アクセスコントロールグループをディレクトリに関連付けるには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [IP アクセスコントロールグループ] を展開し、1 つ以上の IP アクセスコントロールグループを選択します。
5. [Update and Exit] を選択します。

IP アクセスコントロールグループをコピーする

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

既存の IP アクセスコントロールグループから新しいグループを作成するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. グループを選択して、[アクション]、[コピーして新規作成] の順に選択します。
4. [IP グループのコピー] ダイアログボックスで、新しいグループの名前と説明を入力し、[グループのコピー] を選択します。

5. (オプション) 元のグループからコピーしたルールを変更するには、新しいグループを選択し、[編集] を選択します。必要に応じてルールを追加、更新、または削除します。[保存] を選択します。

IP アクセスコントロールグループを削除する

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

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

IP アクセスコントロールグループを削除するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. IP アクセスコントロールグループに関連付けられている各ディレクトリで、ディレクトリを選択し、[アクション]、[更新の詳細] の順に選択します。[IP アクセスコントロールグループ] を展開し、IP アクセスコントロールグループのチェックボックスをオフにして、[更新と終了] を選択します。
4. ナビゲーションペインで [IP アクセスコントロール] を選択します。
5. グループを選択し、[アクション]、[IP グループの削除] を選択します。

WorkSpaces 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、「USB プリンターやその他の USB周辺機器がPCoIPゼロクライアントで機能しない」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。

Android for Chromebook for WorkSpaces Personal をセットアップする

バージョン 2.4.13 は、Amazon Chromebook WorkSpaces 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しているため、 WorkSpaces

Chromebook クライアントアプリケーションにはそれ以上の更新はなく、その使用はサポートされていません。

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

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

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

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

> **Note**
>
> - DCV for Windows および Ubuntu を使用したウェブアクセス WorkSpaces 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。 DCV for Amazon Linux WorkSpaces は AWS GovCloud （ 米国西部) でのみ使用できます。
> - ストリーミング品質とユーザーエクスペリエンスを最大限に高めDCV WorkSpaces るために、 で Web Access を使用することを強くお勧めします。で Web Access を使用する場合の制限は次のとおりですPCoIP WorkSpaces。
>   - を使用したウェブアクセスPCoIP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。
>   - を使用したウェブアクセスPCoIPは Windows でのみサポートされ WorkSpaces、Amazon Linux や Ubuntu ではサポートされません WorkSpaces。

- ウェブアクセスは、 PCoIPプロトコル WorkSpaces を使用している一部の Windows 10 では使用できません。PCoIP WorkSpaces が Windows Server 2019 または 2022 を利用している場合、ウェブアクセスは使用できません。
- を使用したウェブアクセスPCoIP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。

- で macOS を使用してVPNいて、Firefox ウェブブラウザを使用している場合、ウェブブラウザは WorkSpaces Web Access PCoIP WorkSpaces を使用したストリーミングをサポートしません。これは、WebRTC プロトコルの Firefox 実装の制限によるものです。

Important

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

ステップ 1: へのウェブアクセスを有効にする WorkSpaces

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

へのウェブアクセスを有効にするには WorkSpaces

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

> **Note**
>
> Web Access を有効にしたら、変更を適用するため、 を再起動 WorkSpace します。

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

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

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

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

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

グループポリシーオブジェクト (GPOs) を使用して、Windows ディレクトリの一部である Windows WorkSpaces WorkSpaces または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の組織単位と WorkSpaces ユーザーオブジェクトの組織単位を作成することをお勧めします。

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

WorkSpaces ログオンエージェントでユーザーを切り替えるには

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

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

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

最後にログオンしたユーザー名を非表示にするには

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

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

1. グループポリシー管理ツール (gpmc.msc) を開き、 に移動して、使用するディレクトリのGPO ドメインまたはドメインコントローラーレベルで を選択します WorkSpaces。(WorkSpaces グループポリシー管理テンプレートがドメインにインストールされている場合は、 WorkSpaces マシンアカウントに WorkSpaces GPOを使用できます。)
2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. 次のいずれかの設定を開きます。
   - Windows 7 の場合 — Interactive logon: Don't display last signed-in
   - Windows 10 の場合 — Interactive logon: Do not display last user name
5. 該当する設定の [プロパティ] ダイアログボックスで、[有効]、[OK] の順に選択します。

ユーザーがログオンする前に CTRL + ALT + DEL を押すことを要求するには

WorkSpaces Web Access の場合、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必要があります。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と、ユーザーはパスワードを入力するときに信頼できるパスを使用できます。

1. グループポリシー管理ツール (gpmc.msc) を開き、 に移動して、使用するディレクトリのGPO ドメインまたはドメインコントローラーレベルで を選択します WorkSpaces。(WorkSpaces グループポリシー管理テンプレートがドメインにインストールされている場合は、 WorkSpaces マシンアカウントに WorkSpaces GPOを使用できます。)
2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. インタラクティブログオンを開く: CTRL + ALT+ 設定は必要ありませんDEL。
5. [Local Security Setting] タブで、[Disabled] を選択して [OK] を選択します。

セッションがロックされているときにドメインとユーザー情報を表示するには

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

1. グループポリシー管理ツール (gpmc.msc) を開き、 に移動して、使用するディレクトリのGPO ドメインまたはドメインコントローラーレベルで を選択します WorkSpaces。(WorkSpaces グループポリシー管理テンプレートがドメインにインストールされている場合は、 WorkSpaces マシンアカウントに WorkSpaces GPOを使用できます。)
2. メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Options] の順に選択します。
4. [Interactive logon: Display user information when the session is locked] 設定を開きます。
5. [Local Security Setting] タブで、[User display name, domain and user names] を選択し、[OK] を選択します。

グループポリシーとセキュリティポリシーの設定の変更を適用するには

グループポリシーとセキュリティポリシーの設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションの再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。

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

WorkSpaces Personal 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 WorkSpaces ように Amazon を設定する必要があります。また、FedRAMP 認可を持つ、または DoD SRG に準拠している米国 AWS リージョンを使用する必要があります。

FedRAMP 認可のレベル (中または高) または DoD SRG影響レベル (2、4、または 5) WorkSpaces は、Amazon が使用されている米国 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、AWS「コンプライアンスプログラムによる対象範囲内のサービス」を参照してください。

> **Note**
>
> FIPS エンドポイント暗号化の使用に加えて、 を暗号化することもできます WorkSpaces。詳細については、「WorkSpaces Personal WorkSpaces で暗号化」を参照してください。

要件

- Fed 認可を持つ、または DoD に準拠している米国リージョン WorkSpaces で を作成する必要があります。 AWS RAMP DoD SRG
- WorkSpaces ディレクトリは、エンドポイントの暗号化に 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 ディレクトリが新しいか、ディレクトリ WorkSpaces 内のすべての既存のエンドポイント暗号化に FIPS 140-2 検証モードを使用する必要があります。それ以外の場合は、この設定を使用できないため、WorkSpaces 作成する は FedRAMP または DoD 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 WorkSpaces から にアクセスする必要があります。
  - Windows 2.4.3 以降
  - macOS: の場合は 2.4.3 以降PCoIP WorkSpaces、 の場合は 5.21.0 以降 DCV WorkSpaces
  - 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. Fed 認証および DoD RAMPSRG準拠を作成するディレクトリに、既存の が WorkSpaces 関連付けられ WorkSpaces ていないことを確認します。ディレクトリ WorkSpaces に関連付けられていて、ディレクトリで 140-2 FIPS 検証モードの使用がまだ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. エンドポイントの暗号化では、暗号化FIPSモード (標準) の代わりに 140-2 検証モードを選択します。 TLS

7. [Update and Exit] を選択します。
8. これで、FedRAMP 認証および DoD SRG 準拠のこのディレクトリ WorkSpaces から を作成できるようになりました。これらにアクセスするには WorkSpaces、ユーザーは要件セクションで前述した WorkSpaces クライアントアプリケーションの 1 つを使用する必要があります。

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

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

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

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「 WorkSpaces を使用して Linux Amazon に接続するにはどうすればよいですかSSH？」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 SSHへの接続の前提条件 WorkSpaces
- ディレクトリ WorkSpaces 内のすべての Linux SSHへの接続を有効にする
- でのパスワードベースの認証 WorkSpaces
- 特定の Linux SSHへの接続を有効にする WorkSpace
- Linux または Pu WorkSpace を使用して Linux に接続するTTY

Linux SSHへの接続の前提条件 WorkSpaces

- へのインバウンドSSHトラフィックの有効化 WorkSpace - 1 つ以上の Linux へのインバウンドSSHトラフィックを許可するルールを追加するには WorkSpaces、 SSHへの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ます WorkSpaces。例えば、仮想プライベートクラウド (VPC) の外部にあるデバイスのパブリック IP

アドレスや、 VPCと同じ にある別のEC2インスタンスのプライベート IP アドレスを指定できます WorkSpace。

WorkSpace ローカルデバイスから に接続する場合は、インターネットブラウザで検索語「私の IP アドレス」を使用するか、次のサービスを使用できます。IP を確認する。

- への接続 WorkSpace — デバイスから Linux への SSH接続を開始するには、次の情報が必要です WorkSpace。
  - 接続している Active Directory ドメインのネットBIOSネーム。
  - WorkSpace ユーザー名。
  - 接続 WorkSpace 先の のパブリックまたはプライベート IP アドレス。

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

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

接続 WorkSpace する Linux の IP アドレスとユーザー名を確認するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. のリスト WorkSpace で WorkSpaces、SSH接続を有効にする を選択します。
4. 実行中モード列で WorkSpace、ステータスが使用可能であることを確認します。
5. WorkSpace 名前の左にある矢印をクリックしてインラインの概要を表示し、次の情報を書き留めます。

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

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

10. にパブリック IP アドレス WorkSpace がある場合は、IPv4パブリック IP 列に表示されます。このパブリック IP アドレスを書き留めます (該当する場合) 。

接続している Active Directory ドメインの NetBIOS name を検索するには

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

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

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

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

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. ナビゲーションペインで、[Security Groups] を選択します。
3. [Create Security Group (セキュリティグループの作成)] を選択します。
4. 名前を入力します。また、オプションで説明およびセキュリティグループを入力します。
5. でVPC、SSH接続を有効にする VPCを含む WorkSpaces 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。
   - [Type] (タイプ) で、SSH を選択します。
   - Protocol では、 を選択すると が自動的に指定TCPされますSSH。
   - ポート範囲 では、 を選択すると 22 が自動的に指定されますSSH。
   - Source には、ユーザーが への接続に使用するコンピュータのパブリック IP アドレスCIDRの範囲を指定します WorkSpaces。例えば、企業ネットワークやホームネットワークなどです。
   - [説明] (オプション) に、ルールの説明を入力します。
7. [Create] (作成) を選択します。
8. このセキュリティグループを にアタッチします WorkSpaces。このセキュリティグループを に追加する方法の詳細については WorkSpaces、「」を参照してくださいWorkSpaces Personal

のセキュリティグループ。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 WorkSpaces、このブログ記事を参照してください。

でのパスワードベースの認証 WorkSpaces

新しく作成した Linux でパスワード認証を有効にするには WorkSpaces

1. WorkSpaces クライアントを起動し、 にログインします WorkSpace。
2. ターミナルウィンドウを開きます。
3. ターミナルウィンドウで次のコマンドを実行して、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に cloud-init に指示します。
- `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設定ディレクトリ にSSHパスワード認証を有効にするファイルが書き込まれ`/etc/ssh/sshd_config.d/`、設定がすぐに行われるSSHDように再起動されます。

これにより、 でSSHパスワード認証が有効 WorkSpace になり、カスタムイメージを通じて保持されます。cloud-init を設定せずに、SSHD設定ファイルでのみSSHパスワード認証を有効にした場合、設定は一部の Linux ではイメージを通じて保持されません WorkSpaces。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 でパスワード認証を無効にするには WorkSpaces

1. WorkSpaces クライアントを起動し、 にログインします WorkSpace。
2. ターミナルウィンドウを開きます。
3. ターミナルウィンドウで次のコマンドを実行して、cloud-init の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に cloud-init に指示します。
- `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設定ディレクトリ にSSHパスワード認証を有効にするファイルが書き込まれ`/etc/ssh/sshd_config.d/`、設定がすぐに行われるSSHDように再起動されます。

これにより、 SSHで がすぐに無効 WorkSpace になり、カスタムイメージを通じて保持されます。

特定の Linux SSHへの接続を有効にする WorkSpace

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

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

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
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 WorkSpace を有効にする のプライベート IP アドレスを入力します。
4. [セキュリティグループ] 列で、セキュリティグループのリンクをクリックします。
5. [インバウンド] タブで、[編集] を選択します。
6. [ルールの追加] を選択し、次の操作を行います。
   - [Type] (タイプ) で、SSH を選択します。
   - Protocol では、 を選択すると が自動的に指定TCPされますSSH。
   - ポート範囲 では、 を選択すると 22 が自動的に指定されますSSH。
   - ソース 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 の場合`203.0.113.25`、 を指

定203.0.113.25/32してこの単一のIPv4アドレスをCIDR表記で一覧表示します。会社が特定の範囲からアドレスを割り当てている場合、203.0.113.0/24 などの範囲全体を指定します。

- [説明] (オプション) に、ルールの説明を入力します。

7. [Save] を選択します。

Linux または Pu WorkSpace を使用して Linux に接続するTTY

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すると、ユーザーや他のユーザーは Linux または PuTTY を使用してデバイスから に接続できます WorkSpaces。

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

Linux WorkSpace を使用して Linux に接続するには

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

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

以下は、 SSH コマンドの例です。

- *NetBIOS_NAME* は任意の会社です
- *Username* は janedoe
- *WorkSpace IP* は 203.0.113.25 です

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

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

Pu WorkSpace を使用して Linux に接続するにはTTY

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

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

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

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

   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. 開く をクリックします。
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 パスワード) を入力します。

WorkSpaces Personal に必要な設定とサービスコンポーネント

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

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

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

Windows 向けの必須のサービスコンポーネント

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

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

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

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に干渉しないことを確認してください。

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

32 ビットPCoIPエージェント

2021 年 3 月 29 日現在、PCoIPエージェントを 32 ビットから 64 ビットに更新しました。PCoIP プロトコル WorkSpaces を使用している Windows の場合、これは Teradici ファイルの場所が か

ら C:\Program Files (x86)\Teradiciに変更されることを意味しますC:\Program Files \Teradici。通常のメンテナンス期間中にPCoIPエージェントを更新したため、移行中に一部の で 32 ビットエージェントが他の よりも長く使用されている WorkSpaces 可能性があります。

ファイアウォールルール、ウイルス対策ソフトウェアの除外 (クライアント側とホスト側) 、グループポリシーオブジェクト (GPO) の設定、または 32 ビットエージェントへのフルパスに基づく Microsoft System Center Configuration Manager (SCCM) 、Microsoft Endpoint Configuration Manager、または同様の設定管理ツールの設定を構成している場合は、それらの設定に 64 ビットエージェントへのフルパスも追加する必要があります。

32 ビット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、必ず 64 ビットバージョンのコンポーネントにパスを追加してください。すべての WorkSpaces が同時に更新されない可能性があるため、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。置き換えないと、 の一部が機能しない WorkSpaces 場合があります。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 — 64 PCoIP ビットエージェントを使用するように が更新されると、arbiter サービス (C:\Program Files (x86)\Teradici\PCoIP Agent\bin \pcoip_arbiter_win32.exe) WorkSpaces が削除されることに注意してください。

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

Linux 向けの必須のサービスコンポーネント

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

> **Note**
>
> 以外のファイルを変更すると/etc/pcoip-agent/pcoip-agent.conf、 が機能し WorkSpaces なくなり、再構築が必要になる場合があります。/etc/pcoip-agent/

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

- /etc/X11/default-display-manager
- /etc/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 では WorkSpaces、サービスコンポーネントは次の場所にインストールされます。これらのオブジェクトを削除、変更、ブロック、または隔離しないでください。これを行うと WorkSpace、 は正しく機能しません。

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

- /etc/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、 およびユーザーの情報を保存 WorkSpaces および管理します。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、オンプレミス認証情報 WorkSpaces を使用して にサインインし、 からオンプレミスリソースにアクセスできます WorkSpaces。
- 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 ID ソースとして使用するディレクトリを作成します (IAM Identity Center 経由 ）。ディレクトリ WorkSpaces 内の Personal は、Microsoft Entra のネイティブ認証を使用して参加し、Microsoft Windows Autopilot ユーザー駆動モードを介して 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 Bring Your Own Licenses のみをサポートします WorkSpaces。
- カスタム — 選択した ID プロバイダーを使用するディレクトリを (IAM Identity Center を介して) 作成します。 ディレクトリ WorkSpaces 内の は、選択したデバイス管理ソリューションを使用して管理されます JumpCloud。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 Bring Your Own Licenses のみをサポートします WorkSpaces。

これらのディレクトリの設定方法と起動方法を示すチュートリアルについては WorkSpaces、「」を参照してくださいWorkSpaces Personal のディレクトリを作成する。

> **Tip**
>
> さまざまなデプロイシナリオにおけるディレクトリと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 をデプロイするためのベストプラクティス WorkSpaces」を参照してください。

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。一部のディレクトリ管理タスクは、 WorkSpaces コンソールを使用して実行でき、他のタスクはグループポリシーを使用して実行できます。ユーザーとグループの管理の詳細については、 WorkSpaces Personal で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

- 共有ディレクトリは、現在 Amazon での使用はサポートされていません WorkSpaces。
- マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを Amazon で使用するために登録できます WorkSpaces。Amazon で使用するレプリケートされたリージョンにディレクトリを登録しようとすると、失敗 WorkSpaces します。 AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内の Amazon WorkSpaces での使用はサポートされていません。
- Simple AD と AD Connector は無料で使用できます WorkSpaces。Simple AD または AD Connector ディレクトリで 30 日間連続して使用 WorkSpaces されていない場合、このディレクトリは自動的に登録解除され WorkSpaces、AWS Directory Service 料金条件に従ってこのディレクトリに対して課金されます。

  空のディレクトリを削除するには、 WorkSpaces Personal の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すると、WorkSpaces を再度使用するときにいつでも新しいディレクトリを作成できます。

内容

- WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する
- WorkSpaces Personal の組織単位を選択する
- WorkSpaces Personal の自動パブリック IP アドレスを設定する
- WorkSpaces Personal のデバイスのアクセスコントロール
- WorkSpaces Personal でローカル管理者のアクセス許可を管理する
- WorkSpaces Personal の AD Connector アカウント (AD Connector) を更新する
- WorkSpaces Personal の多要素認証 (AD Connector)
- WorkSpaces Personal のディレクトリを作成する

- WorkSpaces Personal のDNSサーバーを更新する
- WorkSpaces Personal のディレクトリを削除する
- AWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする
- WorkSpaces Personal で Active Directory 管理ツールを設定する

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

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

要件

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

- 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 VPC が配置されている にアクセスできる限り、ディレクトリ WorkSpaces は専用のプライベートサブネット内に配置できます。

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

> **Note**
>
> Simple AD と AD Connector は無料で使用できます WorkSpaces。Simple AD または AD Connector ディレクトリで 30 日間連続して使用 WorkSpaces されていない場合、このディレクトリは自動的に登録解除され WorkSpaces、AWS Directory Service 料金条件に従ってこのディレクトリに対して課金されます。
> 空のディレクトリを削除するには、 WorkSpaces Personal の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すると、WorkSpaces を再度使用するときにいつでも新しいディレクトリを作成できます。

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

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

2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [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で、 WorkSpaces タイプに Personal を選択します。WorkSpace デバイス管理では、 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からではない のサブネットVPCを 2 つ選択します。これらのサブネットは の起動に使用されます WorkSpaces。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. セルフサービスのアクセス許可を有効にする ではい を選択して、ユーザーが を再構築したり WorkSpaces、ボリュームサイズを変更したり、コンピューティングタイプや実行モードを変更したりできるようにします。を有効にすると、Amazon の支払い額に影響する可能性があります WorkSpaces。それ以外の場合は [いいえ] を選択します。
8. Amazon を有効にする WorkDocs ではい を選択して、Amazon で使用するディレクトリを登録する WorkDocs か、いいえ を選択します。

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

9. [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、個人用を作成できます WorkSpace。詳細については、「 WorkSpaces Personal WorkSpace で を作成する」を参照してください。

でディレクトリの使用が終了したら WorkSpaces、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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [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 Managed Microsoft AD、Simple AD など、AWS Directory Service を通じて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/ 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. [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. [Save] 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 WorkSpace で 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、「VPC WorkSpaces 個人用の 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/ 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

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、WorkSpaces 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。

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/ 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. [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 の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. [Save] 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 Managed Microsoft AD、Simple AD など、AWS Directory Service を通じて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/ 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. 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. [Save] 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/ 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、[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. [Save] 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。AWS Directory Service での多要素認証の使用の詳細については、AD Connector の多要素認証を有効にするおよび AD Connector の前提条件を参照してください。

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

多要素認証を有効にするには

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

2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [Multi-Factor Authentication] を展開し、[Enable Multi-Factor Authentication] を選択します。
5. [RADIUS server IP address(es)] に、カンマで区切られた RADIUS サーバーのエンドポイントの IP アドレスを入力するか、RADIUSサーバーのロードバランサーの IP アドレスを入力します。
6. [Port] に、RADIUS サーバーが通信で使用しているポートを入力します。オンプレミスネットワークでは、AD Connector からのデフォルトの RADIUS サーバーポート (UDP:1812) を介した受信トラフィックが許可されている必要があります。
7. [Shared secret code] と [Confirm shared secret code] に、RADIUS サーバーの共有シークレットコードを入力します。
8. [Protocol] で、RADIUS サーバープロトコルを選択します。
9. [Server timeout] に、RADIUS サーバーの応答を待つ時間を秒単位で入力します。この値は 1 ~ 50 の範囲の値にする必要があります。
10. [Max retries] に、RADIUS サーバーとの通信を試行する回数を入力します。この値は 0 ~ 10 の範囲の値にする必要があります。
11. [Update and Exit] を選択します。

多要素認証は、[RADIUS Status] が [Enabled] になると使用できます。多要素認証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、 によって管理されるディレクトリを使用して、 WorkSpaces およびユーザーの情報 AWS Directory Service を保存および管理できます。Personal WorkSpaces 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。
- 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**
>
> - 共有ディレクトリは、現在 Amazon での使用はサポートされていません WorkSpaces。
> - マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを Amazon で使用するために登録できます WorkSpaces。Amazon で使用するレプリケートされたリージョンにディレクトリを登録しようとすると、失敗 WorkSpaces します。 AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内の Amazon WorkSpaces での使用はサポートされていません。
> - Simple AD と AD Connector は無料で使用できます WorkSpaces。Simple AD または AD Connector ディレクトリで 30 日間連続して使用 WorkSpaces されていない場合、このディレクトリは自動的に登録解除され WorkSpaces、AWS Directory Service 料金条件に従って課金されます。

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、 のリージョンを選択します WorkSpaces。サポートされているリージョンの詳細については、WorkSpaces AWS 「リージョン別の料金表」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、「VPC WorkSpaces 個人用の を設定する」を参照してください。は、仮想プライベートネットワーク (VPN) 接続または を介してオンプレミスネットワークに接続VPCする必要があります 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。
- からインターネットへのアクセスを提供します WorkSpace。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 の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すると、WorkSpaces を再度使用するときにいつでも新しいディレクトリを作成できます。

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 で 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
- AWS Managed Microsoft AD ディレクトリと WorkSpaces Personal のオンプレミスドメインの間に信頼関係を作成する
- WorkSpaces Personal を使用して専用の 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 WorkSpace の に表示されるコンピュータ名値は、起動 WorkSpace した のタイプ (Amazon Linux、Ubuntu、または Windows) によって異なります。のコンピュータ名は、次のいずれかの形式 WorkSpace になります。

- 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 の場合 WorkSpaces、コンピュータ名の形式はバンドルタイプによって決まります。パブリックバンドルまたはパブリックイメージに基づくカスタムバンドルから WorkSpaces 作成された場合は、パブリックイメージが作成された時点によって決まります。

2020 年 6 月 22 日以降、パブリックバンドルから WorkSpaces 起動される Windows では、IPWSAMZN-*xxxxxxx*C*xxxxxx* 形式ではなく、コンピュータ名の - 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の場合、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* 形式または EC2AMAZ-*xxxxxxx* 形式が使用されます。

カスタムまたはBYOLバンドル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デフォルトを上書きします。カスタム形式を指定するには、WorkSpaces Personal 用のカスタム 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、 で コマンドを使用して、 WorkSpace またはリモートRename-Computerで 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 WorkSpace の に表示されます。

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

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

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

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. [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 Directory Service で[ディレクトリを設定] 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。パスワードの要件に関する詳細については、AWS Directory Service 管理ガイドの AWS Managed Microsoft AD ディレクトリを作成するを参照してください。

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

   f. [VPC] では、作成した VPC を選択します。

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

   h. [Next Step] を選択します。

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き、AWS Directory Service は、2 つのディレクトリサーバー (VPC のプライベートサブネットごとに 1 つ) を作成します。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 WorkSpace で 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/ 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. [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 Directory Service で[ディレクトリを設定] 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 の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/ 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. [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 Directory Service で[ディレクトリを設定] 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。

AWS Managed Microsoft AD ディレクトリと WorkSpaces Personal の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 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 WorkSpaces を使用すると、信頼されたドメインのユーザー WorkSpaces に対して 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. 仮想プライベートクラウド () に AWS Managed Microsoft AD を設定しますVPC。詳細については、 AWS Directory Service 管理ガイドのAWS 「 Managed Microsoft AD ディレクトリの作成」を参照してください。

   > **Note**
   >
   > - 共有ディレクトリは、現在 Amazon での使用はサポートされていません WorkSpaces。
   > - 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 で使用するために登録できます WorkSpaces。Amazon で使用するレプリケートされたリージョンにディレクトリを登録しようとすると、失敗 WorkSpaces します。 AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内の 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。

一方向または双方向の信頼を使用して を管理および認証し WorkSpaces、 を WorkSpaces オンプレミスのユーザーおよびグループにプロビジョニングできます。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 SSSDは、Active Directory 統合に System Security Services Daemon (SSSD) WorkSpaces を使用し、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 には双方向の信頼をお勧めします WorkSpaces。
> - ウェブブラウザ (ウェブアクセス) を使用して Linux に接続することはできません WorkSpaces。

WorkSpaces Personal を使用して専用の 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 が参加し、Microsoft Intune に登録 WorkSpaces されている Bring Your Own License (BYOL) Windows 10 および 11 の個人を作成します。これを作成する前に WorkSpaces、まず Entra ID 参加専用の WorkSpaces Personal ディレクトリを作成する必要があります WorkSpaces。

> **Note**
>
> Microsoft Entra 参加の個人 WorkSpaces は WorkSpaces 、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 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。

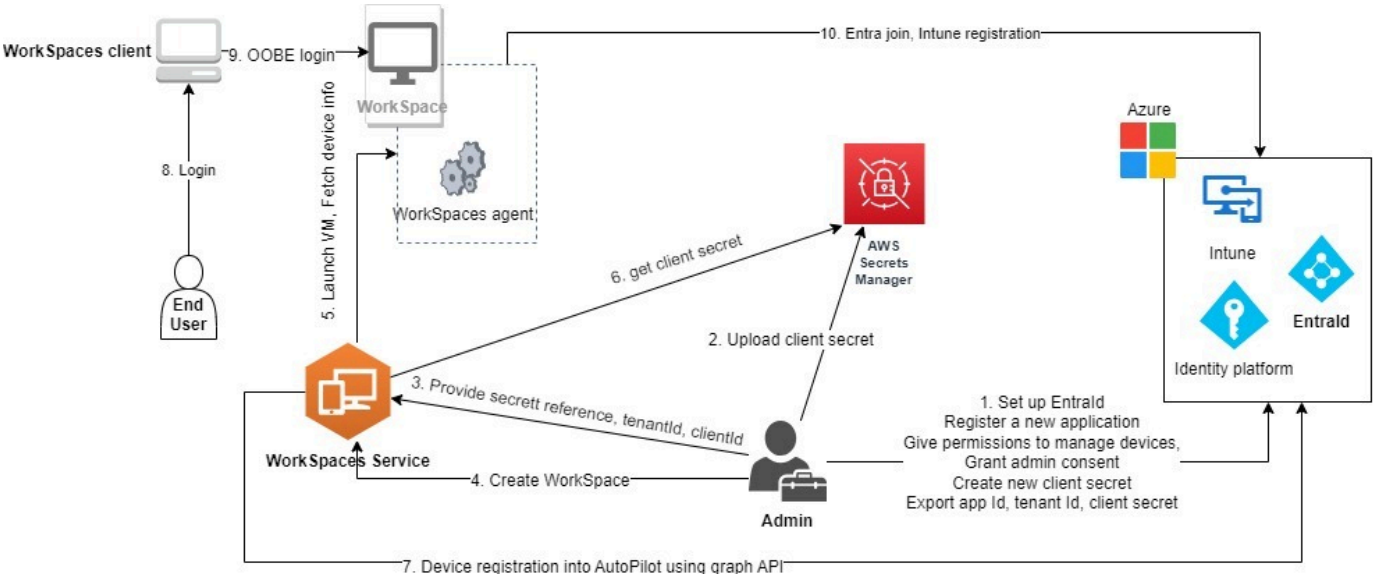
内容

- 概要
- 要件と制限
- ステップ 1: IAM Identity Center 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 Identity Center アプリケーションを設定する (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 WorkSpaces されているユーザーに割り当てられた Microsoft Entra ID 参加の起動に必要なすべての情報が含まれています。ユーザー情報は、アイデンティティセンター WorkSpaces を通じて AWS IAM で利用できるようになります。アイデンティティセンターは、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。Microsoft Windows Autopilot ユーザー駆動モードは、Intune WorkSpaces 登録と Entra join を実行するために使用されます。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 で作成したアプリケーションに割り当てられたAPIアクセス許可につい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。

- Windows 10 または 11 を Entra ID に参加できるように WorkSpaces 、VDAE3/E5 ユーザーサブスクリプションライセンスをユーザーに割り当てます。
- Entra ID ディレクトリは、Windows 10 または 11 Bring Your Own License Personal のみをサポートします WorkSpaces。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 アカウントで有効になっており、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、「で独自の Windows デスクトップライセンスを使用する WorkSpaces」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個人のみをサポートします WorkSpaces。
- 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 Identity Center 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を作成して Entra ID ユーザー WorkSpaces に割り当てるには、IAMIdentity Center AWS を通じてユーザー情報を で使用できるようにする必要があります。IAMIdentity 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「 Identity Center とは」を参照してください。これは 1 回限りの設定です。

> **Note**
>
> WorkSpaces Personal ディレクトリとそれに関連付けられた IAM Identity Center インスタンスは、同じ AWS リージョンに存在する必要があります。

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 Identity Center 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、「 アイデンティティセンターの有効化 AWS IAM」を参照してください。各 WorkSpaces ディレクトリは、1 つの IAM Identity Center 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いて、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する場合は、次の IAM Identity Center 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、サービスコントロールポリシー (SCPs) がこれらのアクセス許可をブロックしていないことを確認してください。の詳細についてはSCPs、「サービスコントロールポリシー (SCPs) 」を参照してください。

2. IAM 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 Identity Center インスタンスに自動的に同期するように IAM Identity Center と Microsoft Entra ID を設定します。詳細については、「Microsoft Entra ID SAMLと IAM Identity Center SCIMで と 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 Identity Center を設定する AWS IAM」を参照してください。
3. Microsoft Entra ID で設定したユーザーが Identity Center インスタンスに AWS IAM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 のユーザーが IAM Identity Center がサポートしていないように設定されていることを示します。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 Identity Center への同期に失敗する」を参照してください。

> **Note**
>
> WorkSpaces は Entra ID UserPrincipalName （ UPN) 属性を使用して個々のユーザーを識別します。その制限は次のとおりです。
>
> - UPNs は 63 文字を超えることはできません。
> - をユーザーに割り当てUPNた後 WorkSpace に を変更した場合、 を以前のUPN状態に戻さない限り、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 ユーザー駆動モードを使用して Microsoft Intune WorkSpaces に登録し、Microsoft Entra ID に結合します。

Amazon WorkSpaces が WorkSpaces Personal を Autopilot に登録できるようにするには、必要な Microsoft Graph アクセスAPI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 に結合 WorkSpace する必要がある新しい個人を作成するには、次のAPIアクセス許可が必要です。
  - `DeviceManagementServiceConfig.ReadWrite.All`
- 個人用の を終了 WorkSpace したり、再構築したりすると、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指定しない場合、 WorkSpace は終了しますが、Intune および Entra ID テナントから削除されないため、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. 個人用の新しい Autopilot デバイスグループを作成します WorkSpaces。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 で作成した Entra ID WorkSpaces Personal ディレクトリのディレクトリ名と一致する必要があります。これは、 が仮想デスクトップを Autopilot に登録するときに WorkSpaces 、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 画面で、 エクスペリエンス (OOBE) Out-of-boxページ。[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 に参加している個人のコンピュータ名をカスタマイズするには、「はい」の「デバイス名の適用」テンプレート WorkSpaces を選択し、登録時にデバイスに名前を付けるとき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、 で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。デフォルト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。デフォルトキーには WorkSpaces サービスからアクセスできません。キーは以下の手順で作成します。

   a. https://console.aws.amazon.com/kms で AWS KMS コンソールを開きます。
   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. レビューページのキーポリシーエディタで、キーポリシーに次のworkspaces.amazonaws.comアクセス許可を含めることで、サービスのプリンシパルにキーへのアクセスを許可していることを確認します。WorkSpaces

```
{
    "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、 でシークレットを作成します。

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

   b. [新しいシークレットを保存] 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. 暗号化 AWS KMS キードロップダウンリストから、前のステップで作成したキーを選択します。

   g. [Next (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workspaces.amazonaws.comアクセス許可に次のリソースポリシーを含めることで、 WorkSpaces サービスのプリンシパルがシークレットにアクセスできるようにします。

```
{
```

```
  "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 参加ユーザー WorkSpaces と Entra ID ユーザーに関する情報を保存する専用 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. ディレクトリの作成ページで、 WorkSpaces タイプに Personal を選択します。WorkSpace デバイス管理では、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 を WorkSpace 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 とそのパスワードを含むシークレットの内容は、 の AWS Secrets Manager コンソールからいつでも更新できますhttps://console.aws.amazon.com/secretsmanager/。
6. 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 Identity Center インスタンスを選択します。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 Identity Center インスタンスを変更することはできません。
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、個人を WorkSpaces 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. でVPC、 の起動VPCに使用した を選択します WorkSpaces。詳細については、「VPC WorkSpaces 個人用の を設定する」を参照してください。
10. サブネット では、同じアベイラビリティーゾーンからではない のサブネットVPCを 2 つ選択します。これらのサブネットは、個人用の を起動するために使用されます WorkSpaces。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 WorkSpaces 起動された にインターネットアクセスがあることを確認します。これは、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、専用を有効にする WorkSpace を選択します。Bring Your Own License (BYOL) Windows 10 または 11 Personal を起動する専用の WorkSpaces Personal ディレクトリを作成するには、これを有効にする必要があります WorkSpaces。

> **Note**
>
> 設定 に専用オプションを有効にする WorkSpace が表示されない場合、アカウントは に対して有効になっていませんBYOL。アカウントBYOLで を有効にするには、「」を参照してくださいで独自の Windows デスクトップライセンスを使用する WorkSpaces。

12. （オプション) タグで、 ディレクトリ WorkSpaces 内の個人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。

また、ディレクトリが作成されると、ユーザーに代わって IAM Identity Center 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 を検索するには、ディレクトリの概要ページARNに移動します。

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

WorkSpaces ディレクトリの IAM Identity Center 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 Identity Center 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 は、ディレクトリの詳細ページの「概要」セクションARNにあります。デフォルトでは、Identity Center インスタンスのすべてのユーザーは、対応する Identity Center アプリケーションを設定 WorkSpaces せずに、割り当てられた にアクセスできます。ただし、IAMIdentity Center 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 WorkSpaces 内の へのユーザーアクセスを管理できます。

IAM Identity Center 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. https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
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 の形式です。 `WorkSpaces.wsd-xxxxx`は WorkSpaces ディレクトリ ID `wsd-xxxxx`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、Identity Center 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 WorkSpaces ていない限り、割り当て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。

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 の BYOL 個人用 WorkSpaces を作成して、AWS IAM アイデンティティセンター ID プロバイダー (IdP) 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) を除き、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
- 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
- ステップ 2: 専用のカスタム WorkSpaces ディレクトリを作成する

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 アカウントの BYOL を有効にし、Windows 10 および 11 のアクティベーションのために個人用 WorkSpaces が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、「で独自の Windows デスクトップライセンスを使用する WorkSpaces」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事前にインストールしておきます。

ステップ 1: IAM アイデンティティセンター を有効にして 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 アイデンティティセンターを通じてユーザー情報を AWS で利用できるようにする必要があります。AWS リソースにアクセスするユーザーの管理には、IAM アイデンティティセンターを使用することをお勧めします。詳細については、「IAM Identity Center 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 AWS で利用できるようにするには

1. AWS で IAM アイデンティティセンターを有効にします。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 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、「AWS IAM アイデンティティセンターの有効化」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 AWS IAM アイデンティティセンターの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/ 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. [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、「VPC WorkSpaces 個人用の 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 WorkSpace で 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 WorkSpace で 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

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

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

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

Active Directory DNSの設定を更新する WorkSpaces 前に、 DNSの設定を更新することをお勧めします (次の手順のステップ 1 で説明) 。

WorkSpaces 代わりに を再構築する場合は、Active Directory のDNSサーバー IP アドレスの 1 つを更新し (ステップ 2) 、 の手順に従って WorkSpaces Personal WorkSpace で を再構築するを再構築します WorkSpaces。を再構築したら WorkSpaces、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、 を再構築します WorkSpaces。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 アドレスは一度に 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、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 サーバー設定を変更する WorkSpaces 15 分前と 15 分後に新しい 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 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: のDNSサーバー設定を更新する WorkSpaces

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 のDNSサーバー設定を更新する WorkSpaces

複数の 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 WorkSpaces することで、次のレジストリ更新を にデプロイできます WorkSpaces。GPOs の使用方法の詳細については、「Personal WorkSpaces で Windows WorkSpaces を管理する」を参照してください。

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

DNS レジストリエディタを使用してレジストリ設定を更新するには

1. Windows で WorkSpaceWindows の検索ボックスを開き、 と入力**registry editor**してレジストリエディタ () を開きますregedit.exe。
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. を再起動するか WorkSpace、サービスを再起動します SkyLightWorkspaceConfigService。

> **Note**
>
> サービスを再起動した後 SkyLightWorkspaceConfigService、ネットワークアダプタに変更が反映されるまでに最大 1 分かかることがあります。

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

を使用してDNSレジストリ設定を更新するには PowerShell

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、サービスを再起動します SkyLightWorkspaceConfigService。

1. Windows で WorkSpace、Windows の検索ボックスを開き、 と入力します**powershell**。[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 に変更します*NewIP1*。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、サービス を再起動します SkyLightWorkspaceConfigService。

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

> **Note**
>
> サービスを再起動した後 SkyLightWorkspaceConfigService、ネットワークアダプタに変更が反映されるまでに最大 1 分かかることがあります。

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

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

複数の Amazon Linux 2 がある場合は WorkSpace、設定管理ソリューションを使用してポリシーを配布および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 のDNSサーバー設定を更新するには WorkSpace

1. Linux で WorkSpace、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
```

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

Ubuntu のDNSサーバー設定を更新する WorkSpaces

複数の Ubuntu がある場合は WorkSpace、設定管理ソリューションを使用してポリシーを配布および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 のDNSサーバー設定を更新するには WorkSpace

1. Ubuntu で WorkSpace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 IP 追加がある場合は、カンマ区切りの値として追加します。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. コマンドを実行してresolvectl status、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 でDNSサーバー設定を更新します。

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

複数の Red Hat Enterprise Linux がある場合は WorkSpace、設定管理ソリューションを使用してポリシーを配布および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 のDNSサーバー設定を更新するには WorkSpace

1. Red Hat Enterprise Linux で WorkSpace、ターミナルウィンドウを開き、以下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ます。

```
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には、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 で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 アドレスは一度に 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 管理ガイドの以下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: DNS オンプレミスドメインの条件付きフォワーダーを設定する
- Simple AD: を設定する DNS

DNS サーバー設定を更新したら、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 を完了したら、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動作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 の更新されたDNSサーバー設定をテストする WorkSpaces

1. *OldIP1* DNS サーバーをシャットダウンします。
2. Windows にログインします WorkSpace。
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、回答で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 を *OldIP2*に置き換えます*NewIP2*。次に、ステップ 2 とステップ 3 を繰り返します。

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

1. *OldIP1* DNS サーバーをシャットダウンします。
2. Linux にログインします WorkSpace。
3. Linux で WorkSpace、ターミナルウィンドウを開きます。
4. DHCP レスポンスで返されるDNSサーバー IP アドレスは、 のローカル/etc/resolv.confファイルに書き込まれます WorkSpace。/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すると、 WorkSpace を再起動すると、そ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 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、回答で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 を *OldIP2*に置き換えます*NewIP2*。次に、ステップ 2 とステップ 3 を繰り返します。

WorkSpaces Personal のディレクトリを削除する

> **Note**
>
> Simple AD と AD Connector は無料で使用できます WorkSpaces。Simple AD または AD Connector ディレクトリで 30 日間連続して使用 WorkSpaces されていない場合、このディレクトリは自動的に登録解除され WorkSpaces、AWS Directory Service 料金条件に従ってこのディレクトリに対して課金されます。
> Simple AD または AD Connector ディレクトリを削除すると、 WorkSpaces を再度使用するときにいつでも新しいディレクトリを作成できます。

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 ディレクトリが削除されると、ディレクトリデータとスナップショットはすべて削除され、復元することはできません。ディレクトリを削除すると、ディレクトリに結合されている Amazon EC2インスタンスはそのまま残ります。ただし、ディレクトリの認証情報を使用して、これら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インスタンスもそのまま残り、オンプレミスディレクトリに結合されたままになります。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 を作成できますBYOL WorkSpaces。詳細については、「WorkSpaces Personal を使用して専用の 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 ドメインに参加していない WorkSpaces を作成できますが、独自のデバイス管理ソフトウェアと IAM Identity Center を使用できます。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 WorkSpaces 内のすべての 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

Amazon、Amazon、または Amazon Chime などの他の WorkSpacesアプリケーションによって使用されなくなった WorkSpaces 場合は WorkDocs WorkMail、 の AWS Directory Service ディレクトリを削除できます。ディレクトリを削除する前に、ディレクトリの登録を解除する必要があります。

ディレクトリの登録を解除するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [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 WorkSpaces 内のすべての 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
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) 内のすべてのリソースを削除した後、 を削除VPCし、NATゲートウェイに使用される 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「 の削除VPC」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。

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

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

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

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

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

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

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

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

WorkSpaces 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集中化することをお勧めします。ディレクトリ管理ツールは WorkSpace にインストールすることができますが、Amazon EC2 インスタンスを使用する方がより堅実なソリューションとなります。

Active Directory 管理ツールを設定するには

1. Amazon EC2 Windows インスタンスを起動し、次のいずれかのオプションを使用して WorkSpaces ディレクトリに結合します。

   - 既存の Amazon EC2 Windows インスタンスがない場合は、インスタンスの起動時に、そのインスタンスをディレクトリドメインに結合できます。詳細については、AWS Directory Service 管理ガイドの Windows EC2 インスタンスにシームレスに参加するを参照してください。
   - 既存の Amazon EC2 Windows インスタンスがある場合は、手動でディレクトリに結合できます。詳細については、AWS Directory Service 管理ガイドの Windows インスタンスを手動で追加するを参照してください。

2. Amazon EC2 Windows インスタンスに Active Directory 管理ツールをインストールします。詳細については、AWS Directory Service 管理ガイドの Active Directory 管理ツールのインストールを参照してください。

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

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

3. ディレクトリ管理者として、ツールを次のように実行します。

a. Windows の [スタート] メニューで、[Windows 管理ツール] を開きます。

b. Shift キーを押しながら、使用するツールへのショートカットを右クリックし、[別のユーザーとして実行] を選択します。

c. 管理者のサインイン認証情報を入力します。Simple AD の場合、ユーザー名は **`Administrator`** で、AWS Managed Microsoft AD の場合、管理者は **`Admin`** です。

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

ユーザーをディレクトリ管理者に昇格するには

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

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

   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

ユーザーを追加または削除するには

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

> **Important**
>
> ユーザーを削除する前に、ユーザーに割り当てられた WorkSpace を削除する必要があります。詳細については、「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 AWS Managed Microsoft AD のユーザーとグループの管理を参照してください。
- Simple AD を使用している場合は、AWS Directory Service 管理ガイドのSimple AD でユーザーとグループを管理するを参照してください。
- AD Connector または信頼関係を使用して Microsoft Active Directory を使用する場合は、Active Directory モジュールを使用してユーザーとグループを管理できます。

ユーザーのパスワードをリセットするには

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

> **Note**
>
> AD Connector を使用している場合、またはユーザーが AWSGovCloud (米国西部) リージョンにいる場合、ユーザーは自分のパスワードをリセットできません。([パスワードを忘れた場合] オプションは、WorkSpaces クライアントアプリケーションのログイン画面では使用できません。)

WorkSpaces 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 でユーザーを管理する
- WorkSpaces Personal でユーザー WorkSpaces 用に複数の を作成する
- 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
- 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 Personal でユーザーの Amazon Connect オーディオ最適化を有効にする
- WorkSpaces Personal で診断ログのアップロードを有効にする

WorkSpaces Personal でユーザーを管理する

の管理者は WorkSpaces、次のタスクを実行して WorkSpaces ユーザーを管理できます。

ユーザー情報を編集する

WorkSpaces コンソールを使用して、 のユーザー情報を編集できます WorkSpace。

> **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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、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。Active WorkSpaces 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、ディレクトリのほとんどの管理タスクを実行します。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、そのユーザー WorkSpace に割り当てられた 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AWS 「 Managed Microsoft 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。
- 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. WorkSpaces ページで、検索ボックスを使用して招待を送信するユーザーを検索し、検索結果 WorkSpace から対応するユーザーを選択します。一度に選択できる は 1 WorkSpace 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. ページにユーザーを招待 WorkSpace で、招待の送信 を選択します。

WorkSpaces Personal でユーザー WorkSpaces 用に複数の を作成する

デフォルトでは、ディレクトリ WorkSpace ごとにユーザーごとに 1 つのみ作成できます。ただし、必要に応じて、ディレクトリの設定に応じて、ユーザー WorkSpace 用に複数の を作成できます。

- のディレクトリが 1 つしかない場合は WorkSpaces、ユーザー用に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 WorkSpace 内の異なる に関連付けられていますが、 はすべて同じ 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、 の登録コード WorkSpaces は同じ WorkSpaces です。
- に複数のディレクトリがある場合は WorkSpaces、個別のディレクトリに WorkSpaces ユーザーの を作成します。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。の登録コード WorkSpaces は異なります。

> **Tip**
>
> ユーザー用に WorkSpaces 作成したすべての を簡単に見つけられるように、それぞれに同じ基本ユーザー名を使用します WorkSpace。

例えば、Active Directory のユーザー名が mmajor の Mary Major という名前のユーザーがいる場合は、mmajor、mmajor1、mmajor2、mmajor3、または mmajor_windows や mmajor_linux などの他のバリアントなどのユーザー名 WorkSpaces で を作成します。すべての に同じ開始基本ユーザー名 (mmajor) WorkSpaces がある限り、 WorkSpaces コンソールでユーザー名でソートして、 WorkSpaces そのユーザーのすべての をグループ化できます。

Important

- ユーザーは、2 つの WorkSpaces が別々のディレクトリにあるDCV WorkSpace 限り、 PCoIPと の両方を持つことができます。同じユーザーが同じディレクトリDCV WorkSpace に PCoIPと を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 WorkSpaces 複数の を設定する場合は、異なる AWS リージョン WorkSpaces の異なるディレクトリに 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。

を切り替えるために WorkSpaces、ユーザーは特定の Workspace に関連付けられたユーザー名と登録コードでログインします。ユーザーが Windows、macOS、または Linux 用の 3.0 以降のバージョンの WorkSpaces クライアントアプリケーションを使用している場合、ユーザーはクライアントアプリケーションの「設定」、「ログイン情報の管理」に移動 WorkSpaces して、 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/ 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. 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、「Personal WorkSpace で を変更する WorkSpaces 」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 で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. [Save] 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 マネジメントコンソールでは、フリー WorkSpaces トの Amazon Connect Contact Control Panel (CCP) 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 オーディオの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 内CCPから を操作できます WorkSpaces。

Amazon Connect 問い合わせコントロールパネル (CCP) の音声最適化は、以下と連携します。

- WorkSpaces Windows クライアント。
- Amazon Linux および Windows WorkSpaces。
- WorkSpaces PCoIPまたは を使用するDCV。

要件

- Amazon Connect で設定する必要があります。
- 通話シグナリング用のメディアCCPなしで APIを作成して、Amazon Connect Stream CCPでカスタム を構築する必要があります。これにより、メディアは標準 を使用してローカルデスクトップで処理されCCP、シグナリングと通話の制御はメディアCCPなしで とのリモート接続で処理されます。Amazon Connect ストリーム の詳細についてはAPI、 の GitHub リポジトリを参照してくださいhttps://github.com/aws/amazon-connect-streams。構築CCPするカスタム は、CCPAmazon Connect エージェントが 内で使用するものです WorkSpaces。
- Amazon Connect でサポートされている WorkSpaces クライアントエンドポイントに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、 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求められますCCP。

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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [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 問い合わせコントロールパネル (CCP) 名を入力します。

   > **Note**
   >
   > に付けた名前CCP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 によってURL生成された Amazon Connect 問い合わせコントロールパネルを入力します。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URL。
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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [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 問い合わせコントロールパネル名 と を更新しますURL。
9. [Save] 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [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 コンソールを使用する

1. https://console.aws.amazon.com/WorkSpaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. 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. [Save] 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 個人用の管理

WorkSpaces コンソール WorkSpaces を使用して を管理できます。

ディレクトリ管理タスクを実行するには、「the section called “ディレクトリ管理を設定する”」を参照してください。

Note

- 、ENA、および PV ドライバーなどのネットワーク依存関係ドライバーはNVMe、必ず で更新してください WorkSpaces。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、「Windows インスタンスの場合は Elastic Network Adapter (ENA) ドライバー をインストールまたはアップグレードする」および「Windows インスタンスの場合は PV ドライバーをアップグレードする」を参照してください。 AWS NVMe ドライバー

- EC2Config、EC2Launch、および EC2Launch V2 エージェントは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と の更新EC2Launch」を参照してください。

内容

- Personal WorkSpaces で Windows WorkSpaces を管理する
- Personal WorkSpaces で Amazon Linux WorkSpaces を管理する
- WorkSpaces Personal WorkSpaces で Ubuntu を管理する
- Rocky Linux を管理する WorkSpaces
- Red Hat Enterprise Linux を管理する WorkSpaces
- WorkSpaces Personal でのリアルタイム通信 WorkSpaces を最適化する
- WorkSpaces Personal で実行モードを管理する
- WorkSpaces Personal でアプリケーションを管理する
- Personal WorkSpace で を変更する WorkSpaces
- WorkSpaces Personal でブランドをカスタマイズする
- WorkSpaces Personal でリソースにタグを付ける
- WorkSpaces Personal のメンテナンス
- WorkSpaces Personal WorkSpaces で暗号化
- WorkSpaces Personal の WorkSpace を再起動する
- WorkSpaces Personal WorkSpace で を再構築する
- WorkSpaces Personal WorkSpace で を復元する
- Microsoft 365 Bring Your Own License (BYOL) in WorkSpaces Personal
- WorkSpaces Personal で Windows BYOL WorkSpaces をアップグレードする
- Personal WorkSpace で を移行する WorkSpaces
- WorkSpaces Personal で WorkSpace を削除する

Personal WorkSpaces で Windows WorkSpaces を管理する

グループポリシーオブジェクト (GPOs) を使用して、Windows WorkSpaces ディレクトリの一部である Windows WorkSpaces または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 を使用して専用の 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 の管理については WorkSpaces、「」を参照してくださいPersonal WorkSpaces で Amazon Linux WorkSpaces を管理する。

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

Amazon に固有のグループポリシー設定を使用するには WorkSpaces、使用しているプロトコルのグループポリシー管理テンプレートを PCoIPまたは のいずれかでインストールする必要がありますDCV。

> **Warning**
>
> グループポリシーの設定は、次のように WorkSpace ユーザーのエクスペリエンスに影響を与える可能性があります。
>
> - インタラクティブなログオンメッセージを実装してログオンバナーを表示すると、ユーザーは にアクセスできなくなります WorkSpaces。現在、インタラクティブの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 でサポートされておりDCV WorkSpaces、ユーザーはログオンバナーを受け入れた後で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、それらのユーザーはクライアントアプリケーションを通じて認証できなくなります。 WorkSpaces このグループポリシー設定の詳細については、Microsoft のドキュメントのリモートデスクトップサービスによるログオンを許可するを参照してください。
- ローカルセキュリティポリシーで ログを許可する から組み込みユーザーグループを削除すると、PCoIP WorkSpaces ユーザーは WorkSpaces クライアントアプリケーション WorkSpaces を介して に接続できなくなります。PCoIP WorkSpaces また、 はPCoIP エージェントソフトウェアの更新を受信しません。 PCoIP エージェントの更新には、セキュリティやその他の修正が含まれている場合や、 の新機能を有効にする場合があります WorkSpaces。このセキュリティポリシーの使用方法の詳細については、Microsoft ドキュメントのローカルでログオンを許可するを参照してください。
- グループポリシー設定は、ドライブアクセスの制限に使用できます。ドライブ C またはドライブ D へのアクセスを制限するようにグループポリシー設定を構成すると、ユーザーはその にアクセスできません WorkSpaces。この問題を回避するために、ユーザーがドライブ C およびドライブ D にアクセスできることを確認します。
- WorkSpaces オーディオ入力機能には、 内のローカルログオンアクセスが必要です WorkSpace。Windows では、オーディオ入力機能はデフォルトで有効になっています WorkSpaces。ただし、 でユーザーのローカルログオンを制限するグループポリシー設定がある場合 WorkSpaces、オーディオ入力は で機能しません WorkSpaces。そのグループポリシー設定を削除すると、 の次回の再起動後にオーディオ入力機能が有効になります WorkSpace。このグループポリシー設定の詳細については、Microsoft のドキュメントのローカルでのログオンを許可するをご参照ください。

  オーディオ入力リダイレクトの有効化または無効化の詳細については、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 PCoIP または 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 DCV を参照してください。
- グループポリシーを使用して Windows パワープランをバランス型または省電力型に設定すると WorkSpaces 、アイドル状態のときに がスリープ状態になる可能性があります。グループポリシーを使用して、Windows の電源プランを [High performance] (高パフォーマンス) に設定することを強くお勧めします。詳細については、「Windows がアイドル状態のままになるとスリープ状態 WorkSpace になる」を参照してください
- グループポリシー設定によっては、セッションから切断されているときに、ユーザーが強制的にログオフされます。ユーザーが で開いているアプリケーション WorkSpaces はすべて閉じられます。

- 「アクティブ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」は、現在 ではサポートされていませんDCV WorkSpaces。アクティビティがあり、DCVセッションがアイドル状態でない場合でも切断が発生するため、セッション中には使用しないでください。

Active Directory 管理ツールを使用して を操作する方法についてはGPOs、「」を参照してくださいWorkSpaces Personal で Active Directory 管理ツールを設定する。

内容

- のグループポリシー管理テンプレートファイルをインストールする DCV
- のグループポリシー設定を管理する DCV
- のグループポリシー管理テンプレートをインストールする PCoIP
- のグループポリシー設定を管理する PCoIP
- Kerberos チケットの最大ライフタイムを設定する
- 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
  - デスクトップトラフィックのプロキシ
  - プロキシサーバーの使用に関する推奨事項
- Amazon WorkSpaces for Zoom 会議メディアプラグインのサポートを有効にする
  - の Zoom 会議メディアプラグインを有効にする DCV
    - 前提条件
    - [開始する前に]
    - Zoom コンポーネントのインストール
  - の Zoom 会議メディアプラグインを有効にする PCoIP
    - 前提条件
    - Windows WorkSpaces ホストでレジストリキーを作成する
    - トラブルシューティング

のグループポリシー管理テンプレートファイルをインストールする DCV

を使用する WorkSpaces ときに に固有のグループポリシー設定を使用するにはDCV、 のグループポリシー管理テンプレート`wsp.admx`と`wsp.adml`ファイルを WorkSpaces ディレクトリのドメインコントローラーのDCVセントラルストアに追加する必要があります。`.admx` および `.adml` ファイルの

詳細については、「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。ディレクトリ管理 WorkSpace またはディレクトリに参加している Amazon EC2インスタンスで次の手順を実行します WorkSpaces。

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 から WorkSpace、 `C:\Program Files\Amazon\WSP` ディレクトリにファイル`wsp.admx`と `wsp.adml` ファイルのコピーを作成します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します`\\example.com`。
3. `sysvol` フォルダを開きます。
4. *`FQDN`* という名前のフォルダを開きます。
5. `Policies` フォルダを開きます。今、`\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies` に入っているはずです。
6. まだ存在しない場合は、`PolicyDefinitions` という名前のフォルダを作成します。
7. `PolicyDefinitions` フォルダを開きます。
8. `wsp.admx` ファイルを `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions` フォルダにコピーします。
9. `PolicyDefinitions` フォルダに `en-US` という名前のフォルダを作成します。
10. `en-US` フォルダを開きます。
11. `wsp.adml` ファイルを `\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US` フォルダにコピーします。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト (フォレスト:) ***FQDN***を展開します。
3. [ドメイン] を展開します。
4. を展開します FQDN (例: `example.com`) 。
5. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。

6. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

> **Note**
>
> をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して を作成することはできませんGPO。代わりに、委任された権限を持つドメインコンテナGPOで を作成してリンクする必要があります。
> でディレクトリを作成すると AWS Managed Microsoft AD、 はドメインルートの下に*yourdomainname*組織単位 (OU) AWS Directory Service を作成します。この OU の名前は、ディレクトリの作成時に入力した NetBIOS 名に基づいています。NetBIOS 名を指定しなかった場合、デフォルトでディレクトリDNS名の最初の部分になります (例えば、 の場合`corp.example.com`、NetBIOS 名は ですcorp)。
> を作成するにはGPO、デフォルトのドメインポリシーを選択する代わりに、OU (またはその下の任意の OU) *yourdomainname* を選択し、コンテキスト (右クリック) メニューを開き、このドメインGPOで を作成するを選択し、ここでリンクします。
> OU の詳細については、*yourdomainname*「 AWS Directory Service 管理ガイド」の「作成内容https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_what_gets_created.html」を参照してください。

7. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
8. このDCVグループポリシーオブジェクトを使用して、 を使用する WorkSpaces ときに に固有のグループポリシー設定を変更できるようになりましたDCV。

のグループポリシー設定を管理する DCV

グループポリシー設定を使用して、 WorkSpaces を使用する Windows を管理するには DCV

1. の最新のWorkSpaces グループポリシー管理テンプレートDCVが、 ディレクトリのドメインコントローラー WorkSpacesのセントラルストアにインストールされていることを確認します。
2. 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。

のプリンターサポートを設定する DCV

デフォルトでは、 は基本的なリモート印刷 WorkSpaces を有効にします。これは、ホスト側で汎用プリンタードライバーを使用して互換性のある印刷を行うため、印刷機能が制限されています。

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 では WorkSpaces、グループポリシー設定を使用して、必要に応じてプリンターのサポートを設定できます。

プリンターのサポートを設定するには

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します)。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

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 DCV

デフォルトでは、 は双方向 (コピー/貼り付け) のクリップボードリダイレクト WorkSpaces をサポートしています。Windows では WorkSpaces、グループポリシー設定を使用してこの機能を無効にしたり、クリップボードのリダイレクトを許可する方向を設定したりできます。

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

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

既知の制限事項

でクリップボードのリダイレクトを有効にすると WorkSpace、Microsoft Office アプリケーションから 890 KB を超えるコンテンツをコピーすると、アプリケーションが遅くなったり、最大 5 秒間応答しなくなる可能性があります。

のセッション再開タイムアウトを設定する DCV

ネットワーク接続が失われると、アクティブな WorkSpaces クライアントセッションは切断されます。Windows および macOS 用の WorkSpaces クライアントアプリケーションは、ネットワーク接続が一定時間内に復元された場合、セッションを自動的に再接続しようとします。デフォルトのセッション再開タイムアウトは 20 分 (1200 秒) ですが、ドメインのグループポリシー設定によって制御 WorkSpaces される の値を変更できます。

自動セッション再起動タイムアウト値を設定するには

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のビデオ入力リダイレクトを有効または無効にする DCV

デフォルトでは、 はローカルカメラからのデータのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のビデオ入力リダイレクトを有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

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 DCV

デフォルトでは、 はローカルマイクからのデータのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

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 DCV

デフォルトでは、 はローカルスピーカーにデータを WorkSpaces リダイレクトします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows のオーディオ出力リダイレクトを有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のタイムゾーンリダイレクトを無効にする DCV

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のようにさまざまな理由から、タイムゾーンのリダイレクトをオフにすることもできます。以下に例を示します。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

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

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します)。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。
6. のタイムゾーンを目的のタイムゾーン WorkSpaces に設定します。

のタイムゾーン WorkSpaces が静的になり、クライアントマシンのタイムゾーンがミラーリングされなくなりました。

DCV セキュリティ設定を構成する

の場合DCV、転送中のデータは 1.2 TLS 暗号化を使用して暗号化されます。デフォルトでは、次の暗号はすべて暗号化に使用でき、クライアントとサーバーはどちらの暗号を使用するかをネゴシエートします。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

Windows では WorkSpaces、グループポリシー設定を使用してTLSセキュリティモードを変更し、特定の暗号スイートを新規追加またはブロックできます。これらの設定とサポートされている暗号スイートの詳細については、[PCoIP セキュリティ設定の構成] グループポリシーダイアログボックスを参照してください。

DCV 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、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動するには WorkSpace、Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

の拡張機能を設定する DCV

デフォルトでは、 WorkSpaces 拡張機能のサポートは無効になっています。必要に応じて、次の方法で拡張機能を使用する WorkSpace ように を設定できます。

- サーバーとクライアント – サーバーとクライアントの両方の拡張機能を有効にする
- サーバーのみ – サーバーのみの拡張機能を有効にする
- クライアントのみ – クライアントのみの拡張機能を有効にする

Windows では WorkSpaces、グループポリシー設定を使用して拡張機能の使用を設定できます。

の拡張機能を設定するには DCV

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。

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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

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 DCV

デフォルトでは、Amazon WorkSpaces はセッション前認証またはセッション内認証のいずれにもスマートカードの使用をサポートしていません。セッション前認証とは、ユーザーが にログインしている間に実行されるスマートカード認証を指します WorkSpaces。セッション内認証とは、ログイン後に実行される認証をいいます。

必要に応じて、グループポリシー設定 WorkSpaces を使用して、Windows のセッション前認証とセッション内認証を有効にできます。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有効にする必要があります。詳細については、AWS Directory Service 管理ガイドの AD Connector のスマートカード認証を有効にするを参照してください。

> **Note**
>
> Windows でスマートカードを使用できるようにするには WorkSpaces、追加のステップが必要です。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 のスマートカードリダイレクトを有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。

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] を選択します。
5. グループポリシー設定の変更は、セッションの WorkSpace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、 を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します)。

の WebAuthn （ FIDO2) リダイレクトを有効または無効にする DCV

デフォルトでは、Amazon WorkSpaces はセッション内認証に WebAuthn 認証機能を使用できます。セッション内認証とは、ログイン後に実行され、セッション内で実行されているウェブアプリケーションによってリクエストされる WebAuthn 認証を指します。

要件

WebAuthn の (FIDO2) リダイレクトには、以下DCV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 Redirection Extension WorkSpaces を実行している にインストールされているウェブブラウザ：
  - Google Chrome 116 以降
  - Microsoft Edge 116 以降

Windows の WebAuthn （ FIDO2) リダイレクトの有効化または無効化 WorkSpaces

必要に応じて、グループポリシー設定を使用して、Windows の WebAuthn 認証機能によるセッション内認証のサポート WorkSpaces を有効または無効にできます。この設定を有効にするか設定しない場合、 WebAuthn リダイレクトが有効になり、ユーザーはリモート内でローカル認証機能を使用できます WorkSpace。

機能を有効にすると、セッション内のブラウザからのすべての WebAuthn リクエストがローカルクライアントにリダイレクトされます。ユーザーは、Windows Hello、 などのローカルにアタッチされたセキュリティデバイス YubiKey 、またはその他のFIDO2準拠認証ツールを使用して、認証プロセスを完了できます。

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

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
2. WebAuthn リダイレクトの有効化/無効化設定を開きます。
3. WebAuthn リダイレクトの有効化/無効化ダイアログボックスで、有効化または無効化を選択します。
4. [OK] を選択します。
5. グループポリシー設定の変更は、 WorkSpace 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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動) WorkSpacesを選択します。

Amazon DCV WebAuthn Redirection Extension のインストール

ユーザーは、次のいずれかを実行して、この機能を有効に WebAuthn した後に Amazon DCV WebAuthn Redirection Extension をインストールする必要があります。

- 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 エージェントバージョンを 2.0.0.1425 以降に更新すると、ユーザーは通知を受け取ります。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、Redirection Extension WebAuthn のインストールプロンプトをブロックすることもできます。

- 以下のGPOポリシーを使用して、ユーザーにリダイレクト拡張機能を強制インストールできます。GPO ポリシーを有効にすると、ユーザーがインターネットアクセスでサポートされているブラウザを起動すると、拡張機能が自動的にインストールされます。
- ユーザーは、Microsoft Edge アドオンまたは Chrome 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 Redirection Extension Native Messaging について

WebAuthn Chrome および Edge ブラウザでのリダイレクトでは、ブラウザ拡張機能とネイティブメッセージングホストが使用されます。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 Redirection Extension は、Active Directory (AD) ドメインに参加しているセッションホストのドメインから一元的にインストールするか、各セッションホストの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 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト (フォレスト:) ***FQDN***を展開します。
4. [ドメイン] を展開します。
5. を展開します FQDN (例: `example.com`) 。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
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] を選択します。
12. グループポリシー設定の変更は、 WorkSpace セッションの再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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動) WorkSpacesを選択します。

> **Note**
>
> 次の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、「マネージド での Chrome ブラウザポリシーの設定PCs」を参照してください。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト (フォレスト:) ***FQDN***を展開します。
4. [ドメイン] を展開します。
5. を展開します FQDN (例: `example.com`) 。
6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
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] を選択します。
12. グループポリシー設定の変更は、 WorkSpace セッションの再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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動) WorkSpacesを選択します。

> **Note**
>
> 次の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"}}
> ```

のウェブRTCリダイレクトを有効または無効にする DCV

ウェブRTCリダイレクトは、 から WorkSpaces 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を強化し、パフォーマンスを向上させ、レイテンシーを短縮します。ただし、ウェブRTCリダイレクトは一般的ではなく、サードパーティーのアプリケーションベンダーが特定の統合を開発する必要があります WorkSpaces。デフォルトでは、ウェブRTCリダイレクトは有効になっていません WorkSpaces。ウェブRTCリダイレクトを使用するには、以下を確認してください。

- 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 拡張機能は、グループポリシー設定を通じて有効になります。
- ウェブRTCリダイレクトが有効になっている
- ウェブRTC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

> **Note**
>
> このリダイレクトは拡張機能として実装され、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、ウェブRTCリダイレクトは機能しません。

要件

のウェブRTCリダイレクトには、以下DCV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 Web Redirection Extension WorkSpaces を実行している にインストールされているDCV ウェブRTCブラウザ：
  - Google Chrome 116 以降
  - Microsoft Edge 116 以降

Windows のウェブRTCリダイレクトの有効化または無効化 WorkSpaces

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

機能を有効にすると、Amazon と統合されているウェブアプリケーション WorkSpaces は、ウェブRTCAPI呼び出し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 のウェブRTCリダイレクトを有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
2. ウェブRTCリダイレクトの設定を開きます。
3. ウェブRTCリダイレクトの設定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] を選択します。

5. グループポリシー設定の変更は、 WorkSpace 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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動) WorkSpacesを選択します。

Amazon DCV WebRTC Redirection Extension のインストール

ユーザーは、次のいずれかを実行して、この機能が有効になった後にウェブRTCリダイレクトを使用するように Amazon DCV WebRTC Redirection Extension をインストールします。

- 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**
>
> 1 回限りのブラウザプロンプトとして、ウェブRTCリダイレクトを有効にすると、ユーザーに通知が送信されます。

- 次のGPOポリシーを使用して、ユーザーにリダイレクト拡張機能を強制インストールできます。GPO ポリシーを有効にすると、ユーザーがインターネットアクセスでサポートされているブラウザを起動すると、拡張機能が自動的にインストールされます。
- ユーザーは、Microsoft Edge アドオンまたは Chrome 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 Redirection Extension は、ドメインから一元的に、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グループポリシーを使用して、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 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト (フォレスト:) ***FQDN***を展開します。
4. [ドメイン] を展開します。
5. を展開します FQDN (例: `example.com`) 。

6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
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] を選択します。
12. グループポリシー設定の変更は、 WorkSpace セッションの再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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動 WorkSpacesを選択します) 。

> **Note**
>
> 次の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、「マネージド での Chrome ブラウザポリシーの設定PCs」を参照してください。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
3. フォレスト (フォレスト:) ***FQDN***を展開します。
4. [ドメイン] を展開します。
5. を展開します FQDN (例: `example.com`) 。

6. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
7. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。
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] を選択します。
12. グループポリシー設定の変更は、 WorkSpace セッションの再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 WorkSpace に移動して を選択して、 を再起動します WorkSpace。次に、アクション、再起動 WorkSpacesを選択します) 。

> **Note**
>
> 次の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"}}
> ```

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 DCV

必要に応じて、Windows ロック画面が検出されたときにユーザーの WorkSpaces セッションを切断できます。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、自分の に対して有効になっている認証のタイプに応じて、自分自身を認証できます WorkSpaces。

このグループポリシー設定は、デフォルトでは無効になっています。必要に応じて、グループポリシー設定 WorkSpaces を使用して、Windows の Windows ロック画面が検出されたときにセッションの切断を有効にできます。

> **Note**
>
> - このグループポリシー設定は、パスワード認証セッションとスマートカード認証セッションの両方に適用されます。
> - Windows でスマートカードを使用できるようにするには WorkSpaces、追加のステップが必要です。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 の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します) 。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。

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 DCV

デフォルトでは、 WorkSpaces は間接ディスプレイドライバー () の使用をサポートしています IDD。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

Windows の間接ディスプレイドライバー (IDD) を有効または無効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
2. AWS 間接表示ドライバーを有効にする 設定を開きます。
3. AWS 間接ディスプレイドライバーを有効にするダイアログボックスで、有効または無効を選択します。
4. [OK] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

   b. 管理コマンドプロンプトで、`gpupdate /force` と入力します。

の表示設定を構成する DCV

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行うことができます。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、イメージエンコーディングは YUV420 に設定されています。エンYUV444コーディングを有効にするを選択すると、高い色精度でYUV444エンコーディングが有効になります。

Windows では WorkSpaces、グループポリシー設定を使用して、最大フレームレート、最小画質、最大画質値を設定できます。

Windows の表示設定を構成するには WorkSpaces

1. グループポリシー管理工ディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

VSync の AWS 仮想表示専用ドライバーの有効化または無効化 DCV

デフォルトでは、 は AWS 仮想表示専用ドライバーVSyncの機能の使用 WorkSpaces をサポートしています。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

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

1. グループポリシー管理工ディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
2. Virtual AWS Display Only Driver 設定の Enable VSync機能を開きます。
3. AWS 仮想表示専用ドライバーVSyncの有効化 ダイアログボックスで、有効化または無効化を選択します。
4. [OK] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、以下を実行します。

a. 次のいずれか WorkSpace を実行して、 を再起動します。

   i. オプション 1 — WorkSpaces コンソールで、再起動 WorkSpace する を選択します。次に、アクション、再起動 WorkSpacesを選択します。

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

b. 設定を適用する WorkSpace には、 に再接続します。

c. WorkSpace をもう一度再起動します。

のログの詳細設定 DCV

デフォルトでは、 のログの詳細レベルDCV WorkSpaces は Info 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 では WorkSpaces、グループポリシー設定を使用してログの詳細レベルを設定できます。

Windows のログの詳細レベルを設定するには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のアイドル切断タイムアウトを設定する DCV

WorkSpaces では、ユーザーが切断される前に、 に接続している間 WorkSpaceに非アクティブにできる期間を設定できます。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 では WorkSpaces、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 のアイドル切断タイムアウトを設定するには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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。

のファイル転送を設定する DCV

デフォルトでは、Amazon はファイル転送関数を WorkSpaces 無効にします。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 セッションのマイストレージフォルダに保存されます。

Windows のファイル転送を有効にするには WorkSpaces

1. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、Amazon、 を選択しますDCV。
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. は、次のいずれかのファイル転送オプション WorkSpaces 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のアップロードのみを許可するUpload Onlyには、 を選択します。
   - セッションから WorkSpaces ローカルコンピュータへのファイルのダウンロードのみを許可するDownload Only場合は、 を選択します。
6. [OK] を選択します。
7. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、およびセッションを再開した後に有効になります WorkSpace。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のグループポリシー管理テンプレートをインストールする PCoIP

PCoIP プロトコルを使用する WorkSpaces ときに Amazon に固有のグループポリシー設定を使用するには、 に使用されているPCoIPエージェントのバージョン (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テンプレートを追加する必要があります WorkSpaces。

> **Note**
>
> を 32 ビットエージェントと 64 ビットエージェント WorkSpaces と混在させる場合は、32 ビットエージェントのグループポリシー管理テンプレートを使用できます。グループポリシー設定は 32 ビットエージェントと 64 ビットエージェントの両方に適用されます。すべての WorkSpaces が 64 ビットエージェントを使用している場合は、64 ビットエージェントの管理テンプレートの使用に切り替えることができます。

WorkSpaces に 32 ビットエージェントまたは 64 ビットエージェントがあるかどうかを確認するには

1. にログインし WorkSpace、表示、送信 Ctrl + Alt + 削除、またはタスクバーを右クリックしてタスクマネージャーを選択してタスクマネージャーを開きます。
2. タスクマネージャで、[詳細] タブに移動し、列見出しを右クリックし、[列の選択] を選択します。
3. [列の選択] ダイアログボックスで、[プラットフォーム] を選択し、[OK] をクリックします。
4. 詳細 タブで を見つけ`pcoip_agent.exe`、プラットフォーム 列でその値をチェックして、PCoIPエージェントが 32 ビットか 64 ビットかを判断します。(32 ビットと 64 ビットの WorkSpaces コンポーネントが混在している場合があります。これは正常です)。

(PCoIP32 ビット) のグループポリシー管理テンプレートをインストールする

32 ビットPCoIPエージェントでPCoIPプロトコルを使用する WorkSpaces ときに に固有のグループポリシー設定を使用するには、 のグループポリシー管理テンプレートをインストールする必要がありますPCoIP。ディレクトリ管理 WorkSpace またはディレクトリに参加している Amazon EC2インスタンスで次の手順を実行します。

.adm ファイルの操作の詳細については、マイクロソフトのドキュメントの「グループポリシー管理用テンプレート (.adm) ファイルを管理するための推奨事項」を参照してください。

のグループポリシー管理テンプレートをインストールするには PCoIP

1. 実行中の Windows から WorkSpace、 `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` ディレクトリに `pcoip.adm` ファイルのコピーを作成します。

2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、 WorkSpaces マシンアカウントを含むドメイン内の組織単位に移動します。
3. マシン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、このドメインGPO で の作成 を選択し、ここでリンクします。
4. 「新規GPO」ダイアログボックスに、WorkSpaces マシンポリシーGPOなどの のわかりやすい名前を入力し、ソーススターターGPOを （ なし ） に設定します。[OK] を選択します。
5. 新しい のコンテキスト (右クリック) メニューを開きGPO、編集を選択します。
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。これを使用してGPO、特定のグループポリシー設定を変更できるようになりました WorkSpaces。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、 WorkSpaces マシンアカウントの GPO WorkSpaces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、コンピュータ設定、ポリシー、管理テンプレート、クラシック管理テンプレート、およびPCoIPセッション変数を選択します。
3. 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、 の使用 WorkSpaces 時に Amazon に固有のグループポリシー設定を変更できるようになりましたPCoIP。

> **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。

のグループポリシー管理テンプレートをインストールする PCoIP (64 ビット)

PCoIP プロトコルを使用する WorkSpaces ときに に固有のグループポリシー設定を使用するには、のグループポリシー管理テンプレートPCoIP.admxとPCoIP.admlファイルを ディレクトリのドメインコントローラー WorkSpacesのPCoIPセントラルストアに追加する必要があります。.admx および .adml ファイルの詳細については、「Windows でグループポリシー管理用テンプレートのセントラルストアを作成および管理する方法」を参照してください。

次の手順では、セントラルストアを作成し、管理用テンプレートファイルをそのストアに追加する方法について説明します。 WorkSpaces ディレクトリ管理 WorkSpace またはディレクトリに参加している 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 から WorkSpace、 C:\Program Files\Teradici\PCoIP Agent \configuration\policyDefinitions ディレクトリに ファイルPCoIP.admxと PCoIP.adml ファイルのコピーを作成します。PCoIP.admlファイルは、そのディレクトリの en-US サブフォルダにあります。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで Windows File Explorer を開き、アドレスバーに、 などの組織の完全修飾ドメイン名 (FQDN) を入力します\\example.com。
3. sysvol フォルダを開きます。
4. *FQDN* という名前のフォルダを開きます。
5. Policies フォルダを開きます。今、*FQDN*\sysvol*FQDN*\Policies に入っているはずです。
6. まだ存在しない場合は、PolicyDefinitions という名前のフォルダを作成します。
7. PolicyDefinitions フォルダを開きます。
8. PCoIP.admx ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions フォルダにコピーします。
9. PolicyDefinitions フォルダに en-US という名前のフォルダを作成します。
10. en-US フォルダを開きます。
11. PCoIP.adml ファイルを *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US フォルダにコピーします。

管理用テンプレートファイルが正しくインストールされていることを確認するには

1. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール () を開きますgpmc.msc。
2. フォレスト (フォレスト:) ***FQDN***を展開します。
3. [ドメイン] を展開します。
4. を展開します FQDN (例: `example.com`) 。
5. [Group Policy Objects (グループポリシーオブジェクト)] を展開します。
6. [Default Domain Policy (デフォルトドメインポリシー)] を選択し、コンテキスト (右クリック) メニューを開き、[Edit (編集)] を選択します。

   > **Note**
   >
   > をバックアップするドメイン WorkSpaces が AWS Managed Microsoft AD ディレクトリの場合、デフォルトのドメインポリシーを使用して を作成することはできませんGPO。代わりに、委任された権限を持つドメインコンテナGPOで を作成してリンクする必要があります。
   > でディレクトリを作成すると AWS Managed Microsoft AD、 はドメインルートの下に*yourdomainname*組織単位 (OU) AWS Directory Service を作成します。この OU の名前は、ディレクトリの作成時に入力した NetBIOS 名に基づいています。NetBIOS 名を指定しなかった場合、デフォルトでディレクトリDNS名の最初の部分になります (例えば、 の場合`corp.example.com`、NetBIOS 名は ですcorp) 。
   > を作成するにはGPO、デフォルトのドメインポリシーを選択する代わりに、OU (またはその下の任意の OU) *yourdomainname* を選択し、コンテキスト (右クリック) メニューを開き、このドメインGPOで を作成するを選択し、ここでリンクします。
   > OU の詳細については、*yourdomainname*「 AWS Directory Service 管理ガイド」の「作成内容https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_what_gets_created.html」を参照してください。

7. グループポリシー管理エディタで、コンピュータ設定、ポリシー、管理テンプレート、およびPCoIPセッション変数を選択します。
8. 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、 を使用する WorkSpaces ときに に固有のグループポリシー設定を変更できるようになりましたPCoIP。

> **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。

のグループポリシー設定を管理する PCoIP

グループポリシー設定を使用して、 WorkSpaces を使用する Windows を管理しますPCoIP。

のプリンターサポートを設定する PCoIP

デフォルトでは、 は基本的なリモート印刷 WorkSpaces を有効にします。これは、ホスト側で汎用プリンタードライバーを使用して互換性のある印刷を行うため、印刷機能が制限されています。

Windows クライアントの高度なリモート印刷では、両面印刷など、プリンター固有の機能を使用できますが、ホスト側に一致するプリンタードライバーをインストールする必要があります。

リモート印刷は仮想チャネルとして実装されます。仮想チャネルが無効になっている場合、リモート印刷は機能しません。

Windows では WorkSpaces、グループポリシー設定を使用して、必要に応じてプリンターのサポートを設定できます。

プリンターのサポートを設定するには

1. （WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. [Configure remote printing] 設定を開きます。
4. [Configure remote printing (リモート印刷を設定)] ダイアログボックスで、次のいずれかを実行します。
   - 高度なリモート印刷を有効にするには、[Enabled (有効)] を選択し、[Options (オプション)] の [Configure remote printing (リモート印刷を設定)] で [Basic and Advanced printing for

Windows clients (Windows クライアントの基本印刷と高度な印刷)] を選択します。クライアントコンピュータの現在のデフォルトプリンターを自動的に使用するには、[Automatically set default printer (デフォルトプリンターを自動的に設定する)] を選択します。

- 印刷を無効にするには、[Enabled (有効)] を選択し、[Options (オプション)] の [Configure remote printing (リモート印刷を設定)] で [printing disabled (印刷無効)] を選択します。

5. [OK] を選択します。
6. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

デフォルトでは、ローカルプリンターへの自動リダイレクトは無効になっています。グループポリシー設定を使用してこの機能を有効にし、 に接続するたびにローカルプリンターをデフォルトプリンターとして設定できます WorkSpace。

> **Note**
>
> ローカルプリンターリダイレクトは Amazon Linux では使用できません WorkSpaces。

ローカルプリンターへの自動リダイレクトを有効にするには

1. (WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. [Configure remote printing] 設定を開きます。
4. [Enabled] (有効) を選択し、[Options] (オプション) の [Configure remote printing] (リモート印刷を設定) で、次のいずれかを選択します。

- Basic and Advanced printing for Windows clients (Windows クライアント用の基本印刷と高度な印刷)
- Basic printing (基本印刷)

5. [Automatically set default printer] (デフォルトのプリンターを自動的に設定) を選択し、[OK] を選択します。
6. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のクリップボードリダイレクト (コピー/貼り付け) を有効または無効にする PCoIP

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

クリップボードのリダイレクトを有効または無効にするには

1. (WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. [Configure clipboard redirection] 設定を開きます。
4. [Configure clipboard redirection (クリップボードのリダイレクトの設定)] ダイアログボックスで、[有効] を選択し、次のいずれかの設定を選択して、クリップボードのリダイレクトが許可される方向を決定します。終了したら、[OK] を選択します。

   - 双方向で無効
   - エージェントからクライアントのみ (ローカルコンピュータWorkSpace へ) を有効にしました
   - クライアントからエージェントのみ有効 (ローカルコンピュータから WorkSpaceへ)
   - 双方向で有効

5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

既知の制限事項

でクリップボードのリダイレクトを有効にすると WorkSpace、Microsoft Office アプリケーションから 890 KB を超えるコンテンツをコピーすると、アプリケーションが最大 5 秒間遅くなったり、応答しなくなる可能性があります。

のセッション再開タイムアウトを設定する PCoIP

ネットワーク接続が失われると、アクティブな WorkSpaces クライアントセッションは切断されます。Windows および macOS 用の WorkSpaces クライアントアプリケーションは、ネットワーク接続が一定時間内に復元された場合、セッションを自動的に再接続しようとします。デフォルトのセッション再開タイムアウトは 20 分ですが、ドメインのグループポリシー設定によって制御 WorkSpaces される の値を変更できます。

自動セッション再起動タイムアウト値を設定するには

1. (WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. [Configure Session Automatic Reconnection Policy] 設定を開きます。
4. [Configure Session Automatic Reconnection Policy] ダイアログボックスで [Enabled] を選択し、[Configure Session Automatic Reconnection Policy] オプションを必要なタイムアウト値 (分単位) に設定して、[OK] を選択します。
5. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

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 PCoIP

デフォルトでは、Amazon はローカルマイクからのデータのリダイレクト WorkSpaces をサポートしています。Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

> **Note**
>
> でユーザーのローカルログオンを制限するグループポリシー設定がある場合 WorkSpaces、オーディオ入力は で機能しません WorkSpaces。そのグループポリシー設定を削除すると、の次回の再起動後にオーディオ入力機能が有効になります WorkSpace。このグループポリシー設定の詳細については、Microsoft のドキュメントの「ローカルでのログオンを許可する」をご参照ください。

オーディオ入力リダイレクトを有効または無効にするには

1. (WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. PCoIP セッション設定で音声の有効化/無効化を開きます。
4. PCoIP セッションダイアログボックスの音声の有効化/無効化 で、有効化または無効化 を選択します。
5. [OK] を選択します。
6. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

のタイムゾーンリダイレクトを無効にする PCoIP

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のようにさまざまな理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Windows で必要な場合は WorkSpaces、グループポリシー設定を使用してこの機能を無効にすることができます。

タイムゾーンのリダイレクトを無効にするには

1. (WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. [Configure timezone redirection] (タイムゾーンリダイレクトを構成) の設定を開きます。
4. [Configure timezone redirection] (タイムゾーンリダイレクトを設定) ダイアログボックスで [Disabled] (無効) を選択します。
5. [OK] を選択します。

6. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

   - を再起動します WorkSpace (Amazon WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します)。
   - 管理コマンドプロンプトで、**`gpupdate /force`** と入力します。
7. のタイムゾーンを目的のタイムゾーン WorkSpaces に設定します。

のタイムゾーン WorkSpaces が静的になり、クライアントマシンのタイムゾーンをミラーリングしなくなりました。

PCoIP セキュリティ設定を構成する

の場合PCoIP、転送中のデータは 1.2 TLS 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、ストリーミングピクセルに暗号化されたUDPトラフィックをAES暗号化とともに使用します。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、暗号化のデフォルトは 128 ビットです。PCoIP セキュリティ設定グループポリシーの設定を使用して、このデフォルトを 256 ビットに変更できます。

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、PCoIP「セキュリティ設定グループポリシーの設定」ダイアログボックスを参照してください。

PCoIP セキュリティ設定を構成するには

1. （WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. PCoIP セキュリティ設定の構成 設定を開きます。
4. PCoIP 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。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、PCoIPData Encryption Ciphers オプションに移動し、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設定を調整し、ブロックする暗号スイートを一覧表示します。これらの設定の詳細については、PCoIP「セキュリティ設定の構成」ダイアログボックスの説明を参照してください。
6. [OK] を選択します。
7. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

U2F のUSB YubiKeyリダイレクトを有効にする

> **Note**
>
> Amazon WorkSpaces は現在、 YubiKey U2F のUSBリダイレクトのみをサポートしています。他のタイプのUSBデバイスはリダイレクトされる場合がありますが、サポートされておらず、正常に動作しない可能性があります。

YubiKey U2F のUSBリダイレクトを有効にするには

1. （WorkSpaces 32 ビット) 用の最新のグループポリシー管理テンプレートまたは PCoIP (WorkSpaces PCoIP64 ビット) 用のグループポリシー管理テンプレートがインストールされていることを確認します。
2. ディレクトリ管理 WorkSpace または WorkSpaces ディレクトリに参加している Amazon EC2 インスタンスで、グループポリシー管理ツール (gpmc.msc) を開き、PCoIPセッション変数に移動します。
3. PCOIP セッション設定USBで Enable/disable 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 設定を開きます。
6. 有効を選択し、USB認可テーブル (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 () の組み合わせです PID。VID/PID の組み合わせの形式は 1xxxxyyyy です。ここで、xxxx は 16 進形式の VID 、yyyy は 16 進形式の PIDです。この例では、1050 が VID、0407 が ですPID。その他の YubiKey USB値については、YubiKey USB「ID 値」を参照してください。

7. USB 認可テーブルの入力 (最大 10 個のルール) で、USBデバイス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。つまり、認可リスト内のUSBデバイスのみが許可されます。

   > **Note**
   >
   > 最大 10 個のUSB承認ルールと最大 10 個の承認USB解除ルールを定義できます。複数のルールを区切るには、縦棒 (|) 文字を使用します。認可/非認可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] を選択します。
9. グループポリシー設定の変更は、 の次のグループポリシーの更新後 WorkSpace 、および WorkSpace セッションが再開された後に有効になります。グループポリシーの変更を適用するには、次のいずれかを実行します。

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

設定を有効にすると、USBデバイスルール設定で制限が設定され WorkSpaces ていない限り、サポートされているすべてのUSBデバイスが にリダイレクトできます。

Kerberos チケットの最大ライフタイムを設定する

Windows の「Remember Me」機能を無効にしていない場合 WorkSpaces、 WorkSpace ユーザーは WorkSpaces クライアントアプリケーションの「Remember Me」または「Leep me ログイン」チェックボックスを使用して認証情報を保存できます。この機能により、ユーザーはクライアントアプリケーションの実行中に簡単に に接続できます WorkSpaces。認証情報は、ユーザーの Kerberos チケットの最大有効期間が終了するまで安全にキャッシュに保存されます。

で AD Connector ディレクトリ WorkSpace を使用している場合は、Microsoft Windows ドキュメントの WorkSpaces 「ユーザーチケットの最大有効期間」の手順に従って、グループポリシーを通じてユーザーの Kerberos チケットの最大有効期間を変更できます。

[Remember Me] (このアカウントを記憶する) 機能を有効または無効にする方法については、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 HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定され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を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Windows のデバイスプロキシサーバー設定を構成できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

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

の場合PCoIP WorkSpaces、デスクトップクライアントアプリケーションはプロキシサーバーの使用も、 のポート TLS 4172 トラフィック UDP (デスクトップトラフィックの場合) の復号化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。

ではDCV WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート TLS 4195 TCP トラフィックのHTTPプロキシサーバーの使用をサポートしています。 の復号化と検査はサポートされていません。

DCV は、 経由のデスクトップトラフィックのプロキシの使用をサポートしていませんUDP。TCP トラフィックのプロキシの使用をサポートするのは、Windows および macOS デスクトップクライアントアプリケーションとウェブアクセスのみです WorkSpaces。

> **Note**
>
> プロキシサーバーを使用することを選択した場合、クライアントアプリケーションが WorkSpaces サービスに対して行うAPI呼び出しもプロキシされます。API 呼び出しとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイテンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket (TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響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を追加しないように、プロキシサーバーを WorkSpace可能な限りクライアントの近く、できれば同じネットワーク内に配置してください。

Amazon WorkSpaces for Zoom 会議メディアプラグインのサポートを有効にする

Zoom は WorkSpaces、 DCVおよび PCoIP Windows ベースの と Zoom VDI プラグインと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り、ビデオ通話はクラウドベースの仮想デスクトップをバイパスし、ユーザーの 内で会議が実行されているときにローカルに似た Zoom エクスペリエンスを提供できます WorkSpace。

の Zoom 会議メディアプラグインを有効にする DCV

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
- 内 WorkSpaces — Zoom VDI 会議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、「の拡張機能を設定する DCV」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、「のセッション再開タイムアウトを設定する DCV」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 にインストールします WorkSpaces。詳細については、「Using Zoom for Amazon WorkSpaces」を参照してください。

1. 内に Zoom VDI 会議クライアントバージョン 5.12.6 以降をインストールします WorkSpace。
2. がインストールされているクライアントに Zoom VDI プラグイン (Windows ユニバーサルインストーラ) バージョン WorkSpace 5.12.6 以降をインストールする
3. プラグインのステータスが Zoom VDIクライアント内で接続済みと表示されることを確認して、VDIプラグインが Zoom トラフィックを最適化していることを確認します。詳細については、「Amazon WorkSpaces 最適化の確認方法」を参照してください。

の Zoom 会議メディアプラグインを有効にする PCoIP

Active Directory への管理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 () を使用してレジストリキーを生成できますGPO。これにより、ユーザーは強制更新を使用してドメイン

WorkSpaces 内のすべての Windows にレジストリキーを送信できます。または、管理者権限を持つユーザーは、 WorkSpaces ホストにレジストリキーを個別にインストールすることもできます。

前提条件

プラグインを使用する前に、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。
- 内 WorkSpaces — Zoom VDI 会議クライアントバージョン 5.12.6 以降。

Windows WorkSpaces ホストでレジストリキーを作成する

Windows WorkSpaces ホストでレジストリキーを作成するには、次の手順を実行します。Windows で Zoom を使用するには、レジストリキーが必要です WorkSpaces。

1. 管理者として Windows レジストリエディタを開きます。
2. \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon に移動します。
3. Extension キーが存在しない場合は、右クリックして [New] (新規) > [Key] (キー) を選択し、「Extension」という名前を付けます。
4. 新しい拡張機能キーで、右クリックして新規 > を選択しDWORD、有効にする名前を付けます。この名前は小文字にする必要があります。
5. 新しい を選択しDWORD、値を 1 に変更します。
6. コンピュータを再起動してプロセスを完了します。
7. WorkSpaces ホストで、最新の Zoom VDIクライアントをダウンロードしてインストールします。 WorkSpaces クライアント (5.4 以降) で、Amazon 用の最新の Zoom VDIクライアントプラグインをダウンロードしてインストールします WorkSpaces。詳細については、Zoom サポートウェブサイトのVDI「リリースとダウンロード」を参照してください。

Zoom を起動してビデオ通話を開始します。

トラブルシューティング

Windows で Zoom をトラブルシューティングするには、次のアクションを実行します WorkSpaces。

- レジストリキー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、 Support センター Support を使用して にお問い合わせください。

次の例を使用して、 ディレクトリの管理者GPOとして 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>
```

Personal WorkSpaces で Amazon Linux WorkSpaces を管理する

Windows と同様に WorkSpaces、Amazon Linux WorkSpaces はドメインに参加しているため、Active Directory ユーザーとグループを使用して次のことができます。

- Amazon Linux の管理 WorkSpaces
- WorkSpaces ユーザーにアクセス権を付与する

Linux インスタンスはグループポリシーに従っていないため、設定管理ソリューションを使用してポリシーの配信と適用を行うことをお勧めします。例えば、AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise、または Ansible を使用できます。

> **Note**
>
> ローカルプリンターリダイレクトは Amazon Linux では使用できません WorkSpaces。

Amazon Linux でのコントロールDCVの動作 WorkSpaces

の動作DCVは、 `/etc/wsp/` ディレクトリにある `wsp.conf` ファイルの設定によって制御されます。ポリシーの変更をデプロイして適用するには、Amazon Linux をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。

> **Note**
>
> - `wsp.conf` ファイルに対して正しくない、またはサポートされていない変更を加えた場合、ポリシーの変更が で新しく確立された接続に適用されない場合があります WorkSpace。
> - WorkSpaces DCV バンドルの Amazon Linux には、現在次の制限があります。
>   - 現在、 AWS GovCloud （ 米国西部) および AWS GovCloud （ 米国東部) でのみ利用できます。
>   - 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 のクリップボードリダイレクトを設定する WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、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、 を切断して再接続するときに有効になります WorkSpace。

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

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.
```
clipboard = X
```

の可能な値*X*は次のとおりです。

`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 のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、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、 を切断して再接続するときに有効になります WorkSpace。

DCV Amazon Linux のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. ファイルの末尾に次の行を追加します。

```
audio-in = X
```

の可能な値*X*は次のとおりです。

`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 のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

必要に応じて、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、 を切断して再接続した後に有効になります WorkSpace。

DCV Amazon Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. ファイルの末尾に次の行を追加します。

```
timezone_redirect= X
```

の可能な値*X*は次のとおりです。

[enabled] (有効) — タイムゾーンのリダイレクトは有効です (デフォルト)

disabled (無効) — タイムゾーンのリダイレクトは無効です

Amazon Linux でのPCoIPエージェントの動作を制御する WorkSpaces

PCoIP エージェントの動作は、 /etc/pcoip-agent/ ディレクトリにある pcoip-agent.conf ファイルの設定によって制御されます。ポリシーの変更をデプロイして適用するには、Amazon Linux をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。エージェントを再起動すると、開いている接続がすべて終了されウィンドウマネージャーが再起動されます。変更を適用するには、 を再起動することをお勧めします WorkSpace。

> **Note**
>
> pcoip-agent.conf ファイルに対して正しくない、またはサポートされていない変更を行うと、 が機能し WorkSpace なくなる可能性があります。が動作し WorkSpace なくなった場合は、 WorkSpace を使用して に接続SSHして変更をロールバックするか、 を再構築 WorkSpaceする必要があります。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。使用可能な設定の完全なリストについては、任意の Amazon Linux のターミナルman pcoip-agent.confからを実行します WorkSpace。

PCoIP Amazon Linux のクリップボードリダイレクトを設定する WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。PCoIP エージェント conf を使用して、必要に応じてこの機能を無効にします。この設定は、 を再起動したときに有効になります WorkSpace。

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

1. 次のコマンドを使用して、昇格された権限を持つエディタで pcoip-agent.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. ファイルの末尾に次の行を追加します。

```
pcoip.server_clipboard_state = X
```

の可能な値*X*は次のとおりです。

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 ドキュメントのPCoIP「仮想チャネル」を参照してください。

PCoIP Amazon Linux のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。PCoIP エージェント conf を使用して、必要に応じてこの機能を無効にします。この設定は、 を再起動したときに有効になります WorkSpace。

PCoIP Amazon Linux のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `pcoip-agent.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. ファイルの末尾に次の行を追加します。

   ```
   pcoip.enable_audio = X
   ```

の可能な値*X*は次のとおりです。

0 – オーディオ入力リダイレクトは無効です

1 – オーディオ入力リダイレクトは有効です

PCoIP Amazon Linux のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- 多くの旅行をするユーザーは、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に保持したいと考えています。

Linux で必要な場合は WorkSpaces、 PCoIP エージェント conf を使用してこの機能を無効にすることができます。この設定は、 を再起動したときに有効になります WorkSpace。

PCoIP Amazon Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `pcoip-agent.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. ファイルの末尾に次の行を追加します。

```
pcoip.enable_timezone_redirect= X
```

の可能な値*X*は次のとおりです。

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SSHへのアクセスを許可する

デフォルトでは、 WorkSpaces を使用して Amazon Linux に接続できるのは、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ですSSH。

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、「」を参照してくださいPersonal WorkSpaces で Linux WorkSpaces SSHの接続を有効にする。

Amazon Linux のデフォルトシェルを上書きする WorkSpaces

Linux のデフォルトシェルを上書きするには WorkSpaces、ユーザーの ~/.bashrc ファイルを編集することをお勧めします。たとえば、Z shell シェルの代わりに Bash を使用するには、/home/*username*/.bashrc に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動 WorkSpace するか、 からログアウトして WorkSpace （ 切断するだけでなく ）、再度ログインする必要があります。

不正なアクセスからカスタムリポジトリを保護する

カスタムリポジトリへのアクセスを制御するには、パスワードを使用するのではなく、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。例えば、ネットワークアクセスコントロールリスト (ACLs) 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 の使用の詳細については、Linux インスタンス用 Amazon ユーザーガイドの Extras Library (Amazon Linux) を参照してください。 EC2

> **Note**
>
> Amazon Linux リポジトリを使用している場合は、Amazon Linux にインターネットアクセス WorkSpaces があるか、このリポジトリとメイン 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 での認証にスマートカードを使用する WorkSpaces

WorkSpaces DCV バンドルの Linux では、認証に共通アクセスカード (CAC) と個人 ID 検証 (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 HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定され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を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Linux のデバイスプロキシサーバー設定を構成できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

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

の場合PCoIP WorkSpaces、デスクトップクライアントアプリケーションはプロキシサーバーの使用も、 のポート TLS 4172 トラフィック UDP (デスクトップトラフィックの場合) の復号化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。

ではDCV WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート TLS 4195 TCP

トラフィックのHTTPプロキシサーバーの使用をサポートしています。 の復号化と検査はサポートされていません。

DCV は、 経由のデスクトップトラフィックのプロキシの使用をサポートしていませんUDP。TCP トラフィックのプロキシの使用をサポートするのは、 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ウェブアクセスのみです。

> **Note**
>
> プロキシサーバーを使用することを選択した場合、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呼び出しもプロキシされます。API 呼び出しとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイテンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket （ TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響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を追加しないように、プロキシサーバーを可能な限り WorkSpace クライアントの近く、できれば同じネットワーク内に配置してください。

WorkSpaces Personal WorkSpaces で Ubuntu を管理する

Windows や Amazon Linux と同様に WorkSpaces、Ubuntu WorkSpaces はドメインに参加しているため、Active Directory ユーザーとグループを使用して次の操作を実行できます。

- Ubuntu の管理 WorkSpaces
- WorkSpaces ユーザーにアクセス権を付与する

を使用して、グループポリシー WorkSpaces で Ubuntu を管理できますADsys。詳細については、Ubuntu Active Directory の統合FAQを参照してください。Landscape や Ansible など、他の構成および管理ソリューションを使用することもできます。

Ubuntu でのコントロールDCV動作 WorkSpaces

の動作DCVは、 /etc/wsp/ ディレクトリにある wsp.conf ファイルの設定によって制御されます。ポリシーの変更をデプロイして適用するには、Ubuntu をサポートする設定管理ソリューションを使用します。変更はすべて、エージェントの起動時に有効になります。

> **Note**
>
> wsp.conf ポリシーに正しくない、またはサポートされていない変更を加えた場合、 への新しく確立された接続に適用されない可能性があります WorkSpace。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。

Ubuntu のクリップボードリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、DCV設定ファイルを使用してこの機能を無効にします。

Ubuntu のクリップボードリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. [policies] グループの末尾に次の行を追加します。

   ```
   clipboard = X
   ```

   の可能な値*X*は次のとおりです。

   [enabled] (有効) — クリップボードリダイレクトは両方向ともに有効です (デフォルト)

   [disabled] (無効) — クリップボードのリダイレクトは両方向ともに無効です

[paste-only] (ペーストのみ) — クリップボードのリダイレクトが有効で、ローカルクライアントデバイスからコンテンツをコピーし、リモートホストデスクトップにペーストするのみが可能です。

[copy-only] (コピーのみ) — クリップボードのリダイレクトが有効で、リモートホストのデスクトップからコンテンツをコピーし、ローカルのクライアントデバイスにペーストするのみが可能です。

Ubuntu のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、DCV設定ファイルを使用してこの機能を無効にします。

Ubuntu のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
audio-in = X
```

の可能な値*X*は次のとおりです。

[enabled] (有効) — オーディオインリダイレクトは有効です (デフォルト)

[disabled] (無効)— オーディオインリダイレクトは無効です

Ubuntu のビデオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はビデオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、DCV設定ファイルを使用してこの機能を無効にします。

Ubuntu のビデオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
video-in = X
```

の可能な値*X*は次のとおりです。

[enabled] (有効) — ビデオインリダイレクトは有効です (デフォルト)

[disabled] (無効)— ビデオインリダイレクトは無効です

Ubuntu のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- ユーザーは多くの旅行をしていて、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に維持したいと考えています。

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。

Ubuntu のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
timezone-redirection = X
```

の可能な値*X*は次のとおりです。

[enabled] (有効) — タイムゾーンのリダイレクトは有効です (デフォルト)

disabled (無効) — タイムゾーンのリダイレクトは無効です

Ubuntu のプリンターリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はプリンターリダイレクト WorkSpaces をサポートします。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 のプリンターリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
remote-printing = X
```

の可能な値*X*は次のとおりです。

[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

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 DCV

画面ロックでセッションの切断を有効にして、ロック画面が検出されたときにユーザーが WorkSpaces セッションを終了できるようにします。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、自分の に対して有効になっている認証のタイプに応じて、自分自身を認証できます WorkSpaces。

デフォルトでは、 WorkSpaces は画面ロック時のセッションの切断をサポートしていません。必要に応じて、DCV設定ファイルを使用してこの機能を有効にします。

Ubuntu の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
disconnect-on-lock = X
```

の可能な値*X*は次のとおりです。

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SSHへのアクセスを許可する

デフォルトでは、 WorkSpaces を使用して Ubuntu に接続できるのは、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ですSSH。 WorkSpaces を使用して他のユーザーやアカウントが Ubuntu に接続できるようにするにはSSH、Active Directory で Ubuntu 管理者専用の WorkSpaces 管理者グループを作成することをお勧めします。

Linux_WorkSpaces_Admins Active Directory グループのメンバーの sudo アクセスを有効にするには

1. 次の例に示すように、sudoers を使用して visudo ファイルを編集します。

```
[username@workspace-id ~]$ sudo visudo
```

2. 次の行を追加します。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

専用の管理者グループを作成したら、次のステップに従ってグループのメンバーの口グインを有効にします。

`Linux_WorkSpaces_Admins` Active Directory グループのメンバーの口グインを有効にするには

1. 昇格された権限で `etc/security/access.conf` を編集します。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 次の行を追加します。

```
+:(Linux_WorkSpaces_Admins):ALL
```

Ubuntu WorkSpaces では、SSH接続用のユーザー名を指定するときにドメイン名を追加する必要はなく、デフォルトではパスワード認証が無効になっています。経由で接続するにはSSH、Ubuntu `$HOME/.ssh/authorized_keys`の にSSHパブリックキーを追加するか WorkSpace、 を編集/`etc/ssh/sshd_config`して PasswordAuthentication を に設定する必要がありますyes。SSH 接続の有効化の詳細については、「Linux SSHの接続を有効にする WorkSpaces」を参照してください。

Ubuntu のデフォルトシェルを上書きする WorkSpaces

Ubuntu のデフォルトシェルを上書きするには WorkSpaces、ユーザーの `~/.bashrc` ファイルを編集することをお勧めします。たとえば、`Z shell` シェルの代わりに `Bash` を使用するには、`/home/username/.bashrc` に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動 WorkSpace するか WorkSpace 、(切断だけでなく) からログアウトしてから再度ログインする必要があります。

インターネットアクセス用のデバイスプロキシサーバー設定を構成する

デフォルトでは、 WorkSpaces クライアントアプリケーションは HTTPS (ポート 443) トラフィックのデバイスオペレーティングシステム設定で指定され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を構成する」の手順に従って、グループポリシー WorkSpaces を通じて Ubuntu のデバイスプロキシサーバー設定を構成できます。 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/configure-proxy-internet

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

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

の場合DCV WorkSpaces、 WorkSpaces Windows クライアントアプリケーション (バージョン 5.1 以降) および macOS クライアントアプリケーション (バージョン 5.4 以降) は、ポート TLS 4195

TCPトラフィックのHTTPプロキシサーバーの使用をサポートしています。 の復号化と検査はサポートされていません。

DCV は、 経由のデスクトップトラフィックのプロキシの使用をサポートしていませんUDP。TCP トラフィックのプロキシの使用をサポートするのは、 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ウェブアクセスのみです。

> **Note**
>
> プロキシサーバーを使用することを選択した場合、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呼び出しもプロキシされます。API 呼び出しとデスクトップトラフィックの両方が同じプロキシサーバーを通過する必要があります。

プロキシサーバーの使用に関する推奨事項

WorkSpaces デスクトップトラフィックでプロキシサーバーを使用することはお勧めしません。

Amazon WorkSpaces デスクトップトラフィックは既に暗号化されているため、プロキシはセキュリティを向上させません。プロキシを使用すると、ネットワークパスに余分なホップが発生してレイテンシーをもたらし、ストリーミング品質に影響する可能性があります。プロキシのサイズがデスクトップストリーミングトラフィックの処理に適切でない場合、プロキシによってスループットが低下する可能性もあります。さらに、ほとんどのプロキシは長時間実行される WebSocket （ TCP) 接続をサポートするように設計されておらず、ストリーミングの品質と安定性に影響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を追加しないように、プロキシサーバーを可能な限り WorkSpace クライアントの近く、できれば同じネットワーク内に配置してください。

Rocky Linux を管理する WorkSpaces

Rocky Linux は、Ansible などの設定および管理ソリューション WorkSpaces で管理できます。

> **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 でのコントロールDCV動作 WorkSpaces

の動作DCVは、 `/etc/wsp/` ディレクトリにある `wsp.conf` ファイルの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**
>
> `wsp.conf` ポリシーに正しくない、またはサポートされていない変更を加えた場合、 への新しく確立された接続に適用されない可能性があります WorkSpace。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。

Rocky Linux のクリップボードリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、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 のクリップボードリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. `[policies]` グループの末尾に次の行を追加します。

   ```
   clipboard = X
   ```

   の可能な値*X*は次のとおりです。

   [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 のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、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 のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
audio-in = X
```

の可能な値*X*は次のとおりです。

[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 のビデオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はビデオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、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 のビデオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
video-in = X
```

の可能な値*X*は次のとおりです。

[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 のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- ユーザーは多くの旅行をしていて、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に維持したいと考えています。

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。

Rocky Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
timezone-redirection = X
```

の可能な値*X*は次のとおりです。

[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 のプリンターリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はプリンターリダイレクト WorkSpaces をサポートします。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 のプリンターリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つ工ディタで 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
```

の可能な値*X*は次のとおりです。

[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

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 DCV

画面ロックでセッションの切断を有効にして、ロック画面が検出されたときにユーザーが WorkSpaces セッションを終了できるようにします。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、自分の に対して有効になっている認証のタイプに応じて、自分自身を認証できます WorkSpaces。

デフォルトでは、 WorkSpaces は画面ロック時のセッションの切断をサポートしていません。必要に応じて、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 の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つ工ディタで 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
```

の可能な値*X*は次のとおりです。

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SSHへのアクセスを許可する

デフォルトでは、 WorkSpaces を使用して Rocky Linux に接続できるのは、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ですSSH。を使用して他のユーザーとアカウントが Rocky Linux WorkSpaces に接続できるようにするにはSSH、Active Directory で Rocky Linux 管理者専用の WorkSpaces 管理者グループを作成することをお勧めします。

Linux_WorkSpaces_Admins Active Directory グループのメンバーの sudo アクセスを有効にするには

1. 次の例に示すように、sudoers を使用して visudo ファイルを編集します。

```
[username@workspace-id ~]$ sudo visudo
```

2. 次の行を追加します。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

専用の管理者グループを作成したら、次のステップに従ってグループのメンバーの口グインを有効にします。

Linux_WorkSpaces_Admins Active Directory グループのメンバーの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
```

Rocky Linux WorkSpaces では、SSH接続用のユーザー名を指定するときにドメイン名を追加する必要はなく、デフォルトではパスワード認証が無効になっています。経由で接続するにはSSH、Rocky Linux $HOME/.ssh/authorized_keysの にSSHパブリックキーを追加するか WorkSpace、 を編集/etc/ssh/sshd_configして PasswordAuthentication を に設定する必要がありますyes。SSH接続の有効化の詳細については、「Linux SSHの接続を有効にする WorkSpaces」を参照してください。

Rocky Linux のデフォルトシェルを上書きする WorkSpaces

Rocky Linux のデフォルトシェルを上書きするには WorkSpaces、ユーザーの ~/.bashrc ファイルを編集することをお勧めします。たとえば、Z shell シェルの代わりに Bash を使用するには、/home/username/.bashrc に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動 WorkSpace するか WorkSpace 、(切断だけでなく) からログアウトしてから再度ログインする必要があります。

Red Hat Enterprise Linux を管理する WorkSpaces

Windows および Amazon Linux と同様に WorkSpaces、Red Hat Enterprise Linux WorkSpaces はドメインに参加しているため、Active Directory ユーザーとグループを使用して次のことができます。

- Red Hat Enterprise Linux の管理 WorkSpaces
- WorkSpaces ユーザーにアクセス権を付与する

を使用して、グループポリシー WorkSpaces で Red Hat Enterprise Linux を管理できます ADsys。詳細については、Red Hat Enterprise Linux Active Directory の統合FAQ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 でDCVの動作を制御する WorkSpaces

の動作DCVは、 `/etc/wsp/` ディレクトリにある `wsp.conf` ファイルの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**
>
> `wsp.conf` ポリシーに正しくない、またはサポートされていない変更を加えた場合、 への新しく確立された接続に適用されない可能性があります WorkSpace。

以降のセクションでは、特定の機能を有効または無効にする方法について説明します。

Red Hat Enterprise Linux のクリップボードリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はクリップボードのリダイレクト WorkSpaces をサポートします。必要に応じて、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 のクリップボードリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. `[policies]` グループの末尾に次の行を追加します。

```
clipboard = X
```

の可能な値*X*は次のとおりです。

[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 のオーディオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はオーディオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、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 のオーディオ入力リダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. `[policies]` グループの末尾に次の行を追加します。

```
audio-in = X
```

の可能な値*X*は次のとおりです。

[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 のビデオ入力リダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はビデオ入力リダイレクト WorkSpaces をサポートします。必要に応じて、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 のビデオインリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. `[policies]` グループの末尾に次の行を追加します。

   ```
   video-in = X
   ```

   の可能な値*X*は次のとおりです。

   [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 のタイムゾーンリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、Workspace 内の時間は、 への接続に使用されているクライアントのタイムゾーンを反映するように設定されています WorkSpace。この動作は、タイムゾーンのリダイレクトによって制御されます。次のような理由から、タイムゾーンのリダイレクトをオフにすることもできます。

- 会社は、すべての従業員が特定のタイムゾーンで業務を行うことを希望している (一部の従業員が他のタイムゾーンにいる場合でも)。
- 特定のタイムゾーンで特定の時間に実行することを意図したタスク WorkSpace が にスケジュールされている。
- ユーザーは多くの旅行をしていて、一貫性と個人設定のために を 1 つのタイムゾーン WorkSpaces に維持したいと考えています。

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。

Red Hat Enterprise Linux のタイムゾーンリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
timezone-redirection = X
```

の可能な値*X*は次のとおりです。

[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 のプリンターリダイレクトを有効または無効にする WorkSpaces

デフォルトでは、 はプリンターリダイレクト WorkSpaces をサポートします。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 のプリンターリダイレクトを有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで wsp.conf ファイルを開きます。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. [policies] グループの末尾に次の行を追加します。

```
remote-printing = X
```

の可能な値*X*は次のとおりです。

[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

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 DCV

画面ロックでセッションの切断を有効にして、ロック画面が検出されたときにユーザーが WorkSpaces セッションを終了できるようにします。 WorkSpaces クライアントから再接続するために、ユーザーは自分のパスワードまたはスマートカードを使用して、自分の に対して有効になっている認証のタイプに応じて、自分自身を認証できます WorkSpaces。

デフォルトでは、 WorkSpaces は画面ロック時のセッションの切断をサポートしていません。必要に応じて、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 の画面ロックでセッションの切断を有効または無効にするには WorkSpaces

1. 次のコマンドを使用して、昇格された権限を持つエディタで `wsp.conf` ファイルを開きます。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. `[policies]` グループの末尾に次の行を追加します。

   ```
   disconnect-on-lock = X
   ```

   の可能な値*X*は次のとおりです。

   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SSHへのアクセスを許可する

デフォルトでは、 WorkSpaces を使用して Red Hat Enterprise Linux に接続できるのは、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ですSSH。 WorkSpaces を使用して他のユーザーとアカウントが Red Hat Enterprise Linux に接続できるようにするにはSSH、Active Directory で Red Hat Enterprise Linux 管理者専用の WorkSpaces 管理者グループを作成することをお勧めします。

Linux_WorkSpaces_Admins Active Directory グループのメンバーの sudo アクセスを有効にするには

1. 次の例に示すように、sudoers を使用して visudo ファイルを編集します。

```
[username@workspace-id ~]$ sudo visudo
```

2. 次の行を追加します。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

専用の管理者グループを作成したら、次のステップに従ってグループのメンバーの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接続用のユーザー名を指定するときにドメイン名を追加する必要はなく、デフォルトではパスワード認証が無効になっています。経由で接続するにはSSH、Red Hat Enterprise Linux $HOME/.ssh/authorized_keysの にSSHパブリックキーを追加するか WorkSpace、 を編集/etc/ssh/sshd_configして PasswordAuthentication を に設定する必要がありますyes。SSH 接続の有効化の詳細については、「Linux SSHの接続を有効にする WorkSpaces」を参照してください。

Red Hat Enterprise Linux のデフォルトシェルを上書きする WorkSpaces

Red Hat Enterprise Linux のデフォルトシェルを上書きするには WorkSpaces、ユーザーの `~/.bashrc` ファイルを編集することをお勧めします。たとえば、`Z shell` シェルの代わりに `Bash` を使用するには、`/home/username/.bashrc` に次の行を追加します。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> この変更を行った後、変更を有効にするには、 を再起動 WorkSpace するか WorkSpace 、(切断だけでなく) からログアウトしてから再度ログインする必要があります。

WorkSpaces Personal でのリアルタイム通信 WorkSpaces を最適化する

Amazon WorkSpaces では、Microsoft Teams、Zoom、Webex などの Unified Communication (UC) アプリケーションのデプロイを容易にするさまざまな手法を提供しています。現代のアプリケーション環境では、ほとんどの UC アプリケーションに、1:1 チャットルーム、共同グループチャットチャネル、シームレスなファイルストレージと交換、ライブイベント、ウェビナー、ブロードキャスト、インタラクティブな画面共有と制御、ホワイトボード、オフラインのオーディオ/ビデオメッセージング機能などのさまざまな機能が備わっています。この機能のほとんどは、追加の微調整や機能強化を必要とせずに、標準機能 WorkSpaces として で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 one-on-one および 集合グループ会議は、このルールの例外を表すことに注意してください。このような機能を正常に組み込むには、多くの場合、 WorkSpaces デプロイプロセス中に専用のフォーカスと計画が必要です。

Amazon 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 WorkSpaces、3 つの異なるリアルタイム通信 (RTC) 設定モードから選択できます。選択するモードは、ユーザーに提供される 1 つまたは複数の特定のアプリケーションと、使用する予定のクライアントデバイスによって異なります。

このドキュメントでは、Amazon の最も一般的な UC アプリケーションのユーザーエクスペリエンスの最適化に焦点を当てています WorkSpaces。 WorkSpaces Core 固有の最適化については、パートナー固有のドキュメントを参照してください。

トピック

- メディア最適化モードの概要
- 使用するRTC最適化モード
- 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、サードパーティーの UC および VoIP アプリケーションはリモート で実行され WorkSpace、メディアフレームワークは直接通信のためにサポートされているクライアントにオフロードされます。次の UC アプリケーションは、Amazon でこのアプローチを使用します WorkSpaces。

- Zoom Meetings
- Cisco Webex Meetings

メディア最適化RTCモードを機能させるには、UC アプリケーションベンダーは、DCV拡張機能SDKなど、利用可能なソフトウェア開発キット (SDK) のいずれか WorkSpaces を使用して 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、「メディア最適化の設定 RTC」を参照してください。

オプション 2: セッション内最適化リアルタイム通信 (セッション内最適化RTC)

このモードでは、変更されていない UC アプリケーションが で実行され WorkSpace、 を介してクライアントデバイスにオーディオおよびビデオトラフィックDCVをチャネルします。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、UC アプリケーションによって消費される にリダイレクトされます。このモードは、幅広いアプリケーションの互換性を提供し、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、「セッション内最適化の設定 RTC」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、 内で動作しているアプリケーション WorkSpace 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 Connect 最適化 WorkSpaces
- Genesys Cloud WebRTC メディアヘルパー
- Microsoft Teams SIP Gateway
- 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、「Direct を設定する RTC」を参照してください。

使用するRTC最適化モード

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相互に補完するように設定することもできます。例えば、Cisco Webex 会議RTC用にメディア最適化を有効にすることを検討してください。この設定により、ユーザーはデスクトップクライアント WorkSpace を介して にアクセスするときに最適化された通信を体験できます。ただし、UC 最適化コンポーネントがない共有インターネットから Webex にアクセスするシナリオでは、Webex はシームレスにセッション内最適化RTCモード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、RTC設定モードは固有の要件によって異なる場合があります。

次の表は、UC アプリケーションの一般的な機能を表し、どのRTC設定モードが最適な結果をもたらすかを定義します。

機能	直接 RTC	メディア最適化 RTC	セッション内最適化 RTC
1:1 チャット	RTC 設定は必要ありません		
グループチャットルーム	RTC 設定は必要ありません		

機能	直接 RTC	メディア最適化 RTC	セッション内最適化 RTC
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 設定は必要ありません		
Audio/video clips/messaging	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

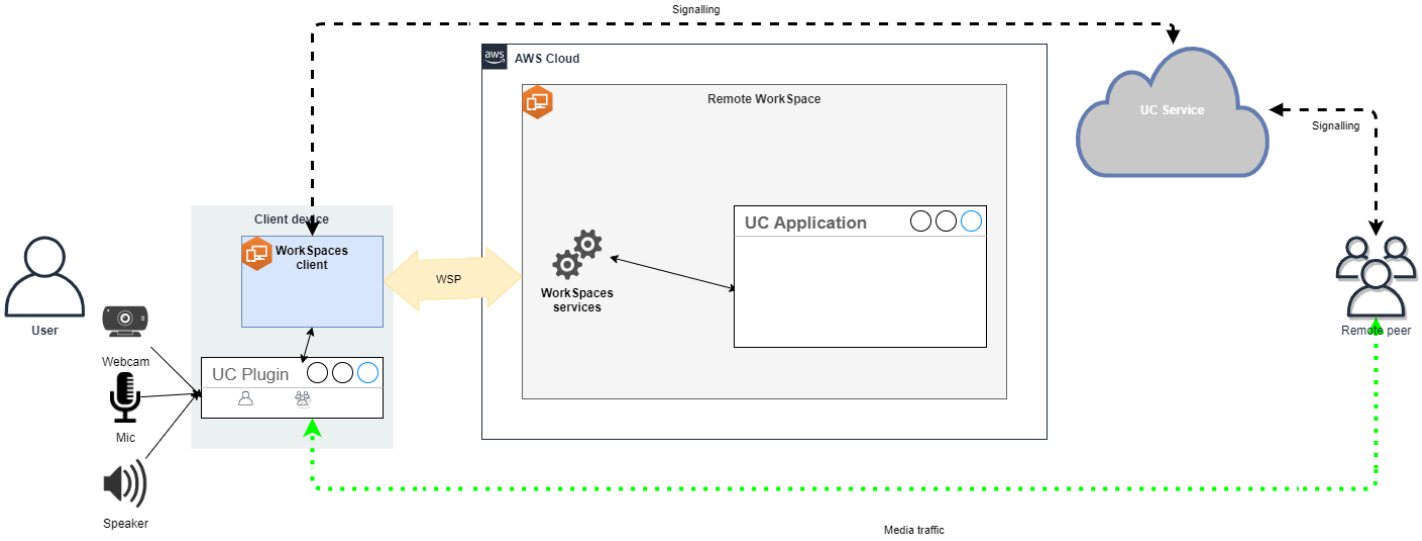
RTC 最適化ガイダンス

メディア最適化の設定 RTC

メディア最適化RTCモードは、UC アプリケーションベンダーが Amazon SDKsが提供する を使用できるようにします。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。

DCV 拡張機能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一般公開されているオプションSDKを含む は、 内で動作する UC アプリケーションモジュール WorkSpace とクライアント側のプラグインとの間に制御チャネルを確立します。通常、この制御チャネルはクライアント拡張機能に通話の開始または通話への参加を指示します。クライアント側拡張機能を通じて通話が確立さ

れると、UC プラグインはマイクからの音声とウェブカメラからのビデオをキャプチャし、それらを UC クラウドまたはコールピアに直接送信します。受信した音声はローカルで再生され、ビデオはリモートクライアント UI にオーバーレイされます。制御チャネルは通話のステータスを伝達します。



Amazon WorkSpaces は現在、メディア最適化RTCモードで次のアプリケーションをサポートしています。

- Zoom 会議 (PCoIPおよび の場合DCV WorkSpaces)
- Cisco Webex 会議 (DCV WorkSpaces のみ)

リストにないアプリケーションを使用している場合は、アプリケーションベンダーに依頼し、WorkSpaces メディア最適化 のサポートをリクエストすることをお勧めしますRTC。このプロセスを迅速化するには、aws-av-offloading@amazon.com に連絡するようお勧めします。

メディア最適化RTCモードでは通話パフォーマンスが向上し、リソース使用率が最小限にWorkSpace抑えられますが、次のような制限があります。

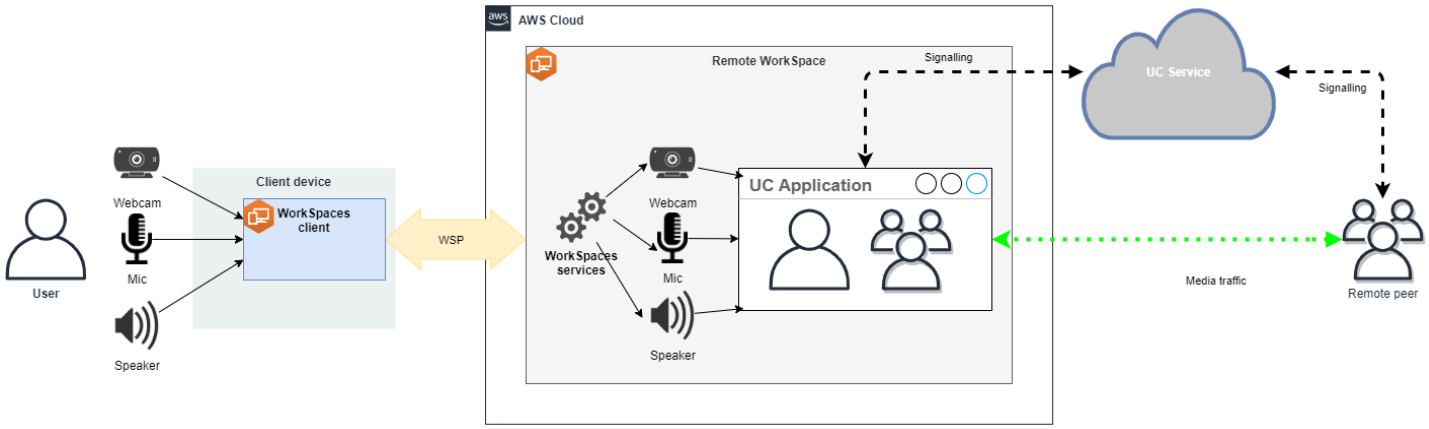
- UC クライアント拡張機能をクライアントデバイスにインストールする必要があります。
- UC クライアント拡張機能は、独立した管理と更新が必要です。
- UC クライアント拡張機能は、モバイルプラットフォームやウェブクライアントなど、特定のクライアントプラットフォームでは使用できない場合があります。
- このモードでは、画面共有の動作が異なる場合があるなど、UC アプリケーションの機能の一部が制限されることがあります。
- クライアント側の拡張機能の使用は、Bring Your Own Device (BYOD) や共有のオリジンなどのシナリオには適していない場合があります。

メディア最適化RTCモードが環境に適していないことが判明した場合、または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、セッション内最適化RTCモードをフォールバックオプションとして設定することをお勧めします。

セッション内最適化の設定 RTC

セッション内最適化RTCモードでは、UC アプリケーションは変更なしで WorkSpaceで動作し、ローカルに似た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、 によってキャプチャDCV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 の両方PCoIP WorkSpaces) とウェブカメラ (のみDCV WorkSpaces) のシグナルがキャプチャされ、 にリダイレクトされ WorkSpace、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向上させるために細心の注意を払って最適化されています。最適化手段には以下が含まれます。

- アダプティブ UDPベースのQUICトランスポートを利用して、効率的なデータ転送を実現します。
- 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。
- 音声最適化オーディオコーデックを実装して、音声品質を維持しながら、 CPUとネットワーク使用率を削減します。
- 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。

これらの最適化は、まとめてリモートRTCモードでの堅牢でスムーズなエクスペリエンスに寄与します。

推奨サイズ

リモートRTCモードを効果的にサポートするには、Amazon の適切なサイジングを確保することが重要です WorkSpaces。リモートは、それぞれの統合通信 (UC) アプリケーションのシステム要件を満たしている WorkSpace 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に、サポートされる最小設定と推奨される WorkSpaces 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	CPU RTC アプリの要件	RAM RTC アプリの要件	最小限サポート WorkSpace	推奨 WorkSpace	最小限サポート WorkSpace	推奨 WorkSpace	リファレンス
Microsoft Teams	2 コア (必須)、4 コア (推奨)	4.0 GB RAM	電力 (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	パフォーマンス (2 vCPU、8 GB メモリ)	電力 (4 vCPU、16 GB メモリ)	Microsoft Teams のハードウェア要件
Zoom	2 コア (必須)、4 コア (推奨)	4.0 GB RAM	電力 (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	パフォーマンス (2 vCPU、8 GB メモリ)	電力 (4 vCPU、16 GB メモリ)	Zoom システム要件: Windows、macOS、Linux
Webex	2 コア (必須)	4.0 GB RAM	電力 (4 vCPU、16 GB メモリ)	PowerPro (8 vCPU、32 GB メモリ)	パフォーマンス (2 vCPU、8 GB メモリ)	電力 (4 vCPU、16 GB メモリ)	Webex サービスのシステム要件

ビデオ会議では、ビデオのエンコードとデコードに大量のリソースが使用されることに注意してください。物理マシンのシナリオでは、これらのタスクは にオフロードされますGPU。以外の ではGPU WorkSpaces、これらのタスクはリモートプロトコルエンコーディングと並行CPUして 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を定期的に行うユーザーには、 設定を選択することを強くお勧めします PowerPro。

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、 以外の場合GPU WorkSpaces、画面共有は多くの場合、より低いフレームレートに制限されます。

を使用した UDPベースのQUICトランスポートの活用 DCV

UDP トランスポートは、RTCアプリケーションの送信に特に適しています。効率を最大化するには、 のQUICトランスポートを利用するようにネットワークが設定されていることを確認します DCV。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のみ使用できることに注意してください。

の UC アプリケーションを設定する WorkSpaces

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、ビデオ処理機能を強化するには、最適なパフォーマンスを実現するには、 GPUが有効な を選択すること WorkSpace が不可欠です。

ほとんどの UC アプリケーションは、高度なビデオ処理を無効にして 以外の のCPU使用率を減らすためのガイダンスを提供しますGPU WorkSpaces。

詳細については、以下のリソースを参照してください。

- Microsoft Teams: 仮想デスクトップ インフラストラクチャ用の Teams
- Zoom 会議: 互換性のないVDIプラグインのユーザーエクスペリエンスの管理
- Webex: Webex App for Virtual Desktop Infrastructure (VDI) のデプロイガイド - Webex App for VDI [Webex App] の管理とトラブルシューティング
- Google Meet: の使用 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、デフォルトでは、オーディオ入力、オーディオ出力、およびビデオ入力によるカメラのリダイレクトを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「 のビデオ入力リダイレクトを有効または無効にDCV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「ウェブカメラやその他のビデオデバイス」を参照してください。

ウェブカメラの最大解像度を制限する

Power またはビデオ会議を使用するユーザー PowerPro WorkSpaces 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。その場合 PowerPro、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

デフォルトでは、 WorkSpaces は 7.1 の忠実度の高いオーディオを からクライアントに配信 WorkSpaces するように設定され、優れた音楽再生品質を実現します。ただし、主なユースケースに音声会議またはビデオ会議が含まれる場合、音声コーデックプロファイルを音声最適化設定に変更すると、 CPUおよび 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
```

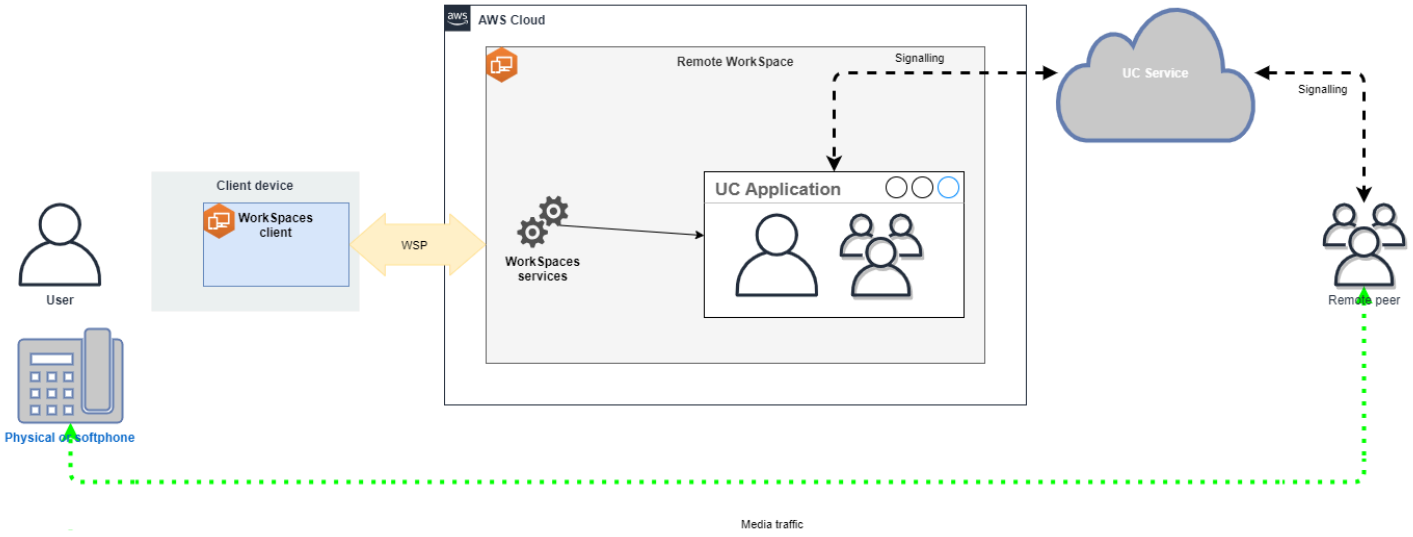
3. `default-profile` と言う名前の文字列値の名前を作成し、`voice` に設定します。

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。

Direct を設定する RTC

ダイレクトRTCモードの設定は、特定の Unified Communication (UC) アプリケーションによって異なり、 WorkSpaces 設定の変更は必要ありません。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 メディアヘルパー
- Amazon Connect:
  - Amazon Connect 最適化 WorkSpaces
- Google Meet:
  - Use a phone for audio in a video meeting

WorkSpaces Personal で実行モードを管理する

の実行モードによって、即時の可用性と支払い方法 (月単位または時間単位) が WorkSpace 決まります。を作成するときに、次の実行モードから選択できます WorkSpace。

- AlwaysOn — を無制限に使用するために固定月額料金を支払うときに使用します WorkSpaces。このモードは、プライマリデスクトップとしてフルタイムを使用する WorkSpaceユーザーに最適です。
- AutoStop - 時間 WorkSpaces 単位で の料金を支払うときに使用します。このモードでは、指定した切断期間が経過すると が WorkSpaces 停止し、アプリケーションとデータの状態が保存されます。

詳細については、WorkSpaces 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 WorkSpace で を選択し、アクション、実行モードのプロパティの変更を選択し、AutoStop 時間 (時間) を設定します。デフォルトでは、AutoStop 時間 (時間) は 1 時間に設定されています。つまり、 WorkSpace は が切断されてから 1 時間後に自動的に WorkSpace 停止します。

WorkSpace が切断され、 AutoStop 期間が終了すると、 が自動的に停止 WorkSpace するまでにさらに数分かかる場合があります。ただし、 AutoStop 期間が終了するとすぐに請求が停止し、その追加時間に対しては課金されません。

可能な場合、デスクトップの状態は 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 WorkSpace 再開され、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が保存された状態に戻ります。

AutoStop Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および は、停止時にデータやプログラムの状態を保持 GraphicsPro WorkSpaces しません。これらの Autostop では WorkSpaces、毎回使用が終了したときに作業を保存することをお勧めします。

Bring-Your-Own-License (BYOL) では AutoStop WorkSpaces、多数の同時ログインにより、 が利用可能 WorkSpaces になるまでの時間が大幅に長くなる可能性があります。多数のユーザーがBYOL AutoStop WorkSpaces 同時に にログインすることが予想される場合は、アカウントマネージャーにアドバイスを求めてください。

> **Important**
>
> AutoStop WorkSpaces WorkSpaces が切断されている場合にのみ、 は自動的に停止します。

WorkSpace は、次の状況でのみ切断されます。

- ユーザーが から手動で切断 WorkSpace するか、Amazon WorkSpaces クライアントアプリケーションを終了した場合。
- クライアントデバイスがシャットダウンされる場合。
- クライアントデバイスと の間に 20 WorkSpace 分以上接続がない場合。

ベストプラクティスとして、 AutoStop WorkSpace ユーザーは毎日使用が終了した WorkSpaces ら、手動で から切断する必要があります。手動で切断するには、Linux、macOS、または Windows 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 Amazon を切断 WorkSpaceまたは終了 WorkSpacesを選択します。Android または の場合はiPad、サイドバーメニューから切断を選択します。

AutoStop WorkSpaces は、次の状況では自動的に停止しない場合があります。

- クライアントデバイスがシャットダウンではなくロック、スリープ、または非アクティブ (ラップトップの蓋が閉じているなど) になっている場合、 WorkSpaces アプリケーションはバックグラウンドで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まだ実行中である限り、 は切断 WorkSpace されないため、 は自動的に停止しない WorkSpace 可能性があります。
- 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、切断を検出できない WorkSpaces 可能性があるため、 が自動的に停止 WorkSpaces せず、請求が停止されない可能性があります。

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。

の実行モードを変更するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. WorkSpace を選択して変更し、アクション、実行モードの変更を選択します。
4. 新しい実行モード、AlwaysOnまたは を選択しAutoStop、保存を選択します。

WorkSpace を使用して 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。

を停止して起動する AutoStop WorkSpace

AutoStop WorkSpaces が切断されると、指定された切断期間が経過すると自動的に停止し、時間単位の請求が中断されます。コストをさらに最適化するために、関連する時間単位の料金を手動で停止できます AutoStop WorkSpaces。は停止し、ユーザーが次回 WorkSpaceにログインしたときにすべてのアプリケーションとデータが保存されます WorkSpace。

ユーザーが停止した に再接続すると WorkSpace、通常は 90 秒以内に中断した場所から再開されます。

使用可能な AutoStop WorkSpaces 、またはエラー状態の再起動 (再起動) を行うことができます。

を停止するには AutoStop WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. 停止 WorkSpace する を選択し、アクション、停止 WorkSpacesを選択します。
4. 確認を求められたら、[Stop WorkSpace] を選択します。

を起動するには AutoStop WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。

3. 開始 WorkSpaces する を選択し、アクション、開始 WorkSpacesを選択します。
4. 確認を求められたら、[Start WorkSpace] を選択します。

に関連付けられている固定インフラストラクチャコストを削除するには AutoStop WorkSpaces、アカウント WorkSpace から 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。

AutoStop WorkSpace を使用して 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

を起動すると WorkSpace、 に関連付けられているすべてのアプリケーションバンドルのリストが WorkSpaces コンソール WorkSpace に表示されます。

に関連付けられているすべてのアプリケーションバンドルのリストを表示するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. 左側のナビゲーションペインから、 を選択しますWorkSpaces。
3. を選択し WorkSpace 、詳細の表示を選択します。
4. アプリケーション で、これに関連付けられているアプリケーションのリスト WorkSpaceとそのインストールステータスを見つけます。

のアプリケーションバンドルは、次の WorkSpace 方法で更新できます。

- にアプリケーションバンドルをインストールする WorkSpace
- からアプリケーションバンドルをアンインストールする WorkSpace
- アプリケーションバンドルをインストールし、 に別のアプリケーションバンドルのセットをアンインストールする WorkSpace

> **Note**
>
> - アプリケーションバンドルを更新するには、 のステータスが `AVAILABLE`または WorkSpace である必要がありますSTOPPED。
> - Manage アプリケーションは Windows でのみ使用できます WorkSpaces。

- [アプリケーションの管理] は、 AWSを通じてサブスクライブされたアプリケーションバンドルでのみ使用できます。

[アプリケーションの管理] でサポートされているバンドル

Manage applications では、 に次のアプリケーションをインストールおよびアンインストールできます WorkSpaces。Microsoft Office 2016 バンドルとMicrosoft Office 2019 の場合は、アンインストールのみが可能です。

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021
- 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

	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 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に従う必要があります。例えば、Standard アプリケーションと Professional アプリケーションを混在させることはできません。
- Microsoft Office/Visio/Project は同じバージョンに従う必要があります。例えば、2019 アプリケーションと 2021 アプリケーションを混在させることはできません。

- Microsoft Office/Visio/Project 2021 Standard/Professionalは、値、グラフィックス、GraphicsPro WorkSpaces バンドルではサポートされていません。
- 値、標準、グラフィックス、 GraphicsPro WorkSpaces バンドルは、Microsoft 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、 PowerProGraphics.g4dn、および 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。
- Microsoft Office 2016 用の Plus アプリケーションバンドルを からアンインストールすると WorkSpaces、その Amazon WorkSpaces バンドルの一部として含まれていた Trend Micro ソリューションにアクセスできなくなります。Amazon で Trend Micro ソリューションを引き続き使用する場合は WorkSpaces、AWS マーケットプレイスで個別に購入できます。
- install/uninstall Microsoft 365 apps, you need to bring in your own tools and installers, Manage application workflow cannot install/uninstall Microsoft 365 アプリに。
- Manage applications を使用して、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 WorkSpaces を含む 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、ディレクトリレベルで WorkSpaces インターネット接続を有効にする必要があります。

でアプリケーションバンドルを更新する WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、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を選択します。
4. 現在のアプリケーションには、この WorkSpace に既にインストールされているアプリケーションバンドルのリストが表示され、アプリケーションの選択には、この にインストールできるアプリケーションバンドルのリストが表示されます WorkSpace。
5. これにアプリケーションバンドルをインストールするには WorkSpace :
   a. インストールするアプリケーションバンドルを選択し WorkSpace、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. ここからアプリケーションバンドルをアンインストールするには WorkSpace :

a. [アプリケーションの選択] で、アンインストールするアプリケーションバンドルを選択し、[関連付け解除] を選択します。

b. 前のステップを繰り返して、他のアプリケーションバンドルをアンインストールします。

c. アプリケーションバンドルのアンインストール中は、[現在のアプリケーション] の下で、`Pending uninstall deployment` 状態でバンドルが表示されます。

7. バンドルのインストールまたはインストール状態を元に戻すには、次のいずれかを実行します。

- バンドルを `Pending uninstall deployment` 状態から戻す場合は、元に戻すアプリケーションを選択し、[関連付け] を選択します。
- バンドルを `Pending install deployment` 状態から戻す場合は、元に戻すアプリケーションを選択し、[関連付け解除] を選択します。

8. インストールまたはアンインストールを選択したアプリケーションバンドルが保留状態になったら、[アプリケーションのデプロイ] を選択します。

> **Important**
>
> アプリケーションのデプロイを選択すると、エンドユーザーセッションは終了し WorkSpaces 、アプリケーションのインストールまたはアンインストール中はアクセスできなくなります。

9. アクションを確認するには、「確認」と入力します。[強制] を選択して、[エラー] 状態のアプリケーションバンドルをインストールまたはアンインストールします。

10. アプリケーションバンドルの進行状況をモニターリングするには:

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

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。

- UPDATING - アプリケーションバンドルの更新はまだ進行中です。
- AVAILABLE / STOPPED - アプリケーションバンドルの更新が完了し、 WorkSpace は元の状態に戻ります。

c. アプリケーションバンドルのインストールまたはアンインストールのステータスをモニタリングするには、 WorkSpace を選択し、詳細の表示を選択します。[アプリケーション] の [ステータス] には、`Pending install`、`Pending uninstall`、`Installed` などのステータスが表示されます。

> **Note**
>
> マネージドアプリケーションを介し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有効化されていないことがユーザーに確認された場合は、手動で WorkSpace 再起動できます。ユーザーは、再起動後にこれらのアプリケーションの使用を開始できます。その他のサポートについては、AWS サポートにお問い合わせください。

で Microsoft Visual Studio 2022 ワークロードを更新する WorkSpace

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 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。

Manage アプリケーションを使用した WorkSpaces 変更済み の管理

にアプリケーションバンドルをインストールまたはアンインストールすると WorkSpaces、以下のアクションが既存の設定に影響を与える可能性があります。

- の復元 WorkSpace - を復元すると、 が正常 WorkSpace であったときに作成されたこれらのボリュームの最新のスナップショットに基づいて、ルートボリュームとユーザーボリュームの両方が WorkSpace 再作成されます。完全な WorkSpace スナップショットは 12 時間ごとに作成されます。詳細については、「 の復元 WorkSpace」を参照してください。少なくとも 12 時間待ってから、Manage アプリケーションを使用して変更された WorkSpaces を復元してください。Manage アプリケーションを使用して変更された次の完全なスナップショット WorkSpaces の前に を復元すると、次の結果になります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して にインストールされたアプリケーションバンドルは から削除されます WorkSpaces が、ライセンスは引き続き有効になり、それらのアプリケーションに対して に課金 WorkSpaces されます。これらのアプリケーションバンドルを に戻すには、アプリケーション管理ワークフローを再度実行し、アプリケーションをアンインストールして新しく起動してから、再度インストール WorkSpaces する必要があります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して から削除されたアプリケーションバンドルは、 に戻ります WorkSpaces。ただし、ライセンスのアクティブ化が行われないため、これらのアプリケーションバンドルは正しく動作しません。これらのアプリケーションバンドルを削除するには、 からこれらのアプリケーションバンドルを手動でアンインストールします WorkSpaces。
- の再構築 WorkSpace - を再構築すると、ルートボリュームが WorkSpace 再作成されます。詳細については、「 の再構築 WorkSpace」を参照してください。Manage アプリケーションを使用して WorkSpaces 変更された を再構築すると、次のようになります。
  - アプリケーション管理ワークフロー WorkSpaces を使用して にインストールされたアプリケーションバンドルは、 から削除され、非アクティブ化されます WorkSpaces。これらのアプリケーションを に戻すには、アプリケーション管理ワークフローを再度実行 WorkSpaces する必要があります。
  - アプリケーション管理ワークフロー WorkSpaces を介して から削除されたアプリケーションバンドルは、 にインストールされ、アクティブ化されます WorkSpaces。これらのアプリケーションバンドルを から削除するには WorkSpaces、アプリケーション管理ワークフローを再度実行する必要があります。
- の移行 WorkSpace - 移行プロセス WorkSpace では、ターゲットバンドルイメージから新しいルートボリュームを使用し、元の の最後に使用可能なスナップショットからユーザーボリューム

を使用して を再作成します WorkSpace。新しい WorkSpace ID WorkSpace を持つ新しい が作成されます。詳細については、「アプリケーションの WorkSpace管理を使用して WorkSpaces 変更された の移行では、次の結果になります。」を参照してください。

- ソースからのすべてのアプリケーションバンドル WorkSpaces は削除され、非アクティブ化されます。新しい送信先 WorkSpaces は、送信先 WorkSpaces バンドルからアプリケーションを継承します。ソース WorkSpaces アプリケーションバンドルは 1 か月分の料金が請求されますが、送信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された料金が請求されます。

Personal WorkSpace で を変更する WorkSpaces

を起動した後 WorkSpace、次の 3 つの方法で設定を変更できます。

- ルートボリューム (Windows の場合はドライブ C、Linux の場合は /)、およびユーザーボリューム (Windows の場合はドライブ D、Linux の場合は /home) のサイズを変更できます。
- コンピューティングタイプを変更して、新しいバンドルを選択できます。
- ストリーミングプロトコルは、 バンドルで WorkSpace を作成APIした場合は、 AWS CLIまたは Amazon WorkSpaces を使用して変更できますPCoIP。

の現在の変更状態を確認するには WorkSpace、矢印を選択して詳細を表示します WorkSpace。[状態] に表示される値は、[コンピューティングの変更]、[ストレージの変更]、および [なし] です。

を変更する場合は WorkSpace、ステータスが AVAILABLEまたは である必要がありますSTOPPED。ボリュームサイズとコンピューティングタイプを同時に変更することはできません。

のボリュームサイズまたはコンピューティングタイプを変更すると、 の請求レート WorkSpace が変更されます WorkSpace。

ユーザーがボリュームとコンピューティングタイプを変更できるようにするには、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

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すことができます。各 WorkSpace ルートボリュームとユーザーボリュームには WorkSpace、変更できないセットグループが付属しています。使用可能なグループは以下のとおりです。

[ルート (GB)、ユーザー (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 ～ 2,000、100 ～ 2,000]

ルートボリュームとユーザーボリュームは、暗号化されているかどうかにかかわらず拡張できます。両方のボリュームとも、6 時間に 1 回拡張できます。ただし、ルートボリュームとユーザーボリュームのサイズを同時に増やすことはできません。詳細については、「Limitations for Increasing Volumes」を参照してください。

> **Note**
>
> のボリュームを拡張すると WorkSpace、 は Windows または Linux 内でボリュームのパーティション WorkSpaces を自動的に拡張します。プロセスが完了したら、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、 の起動後にルートボリュームまたはユーザーボリュームのサイズを小さくすることはできません WorkSpace。代わりに、 を起動するときに、これらのボリュームの最小サイズを必ず指定してください WorkSpace。ルートボリュームの場合は PowerPro WorkSpace 80 GB、ユーザーボリュームの場合は 10 GB 以上の値、標準、パフォーマンス、パワー、または を起動できます。Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または は、ルートボリュームの場合は 100 GB、ユーザーボリュームの場合は 100 GB GraphicsPro WorkSpace で起動できます。

WorkSpace ディスクサイズの増加が進行中、ユーザーはほとんどのタスクを で実行できます WorkSpace。ただし、 WorkSpace コンピューティングタイプの変更、 WorkSpace 実行モードの切り替え、 の再構築 WorkSpace、 の再起動 (再起動) はできません WorkSpace。

> **Note**
>
> ディスクサイズの増加の進行 WorkSpaces 中にユーザーが を使用できるようにする場合は、 のボリュームのサイズを変更するSTOPPED前に、 WorkSpaces のステータス

が AVAILABLEではなく であることを確認します WorkSpaces。 WorkSpaces が の場合STOPPED、ディスクサイズの増加の進行中に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 のボリュームサイズを変更する場合 WorkSpaces、プロセスにかなり時間がかかることがあります。変更 WorkSpaces する が多数ある場合は、 に連絡してサポート AWS Support を受けることをお勧めします。

ボリューム増加の制限

- SSD ボリュームのみサイズを変更できます。
- を起動するときは WorkSpace、ボリュームのサイズを変更するまで 6 時間待つ必要があります。
- ルートボリュームとユーザーボリュームのサイズを同時に増やすことはできません。ルートボリュームを増やすには、まずユーザーボリュームを 100 GB に変更する必要があります。この変更を行った後、ルートボリュームを 175～2000 GB の任意の値に更新できます。ルートボリュームを 175～2000 GB の任意の値に変更した後、ユーザーボリュームを 100～2000 GB の任意の値にさらに更新できます。

  > **Note**
  >
  > 両方のボリュームを増やす場合は、最初の操作が終了するまで 20～30 分待ってから 2 番目の操作を開始する必要があります。

- WorkSpace が Graphics.g4dn、 GraphicsPro.g4dn、Graphics、または でない限り GraphicsPro WorkSpace、ユーザーボリュームが 100 GB の場合、ルートボリュームは 175 GB 未満にすることはできません。Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro WorkSpaces では、ルートボリュームとユーザーボリュームの両方を 100 GB 以上に設定できます。
- ユーザーボリュームが 50 GB の場合、ルートボリュームを 80 GB 以外に更新することはできません。ルートボリュームが 80 GB の場合、ユーザーボリュームは 10、50、または 100 GB のみに設定できます。

のルートボリュームを変更するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。

3. WorkSpace を選択し、アクション、ルートボリュームの変更を選択します。
4. [Root volume sizes] (ルートボリュームサイズ) でボリュームサイズを選択するか、[Custom] (カスタム) を選択してカスタムボリュームサイズを入力します。
5. [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、変更を有効にするために を再起動 WorkSpaceする必要があります。データ損失を避けるため、 を再起動する前に、開いているファイルをユーザーが保存していることを確認してください WorkSpace。

のユーザーボリュームを変更するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. WorkSpace を選択し、アクション、ユーザーボリュームの変更を選択します。
4. [User volume sizes] (ユーザーボリュームサイズ) でボリュームサイズを選択するか、[Custom] (カスタム) を選択してカスタムボリュームサイズを入力します。
5. [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、変更を有効にするために を再起動 WorkSpaceする必要があります。データ損失を避けるため、 を再起動する前に、開いているファイルをユーザーが保存していることを確認してください WorkSpace。

のボリュームサイズを変更するには WorkSpace

`RootVolumeSizeGib` または `UserVolumeSizeGib`プロパティで modify-workspace-properties コマンドを使用します。

コンピューティングタイプの変更

は、スタンダード、パワー、パフォーマンス、 PowerPro コンピューティングタイプ WorkSpace の間で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 Bundles」を参照してください。

> **Note**
>
> - コンピューティングタイプは Graphics.g4dn から GraphicsPro.g4dn に、または Graphics GraphicsPro.g4dn から Graphics.g4dn に変更できます。Graphics.g4dn および GraphicsPro.g4dn のコンピューティングタイプを他の値に変更することはできません。

- 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。を WorkSpaces Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。
- GraphicsPro バンドルは end-of-life 2025 年 10 月 31 日に終了します。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、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。
- Graphics および のコンピューティングタイプを他の値 GraphicsPro に変更することはできません。

コンピューティングの変更をリクエストすると、 は新しいコンピューティングタイプ WorkSpace を使用して WorkSpaces を再起動します。 は、 のオペレーティングシステム、アプリケーション、データ、ストレージ設定 WorkSpaces を保持します WorkSpace。

より大きなコンピューティングタイプは 6 時間に 1 回、より小さなコンピューティングタイプは 30 日に 1 回リクエストできます。新しく起動した の場合 WorkSpace、より大きなコンピューティングタイプをリクエストする前に 6 時間待つ必要があります。

WorkSpace コンピューティングタイプの変更が進行中の場合、ユーザーは から切断され WorkSpace、 を使用または変更することはできません WorkSpace。 WorkSpace は、コンピューティングタイプの変更プロセス中に自動的に再起動されます。

Important

データ損失を回避するには、 WorkSpace コンピューティングタイプを変更する前に、開いているドキュメントやその他のアプリケーションファイルをユーザーが保存していることを確認してください。

コンピューティングタイプの変更プロセスには、最大 1 時間かかる場合があります。

のコンピューティングタイプを変更するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. WorkSpace を選択し、アクション、コンピューティングタイプの変更を選択します。

4. [Compute type] (コンピューティングタイプ) で、コンピューティングタイプを選択します。
5. [Save changes] (変更の保存) をクリックします。

のコンピューティングタイプを変更するには WorkSpace

`ComputeTypeName` プロパティで modify-workspace-properties コマンドを使用します。

プロトコルの変更

WorkSpace がPCoIPバンドルで作成されている場合は、 または Amazon AWS CLIを使用してストリーミングプロトコルを変更できます WorkSpaces API。これにより、移行機能を使用 WorkSpace せずに、既存の を使用してプロトコルを WorkSpace 移行できます。これにより、移行プロセス PCoIP WorkSpaces 中に既存の を再作成することなく、ルートボリュームを使用DCVおよび維持することもできます。

- プロトコルを変更できるのは、 WorkSpace がPCoIPバンドルで作成され、 GPUが有効になっていない場合のみです WorkSpace。
- プロトコルを に変更する前にDCV、 WorkSpace が の次の要件を満たしていることを確認してくださいDCV WorkSpace。
  - WorkSpaces クライアントが をサポートしている DCV
  - がデプロイされているリージョン WorkSpace が をサポート DCV
  - の IP アドレスとポートの要件DCVはオープンです。詳細については、「 の IP アドレスとポートの要件 WorkSpaces」を参照してください。
  - 現在のバンドルが で使用可能であることを確認しますDCV。
  - ビデオ会議で最高のエクスペリエンスを得るには、Power または PowerPro バンドルのみを使用することをお勧めします。

> **Note**
>
> - プロトコルの変更 WorkSpaces を開始する前に、非本番環境でテストすることを強くお勧めします。
> - プロトコルを から PCoIPに変更しDCV、プロトコルを に戻した場合PCoIP、Web Access WorkSpaces 経由で に接続することはできません。

のプロトコルを変更するには WorkSpace

1. 〔オプション] を再起動 WorkSpace し、 AVAILABLE状態になるまで待ってからプロトコルを変更します。
2. 〔オプション] describe-workspaces コマンドを使用して WorkSpace プロパティを一覧表示します。それが AVAILABLE 状態にあり、現在の Protocol が正しいことを確認します。
3. modify-workspace-properties コマンドを使用して、Protocols プロパティを PCOIP から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、 が WorkSpace 再起動して必要な設定が完了するまでに最大 20 分かかることがあります。
5. describe-workspaces コマンドを再度使用してプロパティを WorkSpace一覧表示し、それが AVAILABLE状態であり、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、コンソールでバンドルの説明は更新されません。[Launch Bundle] (バンドルの起動) という表示は変わりません。
> - が 20 分経過しても UNHEALTHY状態 WorkSpace のままの場合は、 コンソール WorkSpace で を再起動します。

6. これで、 に接続できます WorkSpace。

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。

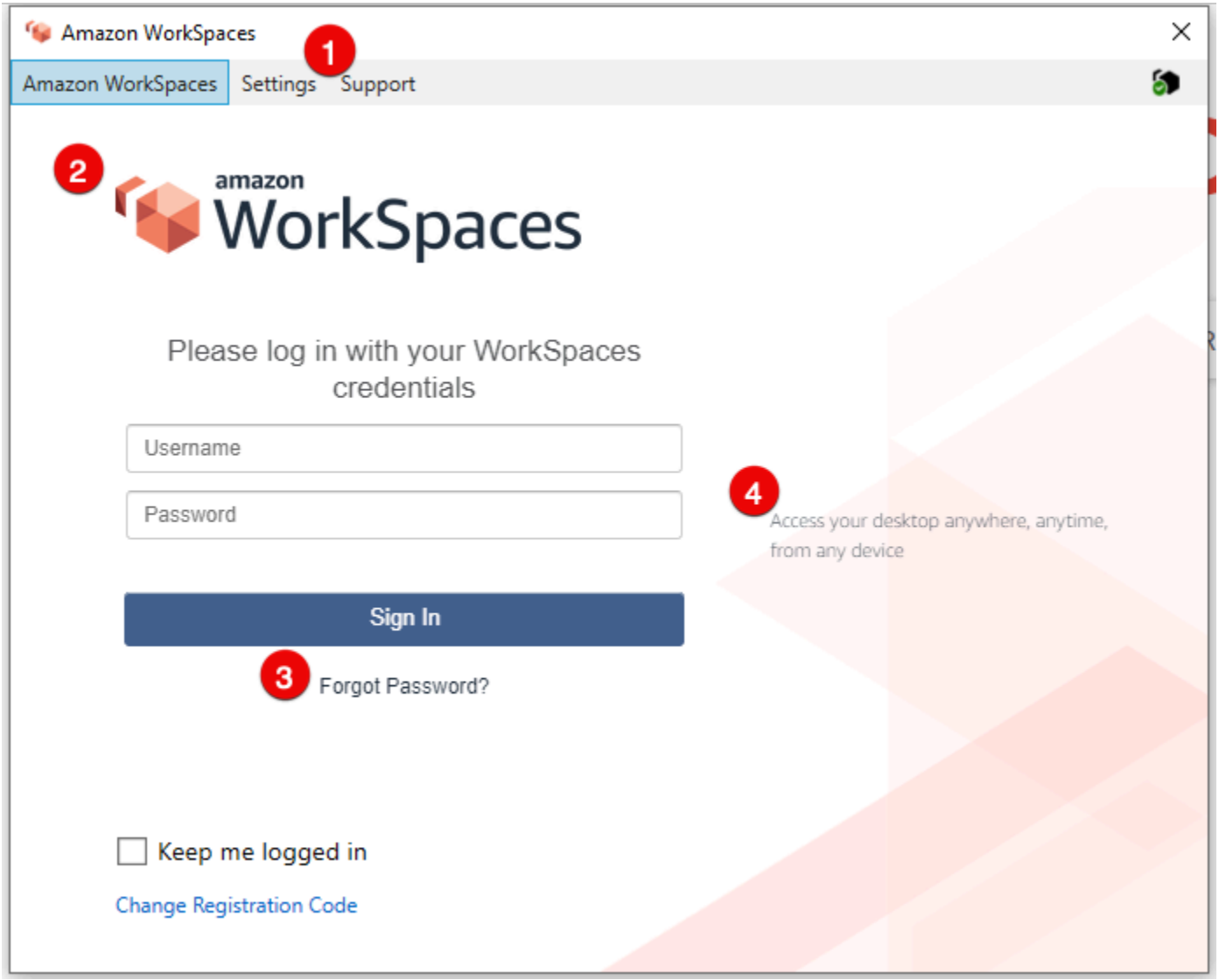
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> AWS GovCloud (US) Region の ClientBranding API を使用してブランド要素を変更するには、WorkSpaces クライアントバージョン 5.10.0 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。 • デフォルトの E メールは workspaces-feedback@amazon.com です。 • 長さの制限: 最小長は 1 です。最大長は 200 です。

ロゴ	Logo 属性を使用して、組織のロゴをカスタマイズできます。	• イメージ形式は、.png ファイルから変換したバイナリ形式のデータオブジェクトのみ使用できます。
		• 推奨解像度:
		  • Android: 978 x 190
		  • デスクトップ: 319 x 55
		  • iOS@2x: 110 x 200
		  • iOS@3x: 1650 x 300

パスワードを忘れた場合のリンク	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：最小長は 1 です。最大長は 200 です。

ブランド要素	説明	要件と推奨事項
ログインメッセージ	`LoginMessage` 属性を使用して、サインイン画面のメッセージをカスタマイズできます。	• 長さの制限: 最小長は 0 です。HTML タグおよび異なるフォントサイズを統合するための最大長は 2,000 文字です。HTML タグがないデフォルトの場合は、ログインメッセージは 600 文字未満にすることをお勧めします。 • サポートされている HTML タグ: `a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

以下は、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。タグの使用は、AWS リソースの管理やデータ (請求データなど) の整理を行うシンプルかつ強力な方法です。

既存のリソースにタグを追加すると、これらのタグは翌月の初日までコスト配分レポートに表示されません。例えば、7 月 15 日に既存の WorkSpace にタグを追加した場合、8 月 1 日までタグはコスト配分レポートに表示されません。詳細については、AWS Billing の「コスト配分タグの使用」を参照してください。

> **Note**
>
> Cost Explorer で WorkSpaces リソースタグを表示するには、AWS Billing ユーザーガイドの「ユーザー定義コスト配分タグのアクティブ化」の手順に従って、WorkSpaces リソースに適用したタグをアクティブにする必要があります。
> タグはアクティベーション後 24 時間後に表示されますが、これらのタグに関連付けられた値が Cost Explorer に表示されるまでに 4 ~ 5 日かかる場合があります。さらに、Cost Explorer でコストデータを表示して提供するには、タグ付けされた WorkSpaces リソースにその期間中に料金が発生する必要があります。[Cost Explorer] には、タグが有効化されてからそれまでのコストデータのみが表示されます。現時点では、履歴データはありません。

タグ付けできるリソース

- WorkSpaces、インポートされたイメージ、および IP アクセスコントロールグループの各リソースは、作成時にタグを追加できます。
- 既存のリソースタイプ (WorkSpaces、登録されたディレクトリ、カスタムバンドル、イメージ、および IP アクセスコントロールグループ) にタグを追加できます。

タグの制限

- リソースあたりのタグの最大数 – 50
- キーの最大長 – 127 文字 (Unicode)
- 値の最大長 – 255 文字 (Unicode)
- タグのキーと値は大文字と小文字が区別されます。使用できる文字は、UTF-8 で表現できる文字、スペース、および数字と、特殊文字 (+、-、=、.、_、:、/、@) です。ただし、先頭または末尾にはスペースを使用しないでください。
- タグの名前または値に `aws:` または `aws:workspaces:` プレフィックスは使用しないでください。これらのプレフィックスは AWS 用に予約されています。これらのプレフィックスが含まれるタグの名前または値は編集または削除できません。

コンソール (ディレクトリ、WorkSpaces、または IP アクセスコントロールグループ) を使用して既存のリソースのタグを更新するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで、ディレクトリ、WorkSpaces、または IP アクセスコントロール のいずれかのリソースタイプを選択します。
3. リソースを選択して、詳細ページを開きます。
4. 次の 1 つ以上の操作を行います。
   - タグを更新するには、[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. WorkSpaces コンソール (https://console.aws.amazon.com/workspaces/) を開きます。
2. ナビゲーションペインで、[Bundles] (バンドル) または [Images] (イメージ) のうち、いずれかのリソースタイプを選択します。
3. リソースを選択して、詳細ページを開きます。
4. [タグ] で、[タグの管理] を選択します。
5. 次の 1 つ以上の操作を行います。

- タグを更新するには、[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/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Directories] を選択します。
3. ディレクトリを選択し、[Actions]、[Update Details] の順に選択します。
4. [メンテナンスモード] を展開します。
5. 自動更新を有効にするには、[Enabled] を選択します。更新を手動で管理する場合は、[無効] を選択します。
6. [Update and Exit] を選択します。

手動メンテナンス

必要に応じて、独自のスケジュールで WorkSpaces を管理できます。メンテナンスタスクを実行する場合は、WorkSpace の状態を [Maintenance] (メンテナンス) に変更することをお勧めします。完了したら、WorkSpace の状態を [Available] (使用可能) に変更します。

WorkSpace が [Maintenance] (メンテナンス) 状態の場合、以下の動作が発生します。

- WorkSpace は、再起動、停止、起動、再構築には対応しません。
- ユーザーは WorkSpace にログインできません。
- AutoStop WorkSpace は、休止状態ではありません。

コンソールを使用して WorkSpace の状態を変更するには

> **Note**
>
> WorkSpace の状態を変更するには、WorkSpace のステータスが [Available] (使用可能) である必要があります。WorkSpace が [Available] (使用可能) 状態ではない場合、[Modify state] (変更状態) の設定は使用できません。

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces] を選択します。
3. WorkSpace を選択して、[Actions] (アクション)、[Modify state] (状態の変更) の順に選択します。
4. [Modify state] (状態の変更) で、[Available] (使用可能) または [Maintenance] (メンテナンス) を選択します。
5. [Save] を選択します。

AWS CLI を使用して WorkSpace の状態を変更するには

modify-workspace-state コマンドを使用します。

WorkSpaces Personal WorkSpaces で暗号化

WorkSpaces は AWS Key Management Service () と統合されていますAWS KMS。これにより、AWS KMS キー WorkSpaces を使用して のストレージボリュームを暗号化できます。を起動すると WorkSpace、ルートボリューム (Microsoft Windows の場合は C ドライブ、Linux の場合は /) とユーザーボリューム (Windows の場合は D ドライブ、Linux の場合は /home) を暗号化できます。これにより、保管時のデータ、ボリュームへのディスク I/O、ボリュームから作成されたスナップショットを暗号化することができます。

> **Note**
>
> - の暗号化に加えて WorkSpaces、特定の AWS 米国リージョンでFIPSエンドポイント暗号化を使用することもできます。詳細については、「WorkSpaces Personal の FedRAMP 認可または DoD SRG コンプライアンスを設定する」を参照してください。
> - BitLocker 暗号化は Amazon ではサポートされていません WorkSpaces。

内容

- 前提条件
- 制限
- を使用した WorkSpaces 暗号化の概要 AWS KMS
- WorkSpaces 暗号化コンテキスト
- ユーザーに代わってKMSキーを使用するアクセス WorkSpaces 許可を付与する
- の暗号化 WorkSpace
- 暗号化された を表示する WorkSpaces

前提条件

暗号化プロセスを開始する前に、 AWS KMS キーが必要です。このKMSキーは、Amazon の AWS マネージドKMSキー WorkSpaces（ aws/workspaces) または対称カスタマーマネージドKMSキーのいずれかです。

- AWS マネージドKMSキー – リージョンの WorkSpaces コンソール WorkSpace から暗号化されていない を初めて起動すると、Amazon はアカウントに AWS マネージドKMSキー (aws/workspaces) WorkSpaces を自動的に作成します。この AWS マネージドKMSキーを選択すると、のユーザーボリュームとルートボリュームを暗号化できます WorkSpace。詳細については、「を使用した WorkSpaces 暗号化の概要 AWS KMS」を参照してください。

  この AWS マネージドKMSキーは、ポリシーや権限を含めて表示でき、 AWS CloudTrail ログでその使用を追跡できますが、このKMSキーを使用または管理することはできません。Amazon はこのKMSキー WorkSpaces を作成および管理します。Amazon のみがこのKMSキー WorkSpaces を使用 WorkSpaces でき、アカウント内の WorkSpaces リソースの暗号化にのみ使用できます。

AWS Amazon が WorkSpaces サポートしているものを含む 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AWS KMS 「キーのローテーション」を参照してください。

- カスタマーマネージドKMSキー – または、 を使用して作成した対称カスタマーマネージドKMSキーを選択できます AWS KMS。ポリシーの設定を含め、このKMSキーを表示、使用、管理できます。KMS キーの作成の詳細については、「 AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。を使用してKMSキーを作成する方法の詳細については AWS KMS API、「 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。

  カスタマーマネージドKMSキーは、自動キーローテーションを有効にしない限り、自動的にローテーションされません。詳細については、「 AWS Key Management Service デベロッパーガイド」のAWS KMS 「キーのローテーション」を参照してください。

> **Important**
>
> KMS キーを手動でローテーションするときは、元のKMSキーと新しいKMSキーの両方を有効にして、 が元のKMSキーが暗号化 WorkSpaces した を復号 AWS KMS できるようにする必要があります。元のKMSキーを有効にしたくない場合は、 を再作成 WorkSpacesし、新しいKMSキーを使用して暗号化する必要があります。

AWS KMS キーを使用して を暗号化するには、次の要件を満たす必要があります WorkSpaces。

- KMSキーは対称である必要があります。Amazon WorkSpaces は非対称KMSキーをサポートしていません。対称KMSキーと非対称キーの区別については、「 AWS Key Management Service デベロッパーガイド」の「対称キーと非対称KMSキーの識別」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には、「 AWS Key Management Service デベロッパーガイド」のKMS「キーの詳細の表示」を参照してください。
- KMSキーに関連付けられた正しいアクセス許可とポリシーが必要です。詳細については、「パート 2: IAMポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する」を参照してください。

制限

- 既存の を暗号化することはできません WorkSpace。の起動 WorkSpace 時に暗号化する必要があります。
- 暗号化された からのカスタムイメージの作成 WorkSpace はサポートされていません。
- 暗号化された の暗号化の無効化 WorkSpace は現在サポートされていません。
- WorkSpaces ルートボリュームの暗号化を有効にして起動すると、プロビジョニングに最大 1 時間かかる場合があります。
- 暗号化された を再起動または再構築するには WorkSpace、まず キーが有効になっている AWS KMS ことを確認します。有効でない場合、 WorkSpace は使用できなくなります。KMS キーが有効になっているかどうかを確認するには、「 AWS Key Management Service デベロッパーガイド」のKMS「キーの詳細の表示」を参照してください。

を使用した WorkSpaces 暗号化の概要 AWS KMS

暗号化されたボリューム WorkSpaces で を作成すると、 は Amazon Elastic Block Store (Amazon EBS) WorkSpaces を使用してそれらのボリュームを作成および管理します。Amazon EBS は、業界標準の AES-256 アルゴリズムを使用して、データキーでボリュームを暗号化します。Amazon EBSと Amazon はどちらもKMSキー WorkSpaces 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 ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。 EC2

暗号化されたボリューム WorkSpaces で を起動すると、このプロセスは次の end-to-endようになります。

1. 暗号化に使用するKMSキーと、 のユーザーとディレクトリを指定します WorkSpace。このアクションは、 がKMSキーをこの目的にのみ使用 WorkSpaces できるようにする許可を作成します。 WorkSpaceつまり、指定されたユーザーとディレクトリに関連付けられた に対してのみ WorkSpace許可を作成します。
2. WorkSpaces は の暗号化されたEBSボリュームを作成し WorkSpace 、使用するKMSキーとボリュームのユーザーとディレクトリを指定します。このアクションにより、Amazon がこの KMS WorkSpace および ボリュームにのみキーEBSを使用できるようにする権限が作成されます。つまり、指定されたユーザーおよびディレクトリ WorkSpace に関連付けられた に対してのみ、指定された ボリュームに対してのみ付与されます。

3. Amazon は、 キーで暗号化されたボリュームデータKMSキーをEBSリクエストし、 WorkSpace ユーザーの Active Directory セキュリティ識別子 (SID) と AWS Directory Service ディレクトリ ID、および暗号化コンテキストとして Amazon EBSボリューム ID を指定します。
4. AWS KMS は新しいデータキーを作成し、KMSキーで暗号化してから、暗号化されたデータキーを Amazon に送信しますEBS。
5. WorkSpaces は Amazon EBSを使用して、暗号化されたボリュームを にアタッチします WorkSpace。Amazon 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EBSに送信しSID、暗号化コンテキストとして使用される WorkSpace ユーザーの 、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 に送信しますEBS。
7. Amazon EBSは、プレーンテキストのデータキーを使用して、暗号化されたボリュームとの間で送受信されるすべてのデータを暗号化します。Amazon は、ボリュームが にアタッチされている限り、プレーンテキストのデータキーをメモリにEBS保持します WorkSpace。
8. Amazon は、 を再起動または再構築する場合に備えて、暗号化されたデータキー (で受信Step 4) をボリュームメタデータとともにEBS保存します WorkSpace。
9. を使用して AWS Management Console を削除する WorkSpace （ または で `TerminateWorkspaces`アクションを使用する WorkSpaces API) WorkSpaces と、Amazon EBS はその のKMSキーの使用を許可した許可を廃止します WorkSpace。

WorkSpaces 暗号化コンテキスト

WorkSpaces はKMS、キーを暗号化オペレーション (`Encrypt`、、 など) `Decrypt`に直接使用しません。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 が (Step 3 の を使用した WorkSpaces 暗号化の概要 AWS KMS) の暗号化されたボリュームの暗号化されたデータキー WorkSpaces をEBSリクエストし、そのデータキーのプレーンテキストコピーをリクエストすると (Step 5) 、リクエストに暗号化コンテキストが含まれます。

暗号化コンテキストは、データの整合性を確保するために が 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るため、特定のKMSキーが使用された理由を理解するのに役立ちます。Amazon は、暗号化コンテキストに以下EBSを使用します。

- に関連付けられている Active Directory ユーザーのセキュリティ識別子 (SID ） WorkSpace
- に関連付けられているディレクトリの AWS Directory Service ディレクトリ ID WorkSpace

- 暗号化されたEBSボリュームの Amazon ボリューム ID

次の例は、Amazon がEBS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キーを使用するアクセス WorkSpaces 許可を付与する

(aws/workspaces) の WorkSpaces AWS マネージドKMSキーまたはカスタマーマネージドKMSキーで WorkSpace データを保護できます。カスタマーマネージドKMSキーを使用する場合は、アカウントの WorkSpaces 管理者に代わってKMSキーを使用する WorkSpaces アクセス許可を付与する必要があります。の WorkSpaces AWS マネージドKMSキーには、デフォルトで必要なアクセス許可があります。

で使用するカスタマーマネージドKMSキーを準備するには WorkSpaces、次の手順を使用します。

1. KMSキーのキーポリシーのキーユーザーのリストに WorkSpaces 管理者を追加する
2. IAMポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する

WorkSpaces 管理者には、 を使用するためのアクセス許可も必要です WorkSpaces。これらのアクセス許可の詳細については、の Identity and Access Management WorkSpaces にアクセスしてください。

パート 1: WorkSpaces 管理者をキーユーザーとして に追加する

WorkSpaces 管理者に必要なアクセス許可を付与するには、 AWS Management Console または を使用できます AWS KMS API。

KMS キーのキーユーザーとして WorkSpaces 管理者を追加するには (コンソール)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/kms で AWS Key Management Service （ AWS KMS) コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクタを使用します。
3. ナビゲーションペインで、[カスタマーマネージドキー] 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 ID またはエイリアスを選択します。
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、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を取得し、ポリシードキュメントをファイルに保存します。
2. 任意のテキストエディタでポリシードキュメントを開きます。 WorkSpaces 管理者に対応するIAMユーザーとロールを、キーユーザーにアクセス許可を付与するポリシーステートメントに追加します。その後、ファイルを保存します。
3. PutKeyPolicy オペレーションを使用して、キーポリシーをKMSキーに適用します。

パート 2: IAMポリシーを使用して WorkSpaces 管理者に追加のアクセス許可を付与する

暗号化に使用するカスタマーマネージドKMSキーを選択する場合は、暗号化を起動するアカウントの IAM ユーザーに代わって Amazon がKMSキー WorkSpaces を使用できるようにするIAMポリシーを確立する必要があります WorkSpaces。そのユーザーには、Amazon を使用するためのアクセス許可も必要です WorkSpaces。IAM ユーザーポリシーの作成と編集の詳細については、「 IAM ユーザーガイド」のIAM「ポリシーの管理」および「」を参照してくださいの Identity and Access Management WorkSpaces。

WorkSpaces 暗号化には、 KMS キーへの制限付きアクセスが必要です。以下は、使用できるサンプルキーのポリシーです。このポリシーにより、 AWS KMS キーを管理できるプリンシパルと、このキーを使用できるプリンシパルが分離されます。このサンプルキーポリシーを使用する前に、サンプルアカウント ID と IAM ユーザー名を、アカウントの実際の値に置き換えてください。

最初のステートメントは、デフォルトの AWS KMS キーポリシーと一致します。これにより、 IAM ポリシーを使用してKMSキーへのアクセスを制御する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 キーを使用できるようにします。このステートメントは、 AWS のサービスが許可を作成、管理できるようにします。ステートメントは、 KMS キーに対する許可を、 アカウントのユーザーに代わって AWS のサービスによって行われた許可に制限する条件要素を使用します。

> **Note**
>
> WorkSpaces 管理者が を使用して暗号化されたボリューム WorkSpaces で AWS Management Console を作成する場合、管理者にはエイリアスとリストキー (`"kms:ListAliases"` および のアクセス許可) を一覧表示する`"kms:ListKeys"`アクセス許可が必要です。 WorkSpaces 管理者が (コンソールではなく) Amazon WorkSpaces API のみを使用している場合は、 `"kms:ListAliases"`および アクセス`"kms:ListKeys"`許可を省略できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

を暗号化するユーザーまたはロールのIAMポリシーには、カスタマーマネージドKMSキーの使用権限と へのアクセス権限が含まれている WorkSpace 必要があります WorkSpaces。IAM ユーザーまたはロールにアクセス WorkSpaces 許可を付与するには、次のサンプルポリシーをIAMユーザーまたはロールにアタッチします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

ユーザーが AWS KMSを使用するには、次の IAM ポリシーが必要です。これにより、ユーザーにKMSキーへの読み取り専用アクセスと、許可を作成する機能が提供されます。

```
{
    "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キーを有効なキーARN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": "*"
```

```
    }
  ]
}
```

の暗号化 WorkSpace

を暗号化するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. 起動 WorkSpaces を選択し、最初の 3 つのステップを完了します。
3. WorkSpaces 設定ステップでは、次の操作を行います。
   a. 暗号化するボリュームを選択します。[Root Volume]、[User Volume]、または両方のボリュームとなります。
   b. 暗号化キー で、Amazon によって作成された AWS マネージド AWS KMS キー WorkSpaces または作成したKMSキーのいずれかの KMS キーを選択します。選択するKMSキーは対称である必要があります。Amazon WorkSpaces は非対称KMSキーをサポートしていません。
   c. [Next Step] (次のステップ) をクリックします。
4. [Launch] WorkSpaces (起動する) を選択します。

暗号化された を表示する WorkSpaces

WorkSpaces コンソールから暗号化された ボリューム WorkSpaces と ボリュームを確認するには、左側のナビゲーションバーWorkSpacesから を選択します。Volume Encryption 列には、各 WorkSpace で暗号化が有効か無効かが表示されます。暗号化された特定のボリュームを確認するには、 WorkSpace エントリを展開して Encrypted Volumes フィールドを表示します。

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、AWS KMS キーが有効であることを最初に確認します。有効でない場合、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。

WorkSpace を再起動するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [WorkSpaces] を選択します。
3. 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 WorkSpace で を再構築する

を再構築すると、 が起動 WorkSpace されたバンドルの最新のイメージのルートボリューム、そのユーザーボリューム、およびそのプライマリ Elastic Network Interface が WorkSpace 再作成されます。を再構築すると、 を復元するよりも多くのデータが WorkSpace 削除されますが WorkSpace、必要なのはユーザーボリュームのスナップショットのみです。を復元するには WorkSpace、「」を参照してください WorkSpaces Personal WorkSpace で を復元する。

を再構築 WorkSpace すると、次のようになります。

- ルートボリューム (Microsoft Windows の場合はドライブ C、Linux の場合は /) は、 WorkSpace が作成されたバンドルの最新のイメージで更新されます。インストールされたアプリケーション、または WorkSpace の作成後に変更されたシステム設定は失われます。
- ユーザーボリューム (Microsoft Windows の場合は D: ドライブ、Linux の場合は /home) が、最新のスナップショットから再作成されます。ユーザーボリュームの現在の内容は上書きされます。

の再構築時に使用する自動スナップショット WorkSpace は 12 時間ごとにスケジュールされます。ユーザーボリュームのこれらのスナップショットは、 の状態に関係なく作成されます WorkSpace。Actions、Rebuild/Restore WorkSpaceを選択すると、最新のスナップショットの日時が表示されます。

を再構築すると WorkSpace、再構築の完了後すぐに (多くの場合 30 分以内に) 新しいスナップショットも作成されます。

- プライマリ Elastic Network Interface が再作成されます。は新しいプライベート IP アドレス WorkSpace を受け取ります。

> **Important**
>
> 2020 年 1 月 14 日以降、パブリック Windows 7 バンドルから WorkSpaces 作成された は再構築できなくなります。Windows 7 から Windows 10 WorkSpaces への移行を検討してください。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。

を再構築できるのは、次の条件が満たされた場合 WorkSpace のみです。

- の状態は、AVAILABLE、、ERROR、STOPPED、または UNHEALTHY WorkSpace である必要がありますREBOOTING。 WorkSpace REBOOTING 状態の を再構築するには、 RebuildWorkspacesAPI オペレーションまたは rebuild-workspaces AWS CLI コマンドを使用する必要があります。
- ユーザーボリュームのスナップショットが存在する必要があります。

を再構築するには WorkSpace

> **Warning**
>
> 暗号化された を再構築するには WorkSpace、まず AWS KMS キーが有効になっていることを確認します。有効でない場合、 WorkSpace は使用できなくなります。KMS キーが有効になっているかどうかを確認するには、「 AWS Key Management Service デベロッパーガイド」のKMS「キーの詳細の表示」を参照してください。

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

2. ナビゲーションペインで、WorkSpaces を選択します。
3. 再構築 WorkSpace する を選択し、アクション、再構築/復元 WorkSpaceを選択します。
4. [Snapshot] (スナップショット) で、スナップショットのタイムスタンプを選択します。
5. [Rebuild] を選択します。

WorkSpace を使用して を再構築するには AWS CLI

rebuild-workspaces コマンドを使用します。

トラブルシューティング

Active Directory でユーザーsAMAccountの名前ユーザー命名属性を変更 WorkSpace した後に を再構築すると、次のエラーメッセージが表示されることがあります。

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

この問題を回避するには、元のユーザーの命名属性に戻ってから再構築を再開するか、 WorkSpace そのユーザーの新しい を作成します。

Microsoft Entra ID 参加の再構築 WorkSpaces

再構築後にユーザーが WorkSpace 初めて にログインするときは、新しい が割り当てられたときと同様に、エクスペリエンス (OOBE) を再度実行 out-of-boxする必要があります WorkSpace。その結果、新しいユーザープロファイルフォルダが に作成され WorkSpace、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、結合された Entra の再構築中 WorkSpace、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 `D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>` の に保存されます WorkSpace。ユーザーは、デスクトップアイコン`D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>`、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ために、元のプロファイルコンテンツを から D:\Users\<USERNAME> のユーザーのプロファイルフォルダにコピーする必要があります。

> **Note**
>
> Microsoft Entra ID に参加している場合は WorkSpaces、可能な限り WorkSpaces、再構築ではなく復元を使用することをお勧めします WorkSpaces。

WorkSpaces Personal WorkSpace で を復元する

を復元すると、 が正常 WorkSpace であったときに作成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 WorkSpace が再作成されます。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 WorkSpace ロールバックされます。を再構築すると、ユーザーボリューム上のデータ WorkSpace のみがロールバックされます。つまり、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ですが、 を再構築するにはユーザーボリュームのスナップショット WorkSpace のみが必要です。を再構築するには WorkSpace、「」を参照してください WorkSpaces Personal WorkSpace で を再構築する。

を復元すると WorkSpace 、次のようになります。

- ルートボリューム (Microsoft Windows の場合はドライブ C、Linux の場合は /) は、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

Actions と Rebuild/Restore WorkSpaceを選択すると、オペレーションに使用されたスナップショットの日時が表示されます。を使用してオペレーションに使用されたスナップショットの日時を確認するには AWS CLI、 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 WorkSpace は、 の作成後すぐに (多くの場合 30 分以内に) 作成されます。 AWS リージョンによっては、 WorkSpace の作成後に最初のスナップショットを取得するの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 が異常 WorkSpace 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、 の再構築 WorkSpaceを試みるか、 サポートにお問い合わせください AWS 。

- 通常の使用中 — の復元時に使用する自動スナップショット WorkSpace は 12 時間ごとにスケジュールされます。 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 に異常がある場合、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 の復元後 — を復元すると WorkSpace、復元が完了した直後に新しいスナップショットが作成されます (多くの場合 30 分以内) 。 AWS リージョンによっては、 WorkSpace が復元された後にこれらのスナップショットを作成するのに数時間かかる場合があります。

  WorkSpace が復元された後、新しいスナップショットを作成する前に が異常 WorkSpace になった場合、 を再度復元 WorkSpace することはできません。その場合は、 の再構築 WorkSpaceを試みるか、 AWS サポートにお問い合わせください。

を復元できるのは、次の条件が満たされた場合 WorkSpace のみです。

- の状態は、AVAILABLE、、UNHEALTHY、または ERROR WorkSpace である必要がありますSTOPPED。
- 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。

を復元するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. 復元 WorkSpace する を選択し、アクション、再構築/復元 WorkSpaceを選択します。
4. [Snapshot] (スナップショット) で、スナップショットのタイムスタンプを選択します。
5. [復元] を選択します。

WorkSpace を使用して を復元するには AWS CLI

restore-workspace コマンドを使用します。

Microsoft 365 Bring Your Own License (BYOL) in WorkSpaces Personal

Amazon WorkSpaces では、Microsoft のライセンス要件を満たしている場合、独自の Microsoft 365 ライセンスを持ち込むことができます。これらのライセンスにより、以下のオペレーティングシステム WorkSpaces を搭載したエンタープライズソフトウェア用の Microsoft 365 Apps を にインストールしてアクティブ化できます。

- Windows 10 (Bring Your Own License)
- Windows 11 (Bring Your Own License)
- Windows Server 2016
- [Windows Server 2019]
- Windows Server 2022

Microsoft 365 Apps for enterprise on を使用するには WorkSpaces、Microsoft 365 E3/E5, Microsoft 365 A3/A5, Microsoft 365 G3/G5 または Microsoft 365 Business Premium へのサブスクリプションが必要です。

Amazon WorkSpaces では、Microsoft 365 ライセンスを使用して、以下を含む Microsoft 365 Apps for enterprise をインストールしてアクティブ化できます。

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

詳細については、Microsoft 365 Apps for enterprise の詳細なリストを参照してください。

Microsoft Project、Microsoft Visio、Microsoft Power Automate など、Microsoft 365 に含まれていない Microsoft アプリケーションも にインストールできます WorkSpaces が、独自の追加ライセンスを持ち込みます。

WorkSpaces マルチリージョンレジリエンスを使用して、プライマリ WorkSpaces およびフェイルオーバーで Microsoft 365 およびその他の Microsoft アプリケーションをインストールして使用できます。

内容

- Microsoft 365 Apps for enterprise WorkSpaces で を作成する
- Microsoft 365 Apps for Enterprise を使用する WorkSpaces ように既存の を移行する
- で Microsoft 365 Apps for enterprise を更新する WorkSpaces

Microsoft 365 Apps for enterprise WorkSpaces で を作成する

Microsoft 365 Apps for enterprise WorkSpaces で を作成するには、アプリケーションがインストールされたカスタムイメージを作成し、それを使用してカスタムバンドルを作成する必要があります。バンドルを使用して、 WorkSpaces アプリケーションがインストールされている新しい を起動できます。 は、Microsoft WorkSpaces 365 Apps for enterprise でパブリックバンドルを提供しません。

Microsoft 365 Apps for enterprise WorkSpaces で を作成するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. 他の Microsoft アプリケーションのイメージ WorkSpace として使用する を起動します WorkSpaces。ここに Microsoft アプリケーションをインストールします。の起動の詳細については WorkSpace、「 を使用して仮想デスクトップを起動 WorkSpacesする」を参照してください。
3. https://clients.amazonworkspaces.com/ でクライアントアプリケーションを起動し、招待メールの登録コードを入力して、登録を選択します。
4. サインインするように求められたら、ユーザーのサインイン認証情報を入力し、[Sign In] (サインイン) を選択します。
5. Microsoft 365 Apps for enterprise をインストールして設定します。
6. からカスタムイメージを作成し WorkSpace、それを使用してカスタムバンドルを作成します。カスタムイメージとバンドルの作成の詳細については、「カスタム WorkSpaces イメージとバンドルの作成」を参照してください。
7. 作成したカスタムバンドル WorkSpaces を使用して を起動します。これら WorkSpaces には Microsoft 365 Apps for enterprise がインストールされています。

Microsoft 365 Apps for Enterprise を使用する WorkSpaces ように既存の を移行する

で Microsoft Office ライセンス WorkSpaces がない場合は AWS、 に Microsoft 365 Apps for enterprise をインストールして設定できます WorkSpaces。

で Microsoft Office ライセンス WorkSpaces をお持ちの場合は AWS、エンタープライズ用 Microsoft 365 アプリ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

から Microsoft Office アプリケーションをアンインストールしても、ライセンスは登録解除 WorkSpaces されません。Microsoft Office ライセンスの料金が発生しないようにするには、次のいずれかを実行して AWS 、 から Microsoft Office アプリケーション WorkSpaces から を登録解除します。

- アプリケーションの管理 (推奨) – Microsoft Office 2016 および 2019 を からアンインストールできます WorkSpaces。詳細については、「アプリケーションの管理」を参照してください。アンインストールしたら、 に Microsoft 365 Apps for enterprise をインストールできます WorkSpaces。
- の移行 WorkSpace – ユーザーボリュームにデータを保持しながら、あるバンドル WorkSpace から別のバンドルに を移行できます。
  - Microsoft Office サブスクリプションがないイメージを含むバンドル WorkSpaces に を移行します。移行が完了したら、 に Microsoft 365 Apps for enterprise をインストールできます WorkSpaces。
  - または、Microsoft 365 Apps for enterprise がすでにインストールされているカスタムイメージ WorkSpaces とバンドルを作成し、 WorkSpaces をこの新しいカスタムバンドルに移行します。移行が完了すると、 WorkSpaces ユーザーは Microsoft 365 Apps for enterprise の使用を開始できます。
  - 移行方法の詳細については WorkSpaces、「 の移行 WorkSpace」を参照してください。

で Microsoft 365 Apps for enterprise を更新する WorkSpaces

デフォルトでは、Microsoft Windows オペレーティングシステムで WorkSpaces 実行されているは、Windows Update から更新を受け取るように設定されています。ただし、Microsoft 365 Apps for enterprise の更新プログラムは Windows Update ではご利用いただけません。Office から自動的に実行されるように更新を設定するかCDN、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 アプリケーション更新の頻度を設定するには、更新チャネルを指定し、ライセンスポリシーの WorkSpaces Microsoft 365 に準拠するように Current または Monthly Enterprise 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
- 考慮事項
- 既知の制限事項
- レジストリキー設定の概要
- インプレースアップグレードの実行
- トラブルシューティング
- PowerShell スクリプトを使用して WorkSpace レジストリを更新する

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

レジストリキー	タイプ	値
		1 – インプレースアップグレードを有効にする
PostUpgradeRestoreProfileOnD	DWORD	0 – (デフォルト) インプレースアップグレード後にユーザープロファイルパスの復元を試みない 1 – インプレースアップグレード後にユーザープロファイルパス (ProfileImagePath) を復元する
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 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 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) AWS PV ドライバーの更新を無効にする 1 – AWS PV ドライバーの更新を有効にする

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
    }
}
```

Personal WorkSpace で を移行する WorkSpaces

> **Note**
>
> から を通じて AWS Microsoft Office バージョンライセンスのサブスクリプションを解除またはアンインストールする場合は WorkSpace、アプリケーションを管理するを使用することをお勧めします。

ユーザーボリュームにデータを保持しながら、あるバンドル WorkSpace から別のバンドルに を移行できます。サンプルシナリオを以下に示します。

- Windows 7 デスクトップエクスペリエンス WorkSpaces から Windows 10 デスクトップエクスペリエンスに移行できます。
- PCoIP プロトコル WorkSpaces から に移行できますDCV。
- Windows Server 2016 搭載バンドルの 32 ビット Microsoft Office WorkSpaces から Windows Server 2019 WorkSpaces および Windows Server 2022 搭載 WorkSpaces バンドルの 64 ビット Microsoft Office に移行できます。
- 1 つのパブリックバンドルまたはカスタムバンドル WorkSpaces から別のバンドルに移行できます。例えば、 GPU対応 (Graphics.g4dn. GraphicsPro.g4dn、Graphics、 GraphicsPro) バンドルからバンドルに移行 non-GPU-enabledしたり、逆方向に移行したりできます。
- Windows 10 WorkSpaces から Windows 11 に移行することはできますBYOLがBYOL、Windows 11 から Windows 10 への移行はサポートされていません。
- バリューバンドルは Windows 11 ではサポートされていません。Windows 7 または 10 の値バンドル WorkSpaces を Windows 11 に移行するには、まず値 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。
- Windows 7 WorkSpaces から Windows 11 に移行する前に、Windows 10 に移行する必要があります。Windows 11 に移行する前に WorkSpace 、Windows 10 に少なくとも 1 回ログインします。Windows 7 から Windows 11 への WorkSpaces 直接移行はサポートされていません。
- Microsoft Office WorkSpaces を使用する Windows AWS は、 を介して Microsoft 365 アプリケーションのカスタム WorkSpaces バンドルに移行できます。移行後、 WorkSpaces は Microsoft Office からサブスクリプション解除されます。
- Microsoft Office WorkSpaces を使用する Windows を、Office 2016/2019 サブスクリプションのないバンドル AWS に移行 WorkSpaces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。
- Windows 10 BYOLBYOP WorkSpaces から Windows 11 に移行し、Windows Server 2019 BYOP WorkSpaces から Windows Server 2022 にライセンス込みで移行できます。

Amazon WorkSpaces バンドルの詳細については、「」を参照してください WorkSpaces Personal のバンドルとイメージ。

移行プロセス WorkSpace では、ターゲットバンドルイメージの新しいルートボリュームと、元の の最後に使用可能なスナップショットのユーザーボリュームを使用して、 を再作成します WorkSpace。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、1 つにつき最大 1 時間かかります WorkSpace。移行プロセスを開始すると、新しい WorkSpace が作成されます。移行が成功しないエラーが発生すると、元の WorkSpace が復元されて元の状態に戻され、新しい WorkSpace は終了します。

目次

- 移行の制限
- 移行シナリオ
- 移行中の動作
- ベストプラクティス
- トラブルシューティング
- 請求への影響
- の移行 WorkSpace

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。Bring Your Own License (BYOL) Windows 7 バンドルに移行することもできません。
- 他のBYOLバンドルBYOL WorkSpaces にのみ移行できます。を BYOL WorkSpace から PCoIP に移行するにはDCV、まず 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、 PCoIPBYOL WorkSpaces をそのDCVBYOLバンドルに移行できます。
- WorkSpace 作成した をパブリックバンドルまたはカスタムバンドルからBYOLバンドルに移行することはできません。
- Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および 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 と GraphicsPro.g4dn は、Windows および Ubuntu の DCVプロトコルで使用できます。グラフィック と GraphicsPro WorkSpaces DCVはまだ に移行できません。
- Linux の移行 WorkSpaces は現在サポートされていません。
- 複数の言語をサポートする AWS リージョンでは、言語バンドル間で移行 WorkSpacesできます。

- ソースバンドルとターゲットバンドルは異なっている必要があります (ただし、複数の言語をサポートするリージョンでは、言語が異なる限り、同じ Windows 10 バンドルに移行できます)。同じバンドル WorkSpace を使用して を更新する場合は、代わりに を再構築します WorkSpace。
- リージョン WorkSpaces 間で移行することはできません。
- 場合によっては、移行が正常に完了しない場合、エラーメッセージが表示されず、移行プロセスが開始されなかったように見えることがあります。移行を試みてから 1 時間後に WorkSpace バンドルが同じままである場合、移行は失敗します。AWS Support センターにアクセスしてサポートをお求めください。
- PCoIP または BYOP WorkSpaces に移行することはできませんDCV WorkSpaces。

移行シナリオ

次の表に、可能な移行シナリオを示します。

移行元 OS	移行先 OS	使用可能
パブリックまたはカスタムバンドル Windows 7	パブリックまたはカスタムバンドル Windows 10	はい
カスタムバンドル Windows 7	パブリックバンドル Windows 7	いいえ
カスタムバンドル Windows 7	カスタムバンドル Windows 7	いいえ
パブリックバンドル Windows 7	カスタムバンドル Windows 7	いいえ
パブリックまたはカスタムバンドル Windows 10	パブリックまたはカスタムバンドル Windows 7	いいえ
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	あり
Windows 7 BYOLバンドル	Windows 7 BYOLバンドル	いいえ
Windows 7 BYOLバンドル	Windows 10 BYOLバンドル	あり
Windows 10 BYOLバンドル	Windows 7 BYOLバンドル	いいえ

移行元 OS	移行先 OS	使用可能
Windows 10 BYOLバンドル	Windows 10 BYOLバンドル	あり
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 	あり
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	あり
Windows 10 BYOLバンドル	Windows 11 BYOLバンドル	あり
Windows 11 BYOLバンドル	Windows 10 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	あり
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	あり
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	あり
Windows 10 BYOP BYOL	Windows 11 BYOP BYOL	あり
Windows 11 BYOP BYOL	Windows 10 BYOP BYOL	いいえ

移行元 OS	移行先 OS	使用可能
Windows Server 2019 搭載パブリック BYOP	Windows Server 2022 搭載パブリック BYOP	あり
Windows Server 2022 搭載パブリック BYOP	Windows Server 2019 搭載パブリック BYOP	いいえ

> **Note**
>
> ウェブアクセスは、Windows Server 2019 搭載のパブリック Windows 10 バンドルPCoIPブランチでは使用できません。

> **Important**
>
> Windows Server 2016 搭載のパブリック Windows 10 プラスバンドルには、Microsoft Office 2016 と Trend Micro Worry-Free Business Security Services が含まれています。Windows Server 2019 搭載のパブリック Windows 10 プラスバンドルには、Microsoft Office 2019 のみが含まれ、Trend Micro Services は含まれません。

移行中の動作

移行中は、ユーザーボリューム (ドライブ D) 上のデータは保持されますが、ルートボリューム (ドライブ C) 上のすべてのデータは失われます。つまり、インストールされているアプリケーション、設定、およびレジストリの変更は、いずれも保持されません。古いユーザープロファイルフォルダの名前が `.NotMigrated` サフィックスで変更され、新しいユーザープロファイルが作成されます。

移行プロセスでは、元のユーザーボリュームの最後のスナップショットに基づいてドライブ D が再作成されます。新しい の最初の起動時に WorkSpace、移行プロセスによって元の`D:\Users\%USERNAME%`フォルダが という名前のフォルダに移動されます`D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`。新しい OS によって新しい `D:\Users\%USERNAME%\` フォルダが生成されます。

新しいユーザープロファイルが作成されると、次のユーザーシェルフォルダ内のファイルが古い `.NotMigrated` プロファイルから新しいプロファイルに移動します。

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

> **Important**
>
> 移行プロセスでは、古いユーザープロファイルから新しいプロファイルへのファイルの移動が試みられます。移行中に移動されなかったファイルは、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダ内に残ります。移行が成功すると、どのファイルが移動されたかを C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs で確認できます。自動的に移動されなかったファイルは、手動で移動できます。
>
> デフォルトでは、パブリックバンドルではローカル検索インデックス作成が無効になっています。有効にすると、デフォルトでは C:\Users ではなく D:\Users を検索する設定となるため、それも調整する必要があります。ローカル検索インデックス作成を D:\Users*username* に設定し、D:\Users に設定していない場合、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダ内のユーザーファイルの移行後にローカル検索インデックス作成が機能しないことがあります。

元の に割り当てられたタグ WorkSpace は移行中に引き継がれ、 の実行モード WorkSpace は保持されます。ただし、新しい は新しい WorkSpace ID、コンピュータ名、および IP アドレス WorkSpace を取得します。

ベストプラクティス

を移行する前に WorkSpace、次の操作を行います。

- ドライブ C の重要なデータを別の場所にバックアップします。ドライブ C 上のすべてのデータは、移行中に消去されます。
- ユーザーボリュームのスナップショットが作成されていることを確認するには、移行 WorkSpace する が少なくとも 12 時間経過していることを確認します。Amazon WorkSpaces コンソールの移

行 WorkSpacesページで、最後のスナップショットの時刻を確認できます。最後のスナップショット以降に作成されたデータは、移行中に失われます。

- 潜在的なデータ損失を回避するには、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ないようにしてください。モードの場合、 は移行 WorkSpaces できないことに注意してくださいADMIN_MAINTENANCE。
- 移行 WorkSpaces する のステータスが AVAILABLE、STOPPED、または であることを確認しますERROR。
- 移行 WorkSpaces する に十分な IP アドレスがあることを確認してください。移行中、 に新しい IP アドレスが割り当てられます WorkSpaces。
- スクリプトを使用して移行する場合は WorkSpaces、 WorkSpaces 一度に 25 個以下のバッチで移行します。

トラブルシューティング

- 移行後にファイルが見つからないことについてユーザーから報告があった場合は、移行プロセス中にユーザープロファイルファイルが移動されなかったかどうかを確認します。どのファイルが移動されたかは、C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs で確認できます。移動されなかったファイルは、D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated フォルダに配置されます。自動的に移動されなかったファイルは、手動で移動できます。
- を使用してAPI移行 WorkSpaces し、移行が成功しない場合、 によって返されるターゲット WorkSpace ID API は使用されず、 WorkSpaceには元の WorkSpace ID が残ります。
- 移行が正常に完了しない場合は、Active Directory で、適切にクリーンアップされたかどうかを確認します。不要 WorkSpaces になった を手動で削除する必要がある場合があります。

請求への影響

移行が発生した月には、新しい と元の の両方に対して日割り計算された金額が請求されます WorkSpaces。例えば、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 日の間は WorkSpace A に対して課金され、5 月 11 日から 5 月 30 日の間は WorkSpace B に対して課金されます。

> **Note**
>
> WorkSpace を別のバンドルタイプ (パフォーマンスからパワー、値からスタンダードなど) に移行する場合、移行プロセス中にルートボリューム (ドライブ C) とユーザーボリューム

(ドライブ D) のサイズが増加する可能性があります。必要に応じて、ルートボリュームは、新しいバンドルのデフォルトのルートボリュームサイズに合わせて増加します。ただし、ユーザーボリュームに対して、元のバンドルのデフォルトとは異なるサイズ (高いサイズまたは低いサイズ) をすでに指定していた場合、移行プロセス中も同じユーザーボリュームサイズが保持されます。それ以外の場合、移行プロセスでは、新しいバンドルのソース WorkSpace ユーザーボリュームサイズとデフォルトのユーザーボリュームサイズのうち大きい方が使用されます。

の移行 WorkSpace

Amazon WorkSpaces コンソール、、 AWS CLI または Amazon WorkSpaces WorkSpaces から移行できますAPI。

を移行するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. を選択し WorkSpace 、アクション、移行 WorkSpacesを選択します。
4. バンドルで、 を移行するバンドルを選択します WorkSpace 。

   > **Note**
   >
   > を BYOL WorkSpace から PCoIP に移行するにはDCV、まず 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、 PCoIPBYOL WorkSpaces をそのDCVBYOLバンドルに移行できます。

5. 移行 WorkSpaces を選択します。

   ステータス WorkSpace が の新しい `PENDING`が Amazon WorkSpaces コンソールに表示されます。移行が完了すると、元の WorkSpace は終了し、新しい のステータス WorkSpace は に設定されます`AVAILABLE`。

6. (オプション) 不要になったカスタムバンドルとイメージを削除する方法については、WorkSpaces 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 を通じて移行するには AWS CLI、migrate-workspace コマンドを使用します。Amazon WorkSpaces 経由で移行するには WorkSpaces API、「Amazon リファレンス」のMigrateWorkSpace「」を参照してください。 WorkSpaces API

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 の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/ 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 の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、ソフトウェアリソースの組み合わせです。を起動するときは WorkSpace、ニーズに合ったバンドルを選択します。で使用できるデフォルトのバンドル WorkSpaces は、パブリックバンドルと呼ばれます。で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。

Windows または Linux を起動 WorkSpace し、カスタマイズした場合は、そこからカスタムイメージを作成できます WorkSpace。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

カスタムイメージを作成したら、カスタム WorkSpace イメージと、選択した基盤となるコンピューティングおよびストレージ設定を組み合わせたカスタムバンドルを構築できます。その後、新しいを起動するときにこのカスタムバンドルを指定 WorkSpaces して、新しい の設定 (ハードウェアとソフトウェア) WorkSpaces が一貫していることを確認できます。

ソフトウェア更新を実行したり、 に追加のソフトウェアをインストールしたりする必要がある場合は WorkSpaces、カスタムバンドルを更新して を再構築できます WorkSpaces。

WorkSpaces は、いくつか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, PCoIP	Value、Standard、Performance、Power PowerPro、Graphics (廃止) GraphicsPro、Graphics.g4dn、 GraphicsPro.g4dn	2027 年 1 月 12 日
[Windows Server 2019]	含まれる	DCV, PCoIP	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, PCoIP	Standard、Performance、Power PowerPro、Graphics (廃止) GraphicsPro、Graphics.g4dn、 GraphicsPro.g4dn	2031 年 10 月 14 日
Windows 10	Bring Your Own License (BYOL)	DCV, PCoIP	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	サポート中

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
Amazon Linux 2	含まれる	DCV, PCoIP	Value、Standard、Performance、Power、 PowerPro	2025 年 6 月 30 日
Ubuntu 22.04 LTS	含まれる	DCV	Value、Standard、Performance、Power PowerPro、Graphics.g4dn、 GraphicsPro.g4dn	2032 年 6 月
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 サポートによってもサポートされません。
- Windows オペレーティングシステムで WorkSpaces 実行されている場合、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
- WorkSpaces Personal 用のカスタム WorkSpaces イメージとバンドルを作成する
- 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

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プロトコル、オペレーティングシステム、ネットワーク、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てください。プロトコルの詳細については、「Amazon のプロトコル WorkSpaces」を参照してください。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

- では、最大ネットワークレイテンシー 250 PCoIP ミリ秒を超えないことをお勧めします WorkSpaces。最適なPCoIP WorkSpaces ユーザーエクスペリエンスを得るには、ネットワークレイテンシーを 100 ミリ秒未満に維持す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。最適なDCVユーザーエクスペリエンスを得るには、 を 250 ミリ秒RTT未満に維持することをお勧めします。RTT が 250 ミリ秒から 400 ミリ秒の間であれば、ユーザーは にアクセスできますが WorkSpace、パフォーマンスは大幅に低下します。
- 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 が提供するBYOPバンドルには、 WorkSpaces 提供されたストリーミングプロトコルがインストールされ WorkSpaces 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 end-of-life 2025 年 10 月 31 日に終了します。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、「Personal WorkSpace で を移行する WorkSpaces 」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 WorkSpaces を使用するには、Graphics.g4dn バンドルに切り替えることをお勧めします。
- グラフィックスと 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を次に示します。のバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。

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。

GraphicsPro バンドル

このバンドルは、ベースラインレベルのグラフィックスパフォーマンスと、 の高レベルのCPUパフォーマンスとメモリを提供します WorkSpaces。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、実写のようなリアルなデザインにはお勧めしません。

Graphics.g4dn バンドル

このバンドルは、高レベルのグラフィックスパフォーマンスと、 用の中レベルのCPUパフォーマンスとメモリを提供し WorkSpaces 、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
- 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 (computer-aided design/computer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、 に高レベルのグラフィックスパフォーマンス、CPUパフォーマンス、メモリを提供し、以下 WorkSpaces に適しています。

- 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 (computer-aided design/computer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 用のカスタム WorkSpaces イメージとバンドルを作成する

Windows または Linux を起動 WorkSpace してカスタマイズした場合は、そこからカスタムイメージとカスタムバンドルを作成できます WorkSpace。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

> **Note**
>
> バンドルを削除し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 を起動するときにこのカスタムバンドルを指定 WorkSpaces して、新しい の設定 (ハードウェアとソフトウェア) WorkSpaces が一貫していることを確認できます。

バンドルごとに異なるコンピューティングオプションとストレージオプションを選択することで、同じカスタムイメージを使用してさまざまなカスタムバンドルを作成できます。

> **Important**
>
> - Windows 10 からイメージを作成する場合は WorkSpace、あるバージョンの Windows 10 から新しいバージョンの Windows 10 (Windows の機能/バージョンのアップグレード) に

アップグレードされた Windows 10 システムでは、イメージの作成はサポートされていないことに注意してください。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、 WorkSpaces イメージ作成プロセスでサポートされています。

- 2020 年 1 月 14 日以降、パブリック Windows 7 バンドルからイメージを作成することはできません。Windows 7 から Windows 10 WorkSpaces への移行を検討してください。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。
- 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。 WorkSpaces を Graphics.g4dn バンドルに移行することをお勧めします。詳細については、「Personal WorkSpace で を移行する WorkSpaces 」を参照してください。
- GraphicsPro バンドルは end-of-life 2025 年 10 月 31 日に終了します。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、「the section called “の移行 WorkSpace”」を参照してください。
- グラフィックスと 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 料金表」を参照してください。

内容

- Windows カスタムイメージを作成するための要件
- Linux カスタムイメージを作成するための要件
- ベストプラクティス
- (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
- ステップ 2: Image Checker を実行する
- ステップ 3: カスタムイメージとカスタムバンドルを作成する
- Windows WorkSpaces カスタムイメージに含まれているもの
- Linux WorkSpace カスタムイメージに含まれているもの

Windows カスタムイメージを作成するための要件

> **Note**
>
> 現在、Windows では 1 GB を 1,073,741,824 バイトと定義しています。のイメージを作成するには、C ドライブで 12,884,901,888 バイト (または 12 GiB) を超える空きがあり、ユーザープロファイルが 10,737,418,240 バイト (または 10 GiB) 未満であることを確認する必要があります WorkSpace。

- のステータスは Available WorkSpace で、変更ステータスは None である必要があります。
- WorkSpaces イメージ上のすべてのアプリケーションとユーザープロファイルは、Microsoft Sysprep と互換性がある必要があります。
- イメージに含めるすべてのアプリケーションは、C ドライブにインストールする必要があります。
- Windows 7 の場合 WorkSpaces、 とその合計サイズ (ファイルとデータ) は 10 GB 未満である必要があります。
- Windows 7 の場合 WorkSpaces、Cドライブには少なくとも 12 GB の空き容量が必要です。
- で実行されているすべてのアプリケーションサービスは、ドメインユーザー認証情報の代わりにローカルシステムアカウント WorkSpace を使用する必要があります。たとえば、Microsoft SQL Server Express のインストールをドメインユーザーの認証情報で実行することはできません。
- は暗号化 WorkSpace しないでください。暗号化された からのイメージの作成 WorkSpace は現在サポートされていません。
- 以下のコンポーネントがイメージに必要です。これらのコンポーネントがないと、イメージから起動 WorkSpaces する が正しく機能しません。詳細については、「the section called “必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 エージェントとドライバー
  - STXHD エージェントとドライバー
  - AWS および WorkSpaces 証明書
  - Skylight エージェント

Linux カスタムイメージを作成するための要件

- のステータスは Available WorkSpace で、変更ステータスは None である必要があります。
- イメージに含めるすべてのアプリケーションは、ユーザーボリューム (/home ディレクトリ) の外にインストールする必要があります。
- ルートボリューム (/) の使用率は 97% 未満である必要があります。
- は暗号化 WorkSpace しないでください。暗号化された からのイメージの作成 WorkSpace は現在サポートされていません。
- 以下のコンポーネントがイメージに必要です。これらのコンポーネントがないと、イメージから起動 WorkSpaces した が正しく機能しません。
  - Cloud-init
  - Teradici PCoIPまたはDCVエージェントとドライバー
  - Skylight エージェント

ベストプラクティス

からイメージを作成する前に WorkSpace、次の操作を行います。

- 本番環境に接続VPCされていない別の を使用します。
- プライベートサブネット WorkSpace に をデプロイし、アウトバウンドトラフィックにNATインスタンスを使用します。
- 小さい Simple AD ディレクトリを使用します。
- ソースの最小ボリュームサイズを使用し WorkSpace、カスタムバンドルを作成するときに必要に応じてボリュームサイズを調整します。
- すべてのオペレーティングシステムの更新 (Windows 機能/バージョンの更新を除く) とすべてのアプリケーションの更新を にインストールします WorkSpace。詳細については、このトピックの冒頭にある「重要な注意点」を参照してください。
- バンドルに含めるべきではないキャッシュされたデータ (ブラウザ履歴、キャッシュファイル、ブラウザ Cookie など) WorkSpace を から削除します。
- バンドルに含めるべきではない から設定を削除します (E WorkSpace メールプロファイルなど)。
- を使用して動的 IP アドレス設定に切り替えますDHCP。
- リージョンで許可されている WorkSpace イメージのクォータを超えていないことを確認してください。デフォルトでは、リージョンごとに 40 個の WorkSpace イメージが許可されます。この

クォータに達した場合、新しいイメージを作成しようとすると失敗します。クォータの引き上げをリクエストするには、WorkSpaces の制限フォームを使用します。

- 暗号化された からイメージを作成しようとしていないことを確認します WorkSpace。暗号化された からのイメージの作成 WorkSpace は現在サポートされていません。
- でウイルス対策ソフトウェアを実行している場合は WorkSpace、イメージの作成中に無効にします。
- でファイアウォールが有効になっている場合は WorkSpace、必要なポートがブロックされていないことを確認してください。詳細については、「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 の場合 WorkSpaces、イメージの作成前にグループポリシーオブジェクト (GPOs) を設定しないでください。
- Windows の場合は WorkSpaces、イメージを作成する前にデフォルトのユーザープロファイル (`C:\Users\Default`) をカスタマイズしないでください。を使用してユーザープロファイルをカスタマイズしGPOs、イメージの作成後に適用することをお勧めします。 は簡単に変更またはロールバックGPOsできるため、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 の場合は WorkSpaces、ホワイトペーパー「Amazon for Linux イメージを準備するためのベストプラクティス WorkSpaces 」も参照してください。
- Linux で DCV を有効に WorkSpaces してスマートカードを使用する場合は、イメージを作成する WorkSpace 前に Linux に対して行う必要があるカスタマイズ WorkSpaces Personal での認証にスマートカードを使用するについて、「」を参照してください。
- 、ENA、および PV ドライバーなどのネットワーク依存関係ドライバーはNVMe、必ず で更新してください WorkSpaces。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、「Windows インスタンス用の Elastic Network Adapter (ENA) ドライバー をインストールまたはアップグレードする」および「Windows インスタンスでの PV ドライバーのアップグレード」を参照してください。 AWS NVMe ドライバー
- EC2Config、EC2Launch、および EC2Launch V2 エージェントは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と の更新EC2Launch」を参照してください。

(オプション) ステップ 1: イメージのカスタムコンピュータ名の形式を指定する

カスタムイメージまたは Bring-Your-Own-License (BYOL) イメージから WorkSpaces 起動した では、デフォルトのコンピュータ名形式を使用する代わりに、コンピュータ名形式にカスタムプレ

フィックスを指定できます。カスタムプレフィックスを指定するには、イメージタイプに応じた適切な手順に従います。

カスタムイメージのカスタムコンピュータ名の形式を指定するには

> **Note**
>
> デフォルトでは、Windows 10 のコンピュータ名の形式 WorkSpaces は DESKTOP-XXXXXで WorkSpaces、Windows 11 のコンピュータ名の形式は ですWORKSPA-XXXXX。

1. カスタムイメージの作成に WorkSpace 使用している で、メモ帳または別のテキストエディタC:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xmlで を開きます。Unattend.xml ファイルの操作の詳細については、Microsoft のドキュメントの「応答ファイル (unattend.xml)」をご参照ください。

   > **Note**
   >
   > の Windows File Explorer から C: ドライブにアクセスするには WorkSpace、アドレスバー**C:**に と入力します。

2. <settings pass="specialize"> セクションで、<ComputerName> がアスタリスク (*) に設定されていることを確認します。<ComputerName> が他の値に設定されている場合、カスタムコンピュータ名の設定は無視されます。<ComputerName> 設定の詳細については、Microsoft ドキュメントの ComputerName「」を参照してください。
3. <settings pass="specialize"> セクションで、<RegisteredOrganization> および <RegisteredOwner> を任意の値に設定します。

   Sysprep では、<RegisteredOwner> および <RegisteredOrganization> に指定した値が連結され、結合された文字列の最初の 7 文字を使用してコンピュータ名が作成されます。例えば、<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 WorkSpaces を使用する のコンピュータ名は EC2AMAZ- で始まります*xxxxxxx*。Windows 11 ベースのイメージの場合、カスタムバンドル WorkSpaces を使用する のコンピュータ名は WORKSPA- で始まります*xxxxxxx*。

> **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> の両方が必須値です。

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 ドキュメントの ComputerName「」を参照してください。
3. <settings pass="specialize"> セクションには、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。たとえば、 **Amazon.com**に <RegisteredOrganization>を指定し、 **EC2**に を指定した場合<RegisteredOwner>、カスタムバンドルから WorkSpaces 作成された のコンピュータ名は EC2AMAZ- で始まります*xxxxxxx*。

> **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> の両方が必須値です。

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 でのみ使用できます WorkSpaces。Linux からイメージを作成する場合は WorkSpace、「」に進みますステップ 3: カスタムイメージとカスタムバンドルを作成する。

Windows がイメージ作成の要件を満た WorkSpace していることを確認するには、Image Checker を実行することをお勧めします。Image Checker は、イメージの作成 WorkSpace に使用する で一連のテストを実行し、見つかっ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**
>
> - は、イメージの作成に使用する前に、Image Checker によって実行されるすべてのテストに合格 WorkSpace する必要があります。
> - Image Checker を実行する前に、最新の Windows セキュリティ更新プログラムと累積更新プログラムが にインストールされていることを確認します WorkSpace。

Image Checker を入手するには、以下のいずれかを実行します。

- を再起動します WorkSpace。Image Checker は再起動時に自動的にダウンロードされ、C:\Program Files\Amazon\ImageChecker.exe にインストールされます。

- https://tools.amazonworkspaces.com/ImageChecker.zip 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、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。

   ステータスが のテストではFAILED、Info を選択して、障害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 のステータスが表示された場合はWARNING、すべての警告を修正するボタンを選択します。

   このツールは、Image Checker が配置されているのと同じディレクトリに出力ログファイルを生成します。デフォルトでは、このファイルは C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log にあります。

   > **Tip**
   >
   > このログファイルは削除しないでください。問題が発生した場合、このログファイルはトラブルシューティングに役立つことがあります。

4. 該当する場合は、テストの失敗や警告の原因となる問題を解決し、 がすべてのテストに WorkSpace合格するまで Image Checker を実行するプロセスを繰り返します。イメージを作成する前に、すべての失敗と警告が解決されている必要があります。
5. がすべてのテストに WorkSpace 合格すると、検証成功メッセージが表示されます。これで、カスタムバンドルを作成する準備ができました。

Image Checker によって検出された問題を解決するためのヒント

Image Checker によって検出された問題を解決するための以下のヒントを参照するほか、C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log で Image Checker のログファイルも確認してください。

PowerShell バージョン 3.0 以降がインストールされている必要があります

Microsoft Windows PowerShellの最新バージョンをインストールします。

> **Important**
>
> PowerShell の実行ポリシーは、RemoteSignedスクリプトを許可するように設定 WorkSpace する必要があります。実行ポリシーを確認するには、Get-ExecutionPolicy PowerShell command を実行します。実行ポリシーが無制限または に設定されていない場合はRemoteSigned、Set-ExecutionPolicy –ExecutionPolicy RemoteSigned コマンドを実行して実行ポリシーの値を変更します。RemoteSigned この設定により WorkSpaces、イメージの作成に必要な Amazon でのスクリプトの実行が可能になります。

C および D ドライブのみが存在できる

イメージに使用される には、 Cおよび WorkSpace Dドライブのみ存在できます。仮想ドライブを含め他のすべてのドライブを削除します。

Windows Update による保留中の再起動は検出できない

- Windows を再起動してセキュリティまたは累積更新プログラムのインストールが完了するまで、イメージ作成プロセスは実行できません。Windows を再起動してこれらの更新を適用し、保留中の他の Windows セキュリティまたは累積更新プログラムをインストールする必要がないことを確認します。
- イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows 10 システム (Windows の機能/バージョンのアップグレード) ではサポートされません。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、WorkSpaces イメージ作成プロセスでサポートされています。

Sysprep ファイルは存在する必要があり、空白にすることはできない

Sysprep ファイルに問題がある場合は、 AWS Support センターに連絡して EC2Configまたは の EC2Launch修復を依頼してください。

ユーザープロファイルのサイズは 10 GB 未満であることが必要

Windows 7 の場合 WorkSpaces、ユーザープロファイル (D:\Users*username*) の合計は 10 GB 未満である必要があります。必要に応じてファイルを削除して、ユーザープロファイルのサイズを小さくします。

ドライブ C には十分な空き容量が必要

Windows 7 では WorkSpaces、ドライブ に 12 GB 以上の空き容量が必要ですC。必要に応じてファイルを削除し、ドライブ C の空き容量を増やします。Windows 10 では WorkSpaces、FAILEDメッセージを受信し、ディスク容量が 2GB を超える場合は無視します。

ドメインアカウントで実行できるサービスがない

イメージの作成プロセスを実行するには、ドメインアカウントで 上のサービス WorkSpace を実行することはできません。すべてのサービスがローカルアカウントで実行されている必要があります。

ローカルアカウントでサービスを実行するには

1. C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log を開き、ドメインアカウントで実行されているサービスのリストを見つけます。
2. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
3. [ログオン方法] で、ドメインアカウントで実行されているサービスを探します。([ローカルシステム]、[ローカルサービス]、または [ネットワークサービス] として実行されているサービスは、イメージの作成を妨げません)
4. ドメインアカウントで実行されているサービスを選択し、[操作]、[プロパティ] の順に選択します。
5. [ログオン] タブを開きます。[ログオン方法] で、[ローカルシステムアカウント] を選択します。
6. [OK] を選択します。

を使用するように を設定 WorkSpace する必要があります DHCP

静的 IP アドレスDHCPの代わりに を使用する WorkSpace ように、 ですべてのネットワークアダプタを設定する必要があります。

を使用するようにすべてのネットワークアダプタを設定するには DHCP

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を選択します。
8. [OK] を選択します。
9. 上のすべてのネットワークアダプタに対してこのプロセスを繰り返します WorkSpace。

リモートデスクトップサービスを有効にすることが必要

イメージ作成プロセスでは、リモートデスクトップサービスを有効にする必要があります。

リモートデスクトップサービスを有効にするには

1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[リモートデスクトップサービス] を見つけます。
3. [リモートデスクトップサービス] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] を選択します。

ユーザープロファイルが存在することが必要

イメージの作成 WorkSpace に使用する には、ユーザープロファイル () が必要です`D:\Users\`*`username`*。このテストに失敗した場合は、AWS Support センターにお問い合わせください。

環境変数のパスを適切に設定することが必要

ローカルマシンの環境変数パスに、System32 および Windows のエントリがありません PowerShell。これらのエントリは、[イメージの作成] を実行するために必要です。

環境変数のパスを設定するには

1. Windows の検索ボックスに「**environment variables**」と入力し、[システム環境変数の編集] を選択します。
2. [システムのプロパティ] ダイアログボックスで、[詳細設定] タブを開き、[環境変数] を選択します。
3. [環境変数] ダイアログボックスの [システム変数] で、[パス] エントリを選択し、[編集] を選択します。
4. [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32
   ```
5. もう一度 [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. [OK] を選択します。
7. を再起動します WorkSpace。

> **Tip**
>
> 環境変数のパスに項目が表示される順序が重要です。正しい順序を決定するには、 の環境変数パス WorkSpace を、新しく作成された Windows インスタンス WorkSpace または新しい Windows インスタンスのパスと比較します。

Windows モジュールインストーラーを有効にすることが必要

イメージ作成プロセスでは、Windows モジュールインストーラーサービスを有効にする必要があります。

Windows モジュールインストーラーサービスを有効にするには

1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。

2. [名前] 列で、[Windows モジュールインストーラー] を見つけます。
3. [Windows モジュールインストーラー] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] を選択します。

Amazon SSM Agent を無効にする必要があります

イメージの作成プロセスでは、Amazon SSM エージェントサービスを無効にする必要があります。

Amazon SSM エージェント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 エージェントを見つけます。
3. Amazon SSM エージェントを選択し、アクション、プロパティを選択します。
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] を選択します。

SSL3 およびTLSバージョン 1.2 を有効にする必要があります

Windows 用 SSL/TLS を設定するには、Microsoft Windows ドキュメントの「How to Enable TLS 1.2」を参照してください。

には 1 つのユーザープロファイルしか存在できません WorkSpace

イメージの作成に使用している には WorkSpace 、1 つの WorkSpaces ユーザープロファイル (`D:\Users\`*`username`*) しか使用できません。の目的のユーザーに属さないユーザープロファイルを削除します WorkSpace。

イメージ作成を機能させるには、 に 3 つのユーザープロファイルのみを含める WorkSpace ことができます。

- (`D:\Users\`*`username`*) の対象ユーザーのユーザー WorkSpaceプロファイル
- デフォルトのユーザープロファイル (デフォルトプロファイルとも呼ばれます)
- 管理者ユーザープロファイル

追加のユーザープロファイルがある場合は、Windows コントロールパネルの詳細システムプロパティを使用して削除できます。

ユーザープロファイルを削除するには

1. 詳細システムプロパティにアクセスするには、以下のいずれかを実行します。
   - Windows + Pause Break キーを押し、[コントロールパネル] > [システムとセキュリティ] > [システム]ダイアログボックスの左側のペインで [システムの詳細設定]を選択します。
   - Windows の検索ボックスに「**control panel**」と入力します。コントロールパネルで、[システムとセキュリティ]、[システム] の順に選択し、[コントロールパネル] > [システムとセキュリティ] > [システム] ダイアログボックスの左側のペインで [システムの詳細設定] を選択します。
2. [システムのプロパティ] ダイアログボックスの [詳細設定] タブで、[ユーザープロファイル] の [設定] を選択します。
3. 管理者プロファイル、デフォルトプロファイル、および目的の WorkSpacesユーザーのプロファイル以外のプロファイルが一覧表示されている場合は、その追加プロファイルを選択して削除を選択します。
4. プロファイルを削除するかどうか尋ねられたら、[はい] を選択します。
5. 必要に応じて、ステップ 3 と 4 を繰り返して、 に属していない他のプロファイルを削除します WorkSpace。
6. [OK] を 2 回選択し、コントロールパネルを閉じます。
7. を再起動します WorkSpace。

AppX パッケージがステージング状態になることはない

1 つ以上の AppX パッケージがステージング状態になっています。これにより、イメージの作成中に Sysprep エラーが発生する可能性があります。

ステージングされたすべての AppX パッケージを削除するには

1. Windows の検索ボックスに「**powershell**」と入力します。[管理者として実行] を選択します。
2. 「このアプリがデバイスに変更を加えることを許可しますか?」と尋ねられたら、[はい] を選択します。

3. Windows PowerShell ウィンドウで、次のコマンドを入力してステージングされたすべての AppX パッケージを一覧表示し、それぞれの後に Enter キーを押します。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                ($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                $_.PackageUserInformation -like "*Staged*")
                                }
```

4. 以下のコマンドを入力して、ステージングされたすべての AppX パッケージを削除し、Enter キーを押します。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Image Checker を再度実行します。それでもこのテストに失敗する場合は、以下のコマンドを入力して、すべての AppX パッケージを削除し、それぞれの後に Enter キーを押します。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows が以前のバージョンからアップグレードされていないこと

イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows システム (Windows の機能/バージョンのアップグレード) ではサポートされません。

イメージを作成するには、Windows の機能/バージョンのアップグレードが完了 WorkSpace していない を使用します。

Windows リアームカウントが 0 でないこと

リアーム機能を使用すると、Windows の試用バージョンのアクティベーション期間を延長できます。イメージ作成プロセスでは、リアームカウントを 0 以外の値にする必要があります。

Windows リアームカウントを確認するには

1. Windows の [スタート] メニューで [Windows システム] を選択し、[コマンドプロンプト] を選択します。
2. [コマンドプロンプト] ウィンドウで、以下のコマンドを入力し、Enter キーを押します。

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

リアームカウントを 0 以外の値にリセットするには、Microsoft Windows ドキュメントの「Sysprep (Generalize) a Windows installation」を参照してください。

トラブルシューティングに関するその他のヒント

が Image Checker によって実行されるすべてのテストに WorkSpace 合格しても、 からイメージを作成できない場合は WorkSpace、次の点を確認してください。

- WorkSpace が Domain™ グループ内のユーザーに割り当てられていないことを確認します。ドメインアカウントがあるかどうかを確認するには、次の PowerShellコマンドを実行します。

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- Windows 7 WorkSpaces のみ: イメージの作成中にユーザープロファイルのコピー中に問題が発生した場合は、次の問題を確認します。
  - 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 (GPOs) 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リクエストされたときに、RDP証明書のサムプリントへのアクセスを制限します。イメージを作成する前に、 WorkSpace を、継承がブロックされ、GPOs適用されていない新しい組織単位 (OU) に移動します。

- 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] を選択します。

ステップ 3: カスタムイメージとカスタムバンドルを作成する

WorkSpace イメージを検証したら、カスタムイメージとカスタムバンドルの作成に進むことができます。

カスタムイメージとカスタムバンドルを作成するには

1. まだ に接続している場合は WorkSpace、 WorkSpaces クライアントアプリケーションで Amazon WorkSpaces を選択して切断します。
2. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
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、イメージの作成を選択します。のステータス WorkSpace が Stopped の場合は、アクション、イメージの作成を選択する前に、まず開始する必要があります (アクション、開始 WorkSpacesを選択 ）。

   > **Note**
   >
   > プログラムでイメージを作成するには、 CreateWorkspaceImage APIアクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceImage」の「」を参照してください。

5. 続行する前に、 を再起動 (再起動 ） WorkSpace するように求めるメッセージが表示されます。Amazon WorkSpaces ソフトウェアを再起動すると、最新バージョンに WorkSpace 更新されます。

メッセージ WorkSpace を閉じて の手順に従って、 を再起動しますWorkSpaces Personal の WorkSpace を再起動する。完了したら、この手順の Step 4 を繰り返します。ただし、再起動メッセージが表示されたら、[次へ] を選択します。イメージを作成するには、 のステータスが Available WorkSpace で、変更ステータスが None である必要があります。

6. イメージを識別するのに役立つイメージの名前と説明を入力し、[イメージの作成] を選択します。イメージの作成中、 のステータス WorkSpace は一時停止になり、 WorkSpace は使用できなくなります。

> **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。イメージは、ステータスが Available に WorkSpace 変わると完了します (これには最大 45 分かかる場合があります) 。

8. イメージを選択し、[Actions] (アクション)、[Create bundle] (バンドルの作成) を選択します。

> **Note**
>
> プログラムでバンドルを作成するには、 CreateWorkspaceBundleAPIアクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceBundle」の「」を参照してください。

9. バンドル名と説明を入力し、次の操作を行います。

   - バンドルハードウェアタイプで、このカスタムバンドル WorkSpaces から起動するときに使用するハードウェアを選択します。
   - [Storage settings] (ストレージ設定) で、ルートボリュームとユーザーボリュームサイズのデフォルトの組み合わせのいずれかを選択するか、[Custom] (カスタム) を選択し、[Root volume size] (ルートボリュームサイズ) と [User volume size] (ユーザーボリュームサイズ) に値 (最大 2000 GB) を入力します。

     デフォルトのルートボリューム (Microsoft Windows の場合は C ドライブ、Linux の場合は /) およびユーザーボリューム (Windows の場合は D ドライブ、Linux の場合は /home) で使用できるサイズの組み合わせは以下のとおりです。

     - ルート: 80 GB、ユーザー: 10 GB、50 GB、または 100 GB

- ルート: 175 GB、ユーザー: 100 GB
- Graphics.g4dn、 GraphicsPro.g4dn、Graphics、および GraphicsPro WorkSpaces のみ: ルート: 100 GB、ユーザー: 100 GB

または、ルートボリュームとユーザーボリュームをそれぞれ 2,000 GB まで拡張できます。

> **Note**
>
> データを確実に保持するために、 の起動後にルートボリュームまたはユーザーボリュームのサイズを小さくすることはできません WorkSpace。代わりに、 の起動時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 WorkSpace。ルートボリュームの場合は PowerPro WorkSpace 80 GB、ユーザーボリュームの場合は 10 GB 以上の値、標準、パフォーマンス、パワー、または を起動できます。Graphics.g4dn、GraphicsPro.g4dn、Graphics、または は、ルートボリュームの場合は 100 GB、ユーザーボリュームの場合は 100 GB GraphicsPro WorkSpace 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ているもの

Windows 7、Windows 10、または Windows 11 からイメージを作成すると WorkSpace、Cドライブの内容全体が含まれます。

Windows 10 または 11 の場合 WorkSpaces、 のユーザープロファイル`D:\Users\`*`username`*はカスタムイメージに含まれません。

Windows 7 `D:\Users\`*`username`*では WorkSpaces、以下を除き、 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ているもの

Amazon Linux からイメージを作成すると WorkSpace、ユーザーボリューム (/home) の内容全体が削除されます。ルートボリューム (/) の内容は含まれますが、以下に該当するフォルダとキーは削除されます。

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/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/ 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 用のカスタム 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 WorkSpace で 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

AWS リージョン内、またはリージョン間でカスタム WorkSpaces イメージをコピーできます。イメージをコピーすると、独自の識別子の付いた同一のイメージを作成したことになります。

コピー先のリージョンで BYOL が有効になっている限り、自分のライセンス使用 (BYOL) イメージを別のリージョンにコピーできます。関係するすべてのアカウントとリージョンで BYOL が有効になっていることを確認してください。

> **Note**
>
> 中国 (寧夏) リージョンでは、同じリージョン内でのみイメージをコピーできます。
> AWS GovCloud (US) Regionで他の AWS リージョンとの間でイメージをコピーするには、AWS サポートにお問い合わせください。
> オプトインリージョンで、他のリージョンにイメージをコピーするには、AWS サポートにお問い合わせください。オプトインリージョンの詳細については、「利用できるリージョン」を参照してください。

別の AWS アカウントによって共有されたイメージをコピーすることもできます。共有イメージの詳細については、WorkSpaces 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 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、の Identity and Access Management WorkSpaces を参照してください。

イメージの一括コピー

コンソールを使用して、イメージを 1 つずつコピーできます。イメージを一括コピーするには、CopyWorkspaceImage API オペレーションまたは AWS Command Line Interface (AWS CLI) 内の copy-workspace-image コマンドを使用します。詳細については、Amazon WorkSpaces API リファレンスの CopyWorkspaceImage または AWS CLI コマンドリファレンスの copy-workspace-image を参照してください。

Important

共有イメージをコピーする前に、正しい AWS アカウントから共有されていることを確認します。イメージが共有されているかどうかを判断し、イメージを所有している AWS アカウント ID を確認するには、DescribeWorkSpaceImages および DescribeWorkspaceImagePermissions API オペレーションを使用するか、AWS CLI で describe-workspace-images および describe-workspace-image-permissions コマンドを使用します。

コンソールを使用してイメージをコピーするには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。

3. イメージを選択し、[Actions] (アクション)、[Copy image] (イメージをコピー) の順に選択します。
4. [Select destination] (対象を選択する) で、イメージのコピー先の AWS リージョンを選択します。
5. [Name of the copy] (コピーの名前) で、コピーしたイメージの新しい名前を入力し、[Description] (説明) で、コピーしたイメージの説明を入力します。
6. (オプション) [Tags] (タグ) で、コピーしたイメージのタグを入力します。詳細については、「WorkSpaces 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

WorkSpaces のカスタムイメージは、同じ AWS リージョン内の AWS アカウント間で共有できます。イメージの共有後、受取人アカウントは、必要に応じてイメージを他の AWS リージョンにコピーできます。イメージのコピーの詳細については、WorkSpaces 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 リージョンでのイメージ数のクォータは適用されます。共有イメージは、受信者がイメージをコピーするまで、受信者アカウントのクォータにはカウントされません。Amazon WorkSpaces クォータの詳細については、 Amazon WorkSpaces クォータ を参照してください。

共有イメージを削除するには、そのイメージを削除する前に共有を解除する必要があります。

ライセンス持ち込みのイメージを共有する

Bring-Your-Own-License (BYOL) イメージは、BYOL が有効になっている AWS アカウントとのみ共有できます。BYOL イメージを共有する先の AWS アカウントも、同じ組織の一部である (同じ支払いアカウントに属する) 必要があります。

> **Note**
>
> AWS GovCloud (米国西部) および AWS GovCloud (米後東部) リージョンでは、AWS アカウント間での BYOL イメージの共有は、現時点ではサポートされていません。AWS GovCloud (米国西部) および AWS GovCloud (米国東部) リージョンのアカウント間で BYOL イメージを共有する場合は、AWS サポートにお問い合わせください。

自分に共有されたイメージ

自分にイメージが共有された場合は、コピーできます。その後、共有イメージのコピーを使用して、新しい WorkSpaces を起動するためのバンドルを作成できます。

> **Important**
>
> 共有イメージをコピーする前に、正しい AWS アカウントから共有されていることを確認します。イメージが共有されているかどうかをプログラムで判断するには、DescribeWorkSpaceImages および DescribeWorkspaceImagePermissions API オペレーションを使用するか、 AWS Command Line Interface (CLI) で describe-workspace-images および describe-workspace-image-permissions コマンドを使用します。

自分に共有されたイメージに対して表示される作成日は、イメージが最初に作成された日付であり、イメージが自分に共有された日付ではありません。

自分にイメージが共有されている場合、そのイメージを他のアカウントと共有することはできません。

イメージを共有するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. イメージを選択して、詳細ページを開きます。
4. イメージの詳細ページの [Shared accounts (共有アカウント)] セクションで、[Add account (アカウントの追加)] を選択します。
5. [Add account (アカウントの追加)] ページの [Add account to share with (共有するアカウントの追加] で、イメージの共有先のアカウントのアカウント ID を入力します。

> **Important**
>
> イメージを共有する前に、共有先の AWS アカウントの ID が正しいことを確認してください。

6. [Share image (イメージの共有)] を選択します。

> **Note**
>
> 共有イメージを使用するには、まず受信者アカウントでイメージをコピーする必要があります。その後、受取人アカウントは、共有イメージのコピーを使用して新しい WorkSpaces を起動するためのバンドルを作成できます。

イメージの共有を停止するには

1. https://console.aws.amazon.com/workspaces/ で WorkSpaces コンソールを開きます。
2. ナビゲーションペインで [Images] を選択します。
3. イメージを選択して、詳細ページを開きます。
4. イメージの詳細ページの [Shared accounts (共有アカウント)] セクションで、共有を停止する AWS アカウントを選択し、[Unshare (共有解除)] を選択します。
5. イメージの共有解除を確認するメッセージが表示されたら、[Unshare (共有解除)] を選択します。

> **Note**
>
> 共有を解除した後にイメージを削除する場合、まず共有されているすべてのアカウントからそのイメージの共有を解除する必要があります。

イメージの共有を解除すると、受信者アカウントはイメージのコピーを作成できなくなります。ただし、受取人アカウント内に既に存在する共有イメージのコピーは、このアカウント内に残り、これらのコピーから新しい WorkSpaces を起動できます。

プログラムによりイメージを共有または共有解除するには

プログラムによりイメージを共有または共有を解除するには、UpdateWorkspaceImagePermission APIオペレーションまたは update-workspace-image-permission AWS Command Line Interface (AWS CLI) コマンドを使用します。イメージが共有されているかどうかを確認するには、DescribeWorkspaceImagePermissions API オペレーションまたは describe-workspace-image-permissions CLI コマンドを使用します。

WorkSpaces 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/ 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/ 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 WorkSpaces を使用して をモニタリングする

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 WorkSpaces を使用して をモニタリングする EventBridge

CloudTrail ログ

AWS CloudTrail は、WorkSpacesのユーザー、ロール、または AWS のサービスによって実行されたアクションのレコードを提供します。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、「Logging WorkSpaces API Calls by Using CloudTrail」を参照してください。スマートカードユーザーの成功したサインインと失敗したサインインが AWS CloudTrail によって ログに記録されます。詳細については、「スマートカードユーザーの AWS サインインイベントを理解する」を参照してください。

CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor は、AWS 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で、インターネットの問題がパフォーマンスや可用性にどのように影響してい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 では、AWS のグローバルネットワークのフットプリントから接続データを取得します。そして、インターネット向けトラフィックのパフォーマンスと可用性に関するベースラインの計算に使用します。現在のところ、Internet Monitor は個々のエンドユーザーにインターネットパフォーマンスを提供することはできませんが、都市レベルや ISP レベルでは提供できます。

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、特定のしきい値をモニタリング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。

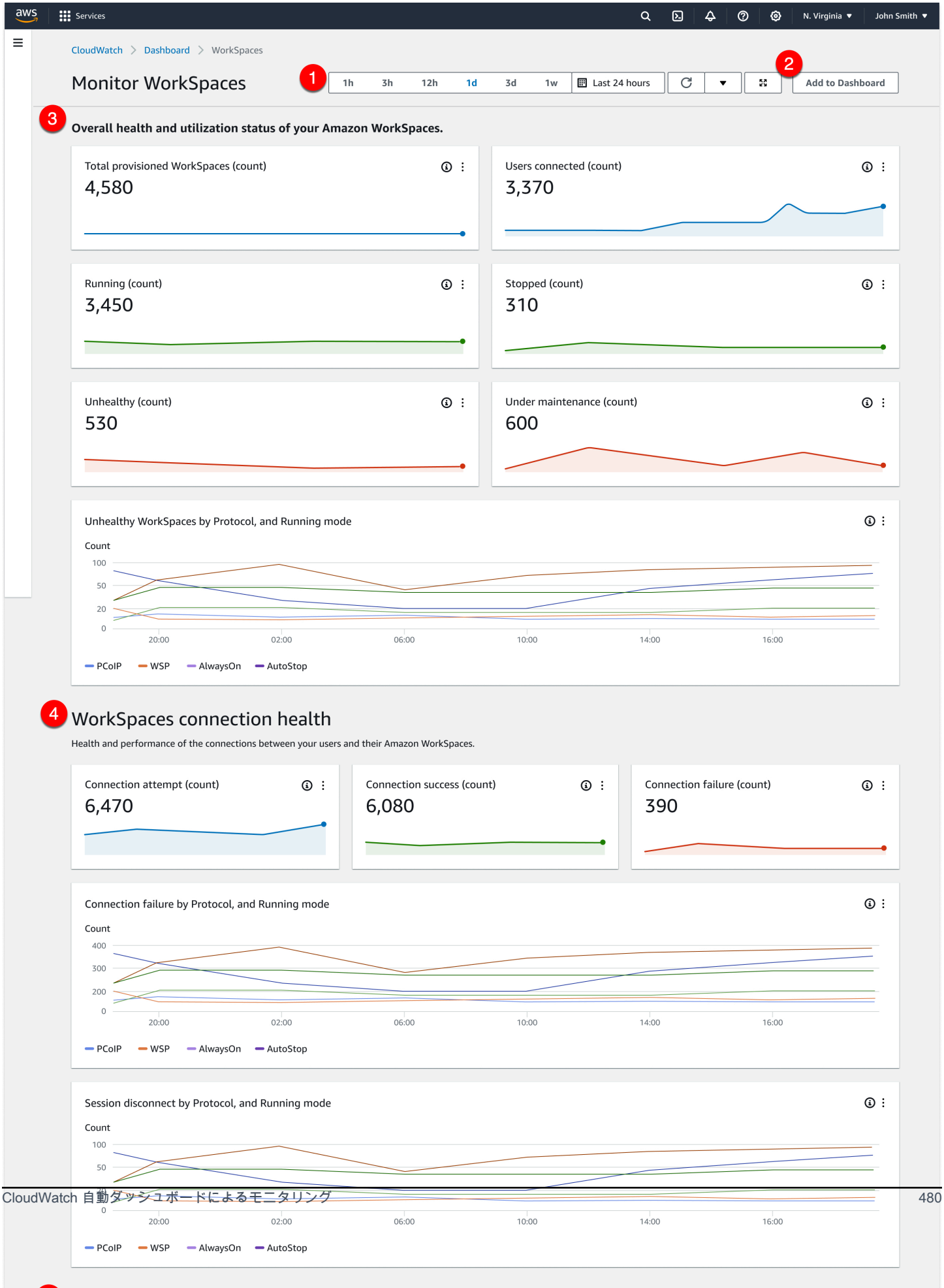
WorkSpaces の CloudWatch 自動ダッシュボードは、すべての商用 AWS リージョンで利用できます。

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 WorkSpaces を使用して をモニタリングする

WorkSpaces と Amazon CloudWatch は統合されているため、パフォーマンスメトリクスを収集して分析できます。これらのメトリクスは、 CloudWatch コンソール、 CloudWatch コマンドラインインターフェイス、または を使用してプログラムでモニタリングできます CloudWatch API。また、 では、メトリクスの指定されたしきい値に達したときにアラームを設定 CloudWatch することもできます。

CloudWatch および アラームの使用の詳細については、「Amazon 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 リージョンのAMAZONサブセットでポート 443 でアクセスを有効にします。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。

内容

- WorkSpaces メトリクス
- WorkSpaces メトリクスのディメンション
- モニタリングの例

WorkSpaces メトリクス

AWS/WorkSpaces 名前空間には、次のメトリクスが含まれます。

メトリクス	説明	ディメンション	統計	単位
Available [1]	正常なステータスを返した WorkSpaces の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
Unhealthy [1]	異常なステータスを返した WorkSpaces の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
		UserName		
ConnectionAttempt [2]	接続試行の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
ConnectionSuccess [2]	成功した接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
ConnectionFailure [2]	失敗した接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	Count
SessionLaunchTime [2、6]	セッションの開始 WorkSpaces にかかる時間。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	秒 (時間)
InSessionLatency [2、6]	WorkSpaces クライアントとの間のラウンドトリップ時間 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	ミリ秒 (時間)

メトリクス	説明	ディメンション	統計	単位
SessionDisconnect [2、6]	ユーザーが開始して失敗した接続を含む、閉じられた接続の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント
UserConnected [3]	ユーザーが接続され WorkSpaces ている の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	Count
Stopped	停止 WorkSpaces されている の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	カウント

メトリクス	説明	ディメンション	統計	単位
Maintenance [4]	メンテナンス WorkSpaces 中の の数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	Count
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	Count
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	Count
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	Count

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 WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Maximum、Minimum	割合 (%)
MemoryUsage	マシンのメモリの使用率。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Maximum、Minimum	割合 (%)
RootVolumeDiskUsage	ルートディスクボリュームの使用率。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId 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 WorkspaceId RunningMode Protocol ComputeType BundleId 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 WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Maximum、Minimum、Data Samples	割合 (%)
UpTime	の最後の再起動からの時間 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Maximum、Minimum、Data Samples	[秒]

[1] WorkSpaces はステータスリクエストを に定期的に送信します WorkSpace。 WorkSpace は、これらのリクエストに応答Available`したとき、およびこれらのリクエストに応答できなかったUnhealthyときにマークされます。これらのメトリクスは、粒度WorkSpace レベルごとに利用でき、組織 WorkSpaces 内のすべての に対して集計されます。

[2] WorkSpaces 各 に対して行われた接続のメトリクスを記録します WorkSpace。これらのメトリクスは、ユーザーが WorkSpaces クライアント経由で正常に認証され、クライアントがセッションを開始した後に出力されます。メトリクスは、詳細度WorkSpace レベルごとに使用でき、ディレクトリ WorkSpaces 内のすべての に対して集計されます。

[3] WorkSpaces は、接続ステータスリクエストを に定期的に送信します WorkSpace。ユーザーは、能動的にセッションを使用している場合、接続済みとしてレポートされます。このメトリクスは、粒度WorkSpace レベルごとに使用でき、組織 WorkSpaces 内のすべての に対して集計されます。

[4] このメトリクス WorkSpaces は、 AutoStop 実行モードで設定された に適用されます。でメンテナンスが有効になっている場合 WorkSpaces、このメトリクス WorkSpaces は、現在メンテナンス中の の数をキャプチャします。このメトリクスは、 がメンテナンス WorkSpace を開始したタイミングと削除されたタイミングを記述する粒度WorkSpace レベルで利用できます。

[5] 信頼できるデバイスの機能がディレクトリに対して有効になっている場合、Amazon は証明書ベースの認証 WorkSpaces を使用して、デバイスが信頼できるかどうかを判断します。ユーザーが にアクセスしようとすると WorkSpaces、これらのメトリクスが出力され、信頼されたデバイス認証が成功または失敗したことを示します。これらのメトリクスは、Amazon WorkSpaces Windows および macOS クライアントアプリケーションに対してのみ、ディレクトリレベルの粒度で使用できます。

[6] Web WorkSpaces Access では使用できません。

[7] このメトリクスは、パケットの平均損失を測定します。

- の場合PCoIP: クライアントからゲートウェイへの平均UDPパケット損失を測定します。

  > **Note**
  >
  > これはゲートウェイで測定されます。

- の場合DCV: ゲートウェイからクライアントへのUDPパケット損失を測定します。

  > **Note**
  >
  > これはゲートウェイで測定されます。

WorkSpaces メトリクスのディメンション

メトリクスデータをフィルタリングするために以下のディメンションを使用します。

ディメンション	説明
DirectoryId	指定されたディレクトリの 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	指定された にメトリクスデータをフィルタリングします WorkSpace。 WorkSpace ID の形式は ですws-XXXXXXXXXX 。
CertificateId	メトリクスデータをフィルタリングして、ディレクトリに関連付けられている指定されたルート証明書にします。証明書 ID の形式は wsc-XXXXXXXXX です。
RunningMode	実行モードでメトリクスデータを にフィルタリング WorkSpaces します。実行モードの形式は AutoStop または です AlwaysOn。
BundleId	プロトコル WorkSpaces によってメトリクスデータを にフィルタリングします。バンドルの形式は wsb-XXXXXXXXXX です。
ComputeType	コンピューティングタイプ WorkSpaces でメトリクスデータを にフィルタリングします。
Protocol	プロトコルタイプ WorkSpaces でメトリクスデータを にフィルタリングします。
UserName	ユーザーの名前 WorkSpaces でメトリクスデータを にフィルタリングします。

ディメンション	説明
	Note は、次のような ASCII以外の文字で構成UserNameすることはできません。 • アクセント文字: é、à、ö、ñ など。 • 非ラテン文字 • 記号: ©#、®#、€、£、µ、¥ など。

モニタリングの例

次の例は、 を使用してアラーム AWS CLI に応答 CloudWatchし、ディレクトリ WorkSpaces 内のどの で接続障害が発生したかを判断する方法を示しています。

CloudWatch アラームに応答するには

1. describe-alarms コマンドを使用して、アラームの対象になっているディレクトリを特定します。

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. describe-workspaces コマンドを使用して、指定されたディレクトリ WorkSpaces 内の のリストを取得します。

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. get-metric-statistics コマンドを使用して、 ディレクトリ WorkSpace 内の各 の CloudWatch メトリクスを取得します。

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
```

```
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Amazon WorkSpaces を使用して をモニタリングする EventBridge

Amazon のイベントを使用して、 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、応答できます WorkSpaces。たとえば、次の目的でイベントを使用できます。

- WorkSpaces ログインイベントを今後の参照用にログとして保存またはアーカイブし、ログを分析してパターンを探し、それらのパターンに基づいてアクションを実行します。
- WAN IP アドレスを使用してユーザーがログインする場所を決定し、 ポリシーを使用して、 のイベントタイプで見つかった WorkSpaces アクセス基準を満たす からのファイルまたはデータにのみユーザーがアクセスできるようにしますWorkSpaces Access。
- ログインデータを分析し、 を使用して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。
- 接続に使用する WorkSpaces クライアントバージョンを確認します WorkSpaces。

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。イベントはほぼリアルタイムで EventBridge に配信されます。を使用すると EventBridge、イベントに応じてプログラムによるアクションをトリガーするルールを作成できます。たとえば、 SNSトピックを呼び出して E メール通知を送信するルールや、Lambda 関数を呼び出して何らかのアクションを実行するルールを設定できます。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

WorkSpaces アクセスイベント

WorkSpaces クライアントアプリケーションは、ユーザーが に正常にログインしたときにWorkSpaces Accessイベントを送信します WorkSpace。すべての WorkSpaces クライアントがこれらのイベントを送信します。

WorkSpaces の使用のために出力されるイベントには、 WorkSpaces クライアントアプリケーションバージョン 4.0.1 以降DCV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、これは Teradici 認証クライアントの IP アドレスです。

`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 にログインした時刻 WorkSpace。

`clientPlatform`

- `Android`
- `Chrome`
- `iOS`
- `Linux`
- `OSX`
- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

のディレクトリの識別子 WorkSpace。domain/ にはディレクトリ識別子を前置する必要があります。例えば、"domain/d-123456789" と指定します。

`clientVersion`

接続に使用されるクライアントバージョン WorkSpaces。

`workspaceId`

WorkSpace の識別子。

イベントを処理する WorkSpacesルールを作成する

イベントを処理するルールを作成するには、 WorkSpaces次の手順に従います。

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. https://console.aws.amazon.com/sns/v3/home で Amazon SNSコンソールを開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. [トピックの作成] を選択します。
4. [Type (タイプ)] で、[Standard (標準)] を選択します。
5. [Name] (名前) で、トピックの名前を入力します。
6. [トピックの作成] を選択します。
7. [Create subscription] を選択します。
8. [Protocol (プロトコル)] として [Email (E メール)] を選択します。
9. [Endpoint] (エンドポイント) で、通知を受信するメールアドレスを入力します。
10. [Create subscription] を選択します。
11. 次の件名の E メールメッセージが表示されます。AWS Notification - Subscription Confirmation。 手順に従ってサブスクリプションを確認します。

WorkSpaces イベントを処理するルールを作成するには

1. で Amazon EventBridge コンソールを開きますhttps://console.aws.amazon.com/events/。
2. ルールの作成を選択します。
3. [Name] (名前) に、ルールの名前を入力します。
4. [ルールタイプ] で、[イベントパターンを持つルール] を選択します。
5. [Next (次へ)] を選択します。
6. [Event pattern] (イベントパターン) の場合は、次のいずれかを実行します。
   a. イベントソース で AWS のサービス を選択します。
   b. [AWS のサービス] で、[WorkSpaces] を選択します。
   c. イベントタイプで、WorkSpacesアクセスを選択します。
   d. デフォルトでは、すべてのイベントに通知が送信されます。必要に応じて、特定のクライアントまたはワークスペースのイベントをフィルタリングするイベントパターンを作成できます。
7. [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. ターゲットタイプ には、AWS のサービス を選択します。
    b. ターゲットの選択 で、SNSトピックを選択します。
    c. トピック で、通知用に作成したSNSトピックを選択します。
9. [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 (次へ)] を選択します。
12. [Create rule] (ルールの作成) を選択します。

スマートカードユーザーの AWS サインインイベントを理解する

AWS CloudTrail は、スマートカードユーザーの成功したサインインイベントと失敗したサインインイベントを記録します。これには、ユーザーが特定の資格情報のチャレンジや要素を解決するよう求められるたびにキャプチャされるサインインイベントに加えて、その特定の認証情報の検証リクエストのステータスが含まれます。必要な認証情報のチャレンジをすべて完了したユーザーだけがサインインを許可され、`UserAuthentication` イベントがログに記録されます。

次の表は、サインインの CloudTrail イベント名とその目的を示します。

イベント名	イベントの目的
`CredentialChallenge`	ユーザーは AWS サインインで特定の認証情報のチャレンジを解決するように要求されたことを示し、必要な `CredentialType` (スマートカードなど) を指定します。
`CredentialVerification`	ユーザーが特定の `CredentialChallenge` リクエストの解決を試みたことを通知し、その認証情報が成功したか失敗したかを指定します。
`UserAuthentication`	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知します。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、`UserAuthentication` イベントはログに記録されません。

次の表は、特定のサインイン CloudTrail イベント内に含まれる追加の有用なイベントデータフィールドを示します。

イベント名	イベントの目的	サインインイベントの適用性	値の例
AuthWorkflowID	サインインシーケンス全体で発生するすべてのイベントを相関させます。各ユーザーサインインで、AWS サインインによって複数のイベントが送信されることがあります。	CredentialChallenge , CredentialVerification , UserAuthentication	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
CredentialType	ユーザーが特定の CredentialChallenge リクエストの解決を試みたことを通知し、その認証情報が成功したか失敗したかを指定します。	CredentialChallenge , CredentialVerification , UserAuthentication	CredentialType": "SMARTCARD" (possible values today: SMARTCARD)
LoginTo	要求されたすべての認証要件をユーザーが正常に完了し、正常にサインインしたことを通知します。ユーザーが必要な認証情報のチャレンジを正常に完了できなかった場合、UserAuthentication イベントは口グに記録されません。	UserAuthentication	"LoginTo": "https://skylight.local“

AWS サインインシナリオのイベント例

以下の例は、さまざまなサインインシナリオで予想される CloudTrail イベントのシーケンスを示します。

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"
    }
}
```


テンプレートを使用して AWS CloudFormation カスタム CloudWatch ダッシュボードを作成する

AWS には、 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 WorkSpaces。次の AWS CloudFormation テンプレートオプションから選択して、 AWS CloudFormation コンソール WorkSpaces で のカスタムダッシュボードを作成します。

開始する前に考慮すべき点

カスタム CloudWatch ダッシュボードの使用を開始する前に、次の点を考慮してください。

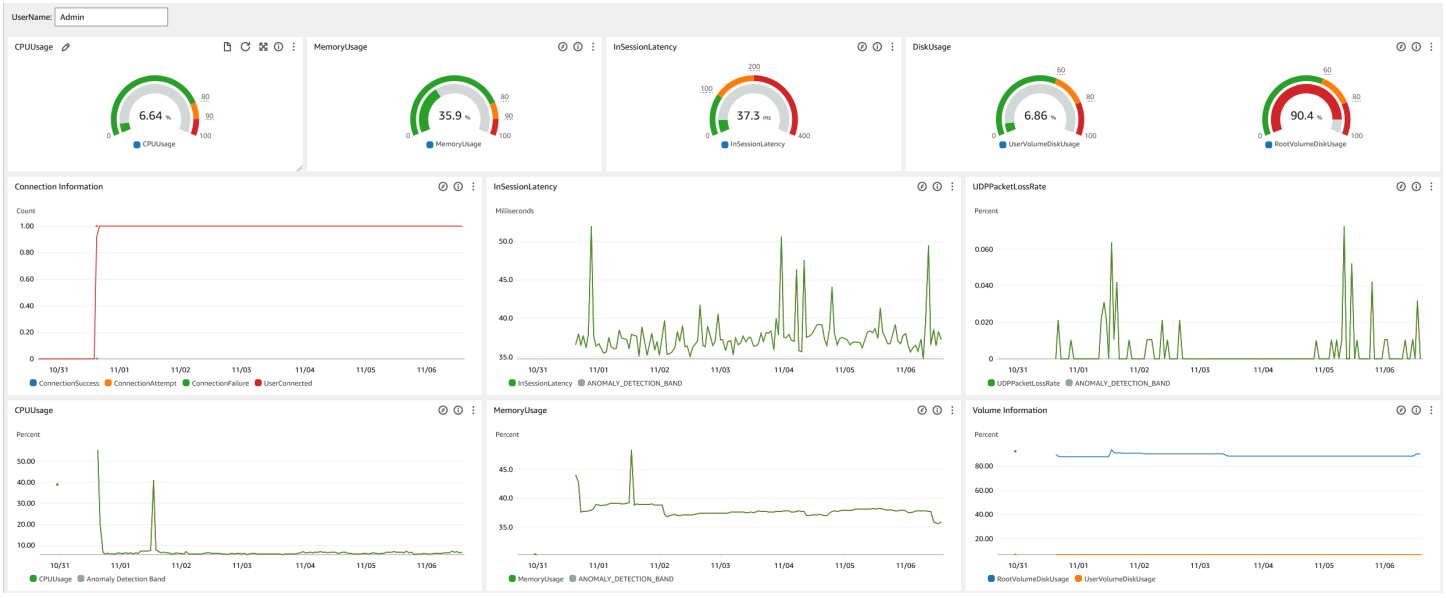
- モニタリング WorkSpaces するデプロイされた AWS リージョン と同じ にダッシュボードを作成します。
- CloudWatch コンソールを使用してカスタムダッシュボードを作成することもできます。
- コストはカスタム CloudWatch ダッシュボードに関連付けられている場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

ヘルプデスク用ダッシュボード

ヘルプデスクダッシュボードには、特定の に関する以下のメトリクスが表示されます WorkSpace。

- 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。



CloudWatch を使用して 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 AWS CloudFormation。

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、ヘルプデスクのカスタム 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ているページが開きます。
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. DashboardName 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。

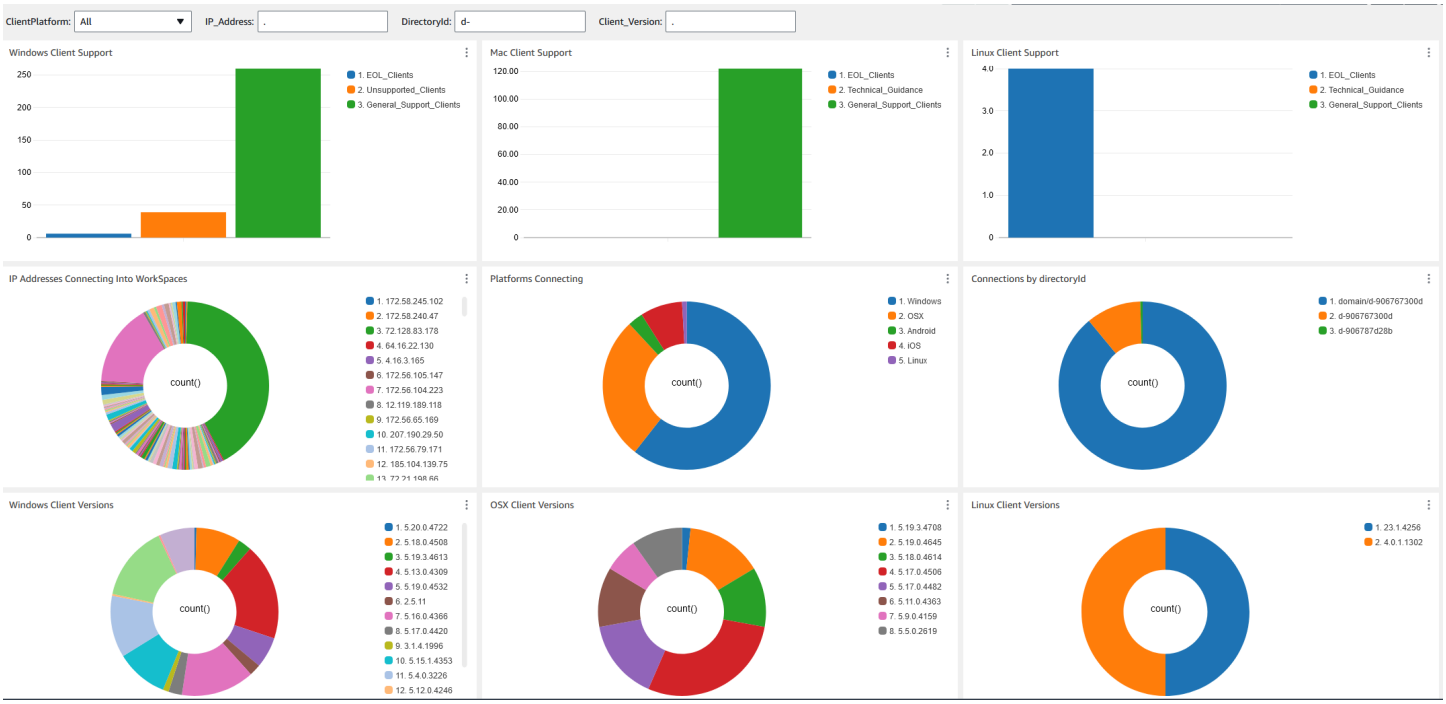
   ダッシュボード名には、英数字、ダッシュ (-)、アンダースコア (_) のみを使用できます。
6. [Next (次へ)] を選択します。
7. [スタックオプションの設定] ページでデフォルトの選択内容を確認し、[次へ] を選択します。
8. [変換では、アクセス機能が必要になる場合があります] まで下にスクロールし、確認のチェックボックスをオンにします。次に、送信を選択してスタックとカスタム CloudWatchダッシュボードを作成します。

   > **Important**
   >
   > コストはカスタム CloudWatch ダッシュボードに関連付けられている場合があります。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. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
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、 UserName の WorkSpace 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

Connection Insights ダッシュボードには、 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、および IP アドレスが表示されます WorkSpaces。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。



CloudWatch を使用して 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 AWS CloudFormation。

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、Connection Insights 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ているページが開きます。
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. DashboardName 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。その他の関連する CloudWatch アクセスグループ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. にLogRetention、 を保持する日数を入力します LogGroup 。
7. でSetupEventBridge、 WorkSpaces 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. でWorkSpaceAccessLogsName、 WorkSpaces アクセスログ CloudWatch LogGroup がある 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ている場合があります。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。

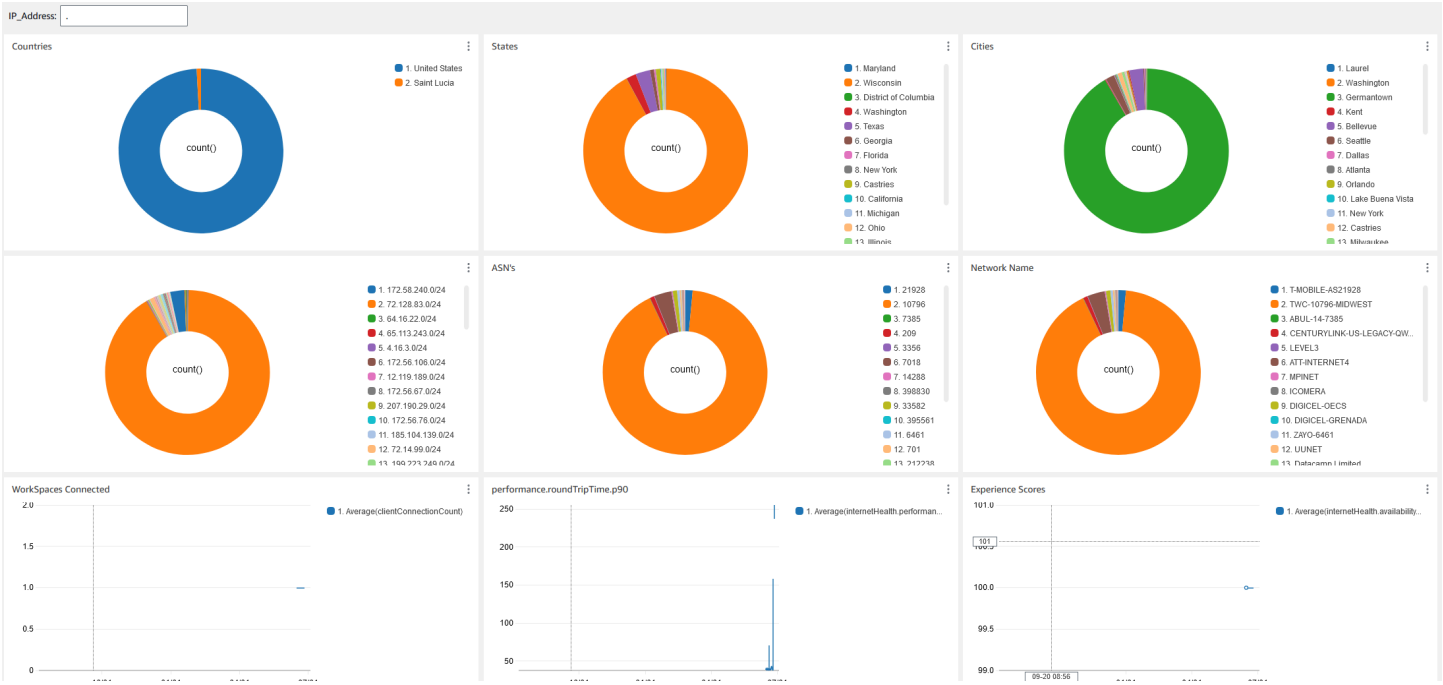
12. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
13. 左のナビゲーションバーの [ダッシュボード] を選択します。
14. [カスタムダッシュボード] で、この手順の前半で入力したダッシュボード名を持つダッシュボードを選択します。
15. Connection Insights ダッシュボードを使用して WorkSpaceデータをモニタリングできるようになりました。

インターネットモニタリング用ダッシュボード

Internet Monitoring ダッシュボードには、ユーザーが WorkSpaces インスタンスに参加するために使用するインターネットサービスプロバイダー (ISP) に関する詳細が表示されます。都市、州、、ネッ

トワーク名ASN、接続数、 WorkSpacesパフォーマンス、エクスペリエンスの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 インターネットモニターをデプロイして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。



CloudWatch を使用して 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、Internet Monitor で CloudWatch Internet Monitor 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た Amazon CloudWatch Internet Monitor でのモニターの作成」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、Internet Monitoring 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ているページが開きます。
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. DashboardName 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。その他の関連する CloudWatch アクセスグループ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. でResourcesToMonitor、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. でMonitorName、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ている場合があります。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. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
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. Internet Monitoring ダッシュボードを使用して WorkSpace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
- WorkSpaces 個人用のマルチリージョンレジリエンス

WorkSpaces Personal のクロスリージョンリダイレクト

Amazon のクロスリージョンリダイレクト機能を使用すると WorkSpaces、完全修飾ドメイン名 (FQDN) を登録コードとして使用できます WorkSpaces。クロスリージョンリダイレクトは、ドメインネームシステム (DNS) ルーティングポリシーと連携して、プライマリ WorkSpaces が利用できない場合に WorkSpaces ユーザーを代替 にリダイレクト WorkSpaces します。例えば、DNSフェイルオーバールーティングポリシーを使用すると、プライマリ AWS リージョン WorkSpaces の にアク

セスできない場合に、指定したフェイルオーバーリージョン WorkSpaces の にユーザーを接続できます。

フェDNSイルオーバールーティングポリシーとともにクロスリージョンリダイレクトを使用すると、リージョンの耐障害性と高可用性を実現できます。この機能は、トラフィックの分散やメンテナンス WorkSpaces 期間中の代替手段の提供など、他の目的でも使用できます。DNS 設定に Amazon Route 53 を使用する場合は、Amazon CloudWatch アラームをモニタリングするヘルスチェックを利用できます。

この機能を使用するには、2 つ (またはそれ以上) の AWS リージョンでユーザー WorkSpaces 用にを設定する必要があります。また、接続エイリアスと呼ばれる特別な FQDNベースの登録コードを作成する必要があります。これらの接続エイリアスは、 WorkSpaces ユーザーのリージョン固有の登録コードを置き換えます。 (リージョン固有の登録コードは有効ですが、クロスリージョンリダイレクトが機能するには、ユーザーはFQDN代わりに を登録コードとして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、接続文字列を指定します。接続文字列は、 `www.example.com`やFQDNなどの ですdesktop.example.com。このドメインをクロスリージョンリダイレクトに使用するには、ドメインレジストラに登録し、ドメインの DNSサービスを設定する必要があります。

接続エイリアスを作成したら、異なるリージョンの WorkSpaces ディレクトリに関連付けて、関連付けペアを作成します。関連付けペアごとに、プライマリリージョンと 1 つ以上のフェイルオーバーリージョンがあります。プライマリリージョンで停止が発生した場合、DNSフェイルオーバールーティングポリシーは、フェイルオーバーリージョンでユーザー用に WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。

プライマリリージョンとフェイルオーバーリージョンを指定するには、DNSフェイルオーバールーティングポリシーを設定するときにリージョンの優先度 (プライマリまたはセカンダリ) を定義します。

内容

- 前提条件
- 制限
- ステップ 1: 接続エイリアスを作成する
- (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
- 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
- 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

- 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
- IAM 接続エイリアスの関連付けと関連付け解除を行う アクセス許可
- 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FQDNで として使用するドメインを所有して登録する必要があります。別のドメインレジストラをまだ使用していない場合は、Amazon Route 53 を使用してドメインを登録できます。詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 を使用したドメイン名の登録を参照してください。

  > **Important**
  >
  > Amazon と組み合わせて使用するドメイン名を使用するには、必要なすべての権限が必要です WorkSpaces。お客様は、ドメイン名が第三者の法的権利を侵害または侵害しないこと、または適用法に違反しないことに同意するものとします。

  ドメイン名の長さの合計は 255 文字を超えることはできません。ドメイン名の詳細については、「Amazon Route 53 デベロッパーガイド」のDNS「ドメイン名形式」を参照してください。

  クロスリージョンリダイレクトは、パブリックドメイン名とプライベートDNSゾーンのドメイン名の両方で機能します。プライベートDNSゾーンを使用している場合は、 を含む仮想プライベートクラウド (VPN) への仮想プライベートネットワーク (VPC) 接続を提供する必要がありますWorkSpaces。 WorkSpaces ユーザーがパブリックインターネットFQDNからプライベート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 サービスを設定し、必要なDNSルーティングポリシーを設定する必要があります。クロスリージョンリダイレクトは、DNSルーティングポリシーと組み合わせて機能し、必要に応じてWorkSpaces ユーザーをリダイレクトします。
- クロスリージョンリダイレクトを設定するプライマリリージョンとフェイルオーバーリージョンごとに、 ユーザー WorkSpaces 用に を作成します。各リージョンの各 WorkSpaces ディレクトリで同じユーザー名を使用していることを確認してください。Active Directory ユーザーデータを同期させるには、AD Connector を使用して、ユーザー WorkSpaces 用に設定した各リージョンで同じ Active Directory を指すことをお勧めします。作成の詳細については WorkSpaces、「起動 WorkSpaces」を参照してください。

> **Important**
>
> マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを Amazon で使用するために登録できます WorkSpaces。Amazon で使用するレプリケートされたリージョンにディレクトリを登録しようとすると、失敗 WorkSpaces します。 AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内の Amazon WorkSpaces での使用はサポートされていません。

クロスリージョンリダイレクトの設定が完了したら、 WorkSpaces ユーザーがプライマリリージョンのリージョンFQDNベースの登録コード (などWSpdx+ABC12D) ではなく、 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、「」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ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する。

> **Note**
>
> Active Directory でユーザーを作成する代わりに WorkSpaces コンソールでユーザーを作成すると、新しい を起動するたびに、 はリージョンベースの登録コードを含む招待メールをユーザー WorkSpaces に自動的に送信します WorkSpace。つまり、フェイルオーバーリージョンでユーザー WorkSpaces 用に を設定すると、ユーザーにはこれらのフェイルオーバーに関する E メールも自動的に送信されます WorkSpaces。リージョンベースの登録コードを含む E メールを無視するようにユーザーに指示する必要があります。

制限

- クロスリージョンリダイレクトは、プライマリリージョンへの接続が失敗したかどうかを自動的にチェックせず、 を別のリージョンにフェイル WorkSpaces オーバーします。つまり、自動フェイルオーバーは発生しません。

  自動フェイルオーバーシナリオを実装するには、リージョン間リダイレクトと組み合わせて他のメカニズムを使用する必要があります。例えば、Amazon Route 53 フェイルオーバーDNSルーティングポリシーと、プライマリリージョンの CloudWatch アラームをモニタリングする Route 53 ヘルスチェックを組み合わせることができます。プライマリリージョンの CloudWatch アラームがトリガーされると、DNSフェイルオーバールーティングポリシーは、フェイルオーバーリージョンでユーザー用に WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。
- クロスリージョンリダイレクトを使用している場合、ユーザーデータは異なるリージョン WorkSpaces の 間で保持されません。Amazon WorkDocs が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サポートされている場合は、ユーザーが異なるリージョンからファイルにアクセスできるように、 WorkDocs WorkSpaces ユーザーに Amazon を設定することをお勧めします。Amazon の詳細については WorkDocs、「Amazon 管理ガイド」の「Amazon WorkDocs Drive」を参照してください。 WorkDocs ユーザーに対して Amazon を有効にする方法の詳細については、 WorkDocs WorkSpace WorkSpaces Personal に既存の AWS Directory Service ディレクトリを登録する「」および「」を参照してくださいAWS Managed Microsoft AD 用に Amazon WorkDocs を有効にする。 WorkSpaces ユーザーが WorkDocs で Amazon をセットアップする方法については WorkSpaces、「Amazon WorkSpaces ユーザーガイド」の「 との統合 WorkDocs」を参照してください。
- クロスリージョンリダイレクトは、Linux、macOS、および Windows WorkSpaces クライアントアプリケーションのバージョン 3.0.9 以降でのみサポートされています。ウェブアクセスでクロスリージョンリダイレクトを使用することもできます。
- クロスリージョンリダイレクトは、 および中国 (寧夏) AWS リージョンを除く、Amazon WorkSpaces が利用可能なすべての リージョンで使用できます。 AWS GovCloud (US) Region

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

2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクト] で、[接続エイリアスの作成] を選択します。
5. Connection 文字列には、 FQDN`www.example.com`や などの を入力しますす`desktop.example.com`。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. これらの手順を繰り返しますが、 ではStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、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、そのリージョンのディレクトリに関連付けることができるのは 1 つのアカウント (自分のアカウントまたは共有アカウント) のみです。

接続エイリアスを別の AWS アカウントと共有するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
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 2 つ以上のリージョンの WorkSpaces ディレクトリに関連付けると、ディレクトリ間に関連付けペアが作成されます。関連付けペアごとに、プライマリリージョンと 1 つ以上のフェイルオーバーリージョンがあります。

例えば、プライマリリージョンが米国西部 (オレゴン) リージョンである場合、米国西部 (オレゴン) リージョンの WorkSpaces ディレクトリと米国東部 (バージニア北部) リージョンの WorkSpaces ディレクトリをペアリングできます。プライマリリージョンで停止が発生した場合、クロスリージョンリダイレクトは、DNSフェイルオーバールーティングポリシーおよび米国西部 (オレゴン) リージョンで実施されているヘルスチェックと組み合わせて機能し、米国東部 (バージニア北部) WorkSpaces リージョンで設定した にユーザーをリダイレクトします。クロスリージョンリダイレクトのエクスペリエンスの詳細については、クロスリージョンリダイレクト時の動作 を参照してください。

> **Note**
>
> WorkSpaces ユーザーがフェイルオーバーリージョンからかなり離れている (例えば、数千マイル離れている) 場合は、通常よりも応答性が低下する WorkSpaces 可能性があります。ロケーションからさまざまな AWS リージョンへの往復時間 (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、そのリージョンのディレクトリに関連付けることができるのは 1 つのアカウント (自分のアカウントまたは共有アカウント) のみです。

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. [クロスリージョンリダイレクトの関連付け] で、接続文字列を選択し、[アクション]、[関連付け/関連付け解除] を選択します。

   接続エイリアスの詳細ページから、接続エイリアスをディレクトリに関連付けることもできます。これを行うには、[関連付けられたディレクトリ] で、[ディレクトリを関連付ける] を選択します。
5. 関連付け/関連付け解除ページのディレクトリへの関連付けで、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、プライマリリージョンのディレクトリのみを Amazon で使用できます WorkSpaces。Amazon でレプリケートされたリージョンでディレクトリを使用しようとすると失敗 WorkSpaces します。 AWS Managed Microsoft AD を使用したマルチリージョンレプリケーションは、レプリケートされたリージョン内の Amazon WorkSpaces での使用はサポートされていません。
6. [関連付ける] を選択します。
7. これらの手順を繰り返しますが、 ではStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、フェイルオーバーリージョンごとにこれらのステップを繰り返します。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ペアを作成したら、接続文字列で使用したドメインDNSのサービスを設定できます。この目的のために任意のDNSサービスプロバイダーを使用できま

す。希望するDNSサービスプロバイダーがまだない場合は、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DNS「サービスとしての Amazon Route 53 の設定」を参照してください。

ドメインDNSのサービスを設定したら、クロスリージョンリダイレクトに使用するDNSルーティングポリシーを設定する必要があります。例えば、Amazon Route 53 ヘルスチェックを使用して、ユーザーが特定のリージョン WorkSpaces の に接続できるかどうかを判断できます。ユーザーが接続できない場合は、DNSフェイルオーバーポリシーを使用して、あるリージョンから別のリージョンにDNSトラフィックをルーティングできます。

DNS ルーティングポリシーの選択の詳細については、「Amazon Route 53 デベロッパーガイド」の「ルーティングポリシーの選択」を参照してください。Amazon Route 53 ヘルスチェックの詳細については、Amazon Route 53 デベロッパーガイドの Amazon Route 53 によるリソースのヘルスチェック方法を参照してください。

DNS ルーティングポリシーを設定するときは、接続エイリアスとプライマリリージョンのディレクトリ間の関連付けの接続識別子が必要です。 WorkSpaces また、接続エイリアスとフェイルオーバーリージョン内の WorkSpaces ディレクトリ間の関連付けには、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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで [アカウント設定] を選択します。
4. クロスリージョンリダイレクトの関連付けで、接続文字列テキスト (FQDN) を選択して、接続エイリアスの詳細ページを表示します。
5. 接続エイリアスの詳細ページの [関連付けられたディレクトリ] で、[接続識別子] に表示される値をメモします。
6. これらの手順を繰り返しますが、 ではStep 2、必ず のフェイルオーバーリージョンを選択してください WorkSpaces。複数のフェイルオーバーリージョンがある場合は、これらのステップを繰り返して、各フェイルオーバーリージョンの接続 ID を調べます。

例: Route 53 を使用してDNSフェイルオーバールーティングポリシーを設定するには

次の例では、ドメインのパブリックホストゾーンを設定します。ただし、パブリックホストゾーンまたはプライベートホストゾーンを設定できます。ホストゾーンの設定の詳細については、Amazon Route 53 デベロッパーガイドのホストゾーンの使用を参照してください。

この例では、フェイルオーバールーティングポリシーも使用します。クロスリージョンリダイレクト戦略には、他のルーティングポリシータイプを使用できます。DNS ルーティングポリシーの選択の詳細については、「Amazon Route 53 デベロッパーガイド」の「ルーティングポリシーの選択」を参照してください。

Route 53 でフェイルオーバールーティングポリシーを設定する場合、プライマリリージョンのヘルスチェックが必要です。Route 53 でのヘルスチェックの作成の詳細については、Amazon Route 53 デベロッパーガイドの「Amazon Route 53 ヘルスチェックの作成」および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、削除」を参照してください。

Route 53 ヘルスチェックで Amazon CloudWatch アラームを使用する場合は、プライマリリージョンのリソースをモニタリングするアラームも設定 CloudWatch する必要があります。詳細については CloudWatch、「Amazon ユーザーガイド」の「Amazon CloudWatchとは」を参照してください。CloudWatch Route 53 がヘルスチェックで CloudWatch アラームを使用する方法の詳細については、「Amazon Route 53 デベロッパーガイド」の「アラームをモニタリングするヘルスチェックのステータスを Route 53 が判断する方法 CloudWatch 」および CloudWatch 「アラームのモニタリング」を参照してください。

Route 53 でDNSフェイルオーバールーティングポリシーを設定するには、まずドメインのホストゾーンを作成する必要があります。

1. で Route 53 コンソールを開きますhttps://console.aws.amazon.com/route53/。
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. で Route 53 コンソールを開きますhttps://console.aws.amazon.com/route53/。

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. モニタリングする対象 で、エンドポイント、他のヘルスチェックのステータス (計算されたヘルスチェック) 、または CloudWatch アラームの状態を選択します。
5. 前のステップで選択した内容に応じて、ヘルスチェックを設定し、[次へ] を選択します。
6. [ヘルスチェックが失敗したときに通知を受け取る] ページの [アラームの作成] で、[はい] または [いいえ] を選択します。
7. [ヘルスチェックの作成] を選択します。

ヘルスチェックを作成したら、DNSフェイルオーバーレコードを作成できます。

1. で Route 53 コンソールを開きますhttps://console.aws.amazon.com/route53/。
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 の場合は`desktop.example.com`、 と入力します**`desktop`**。

   > **Note**
   >
   > ルートドメインを使用する場合は、[レコード名] を空白のままにします。ただし、 専用にドメインを設定していない限り`workspaces`、 `desktop`や などのサブドメインを使用することをお勧めします WorkSpaces。

7. レコードタイプで、 TXT - E メール送信者の検証とアプリケーション固有の値に使用します。
8. TTL 秒設定はデフォルトのままにしておきます。
9. に追加するフェイルオーバーレコードで***`your_domain_name`***、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、 に追加するフェイルオーバーレコード***your_domain_name***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. に追加するフェイルオーバーレコードで***your_domain_name***、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、 に追加するフェイルオーバーレコード***your_domain_name***の下に表示されます。

プライマリリージョンに設定したヘルスチェックが失敗した場合、DNSフェイルオーバールーティングポリシーは WorkSpaces ユーザーをフェイルオーバーリージョンにリダイレクトします。Route 53 は引き続きプライマリリージョンのヘルスチェックを監視し、プライマリリージョンのヘルスチェックが失敗しなくなった場合、Route 53 は自動的に WorkSpaces ユーザーをプライマリリージョン WorkSpaces の 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「レコードTXT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

停止中に必要に応じてユーザーの がリダイレクト WorkSpaces されるようにするには、接続文字列 (FQDN) をユーザーに送信する必要があります。リージョンベースの登録コード (などWSpdx+ABC12D) を既に WorkSpaces ユーザーに発行している場合、それらのコードは有効です。ただし、クロスリージョンリダイレクトが機能するには、 WorkSpaces ユーザーがクライアントアプリケーション WorkSpaces に WorkSpaces を登録するときに、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、 WorkSpaces は、新しい を起動するたびに、リージョンベースの登録コード (などWSpdx+ABC12D) を含む招待メールをユーザーに自動的に送信します WorkSpace。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 に自動的に送信される招待 E メールには、接続文字列の代わりにこのリージョンベースの登録コード WorkSpaces が含まれています。
>
> WorkSpaces ユーザーがリージョンベースの登録コードではなく接続文字列を使用していることを確認するには、次の手順を使用して、接続文字列を含む別の E メールを送信する必要があります。

接続文字列を WorkSpaces ユーザーに送信するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで、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 WorkSpace から対応するユーザーを選択します。一度に選択できる は 1 WorkSpace つだけです。
5. [アクション]、[Invite User (ユーザーを招待)] の順に選択します。
6. ユーザーを招待 WorkSpaces ページに、ユーザーに送信する E メールテンプレートが表示されます。

7. （オプション) WorkSpaces ディレクトリに関連付けられている接続エイリアスが複数ある場合は、接続エイリアス文字列リストからユーザーに使用する接続文字列を選択します。E メールテンプレートが更新され、選択した文字列が表示されます。
8. メールアプリケーションを使用して、E メールテンプレートテキストをコピーしユーザー宛のメールに貼り付けます。E メールアプリケーションでは、必要に応じてテキストを変更できます。招待 E メールの準備ができたら、ユーザーに送信します。

クロスリージョンリダイレクトアーキテクチャ図

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 WorkSpaces での作成と保守が容易ではなく、クロスリージョンデータレプリケーションも許可されません。プライマリリージョンとセカンダリリージョン WorkSpaces の両方で を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

停止が発生した場合は、DNSレコードを手動で更新するか、フェイルオーバーリージョンを決定するヘルスチェックに基づいて自動ルーティングポリシーを使用できます。「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 WorkSpaces のから切断されます。再接続しようとすると、次のエラーメッセージが表示されます。

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

その後、ユーザーは再度ログインするように求められます。登録コードFQDNとして を使用している場合、再度ログインすると、DNSフェイルオーバールーティングポリシー WorkSpaces によってフェイルオーバーリージョンで設定した にリダイレクトされます。

> **Note**
>
> 場合によっては、ユーザーが再度ログインしたときに再接続できないことがあります。この動作が発生した場合は、 WorkSpaces クライアントアプリケーションを閉じて再起動してから、再度ログインする必要があります。

ディレクトリからの接続エイリアスの関連付けを解除する

ディレクトリから接続エイリアスの関連付けを解除できるのは、ディレクトリを所有するアカウントだけです。

接続エイリアスを別のアカウントと共有していて、そのアカウントがそのアカウントが所有するディレクトリに接続エイリアスを関連付けている場合は、そのアカウントを使用して接続エイリアスとディレクトリとの関連付けを解除する必要があります。

ディレクトリから接続エイリアスの関連付けを解除するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、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**
>
> ユーザーの登録コードFQDN WorkSpaces として を使用しなくなった場合は、潜在的なセキュリティ問題を防ぐために、特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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、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。

IAM 接続エイリアスの関連付けと関連付け解除を行う アクセス許可

IAM ユーザーを使用して接続エイリアスの関連付けまたは関連付け解除を行う場合、ユーザーには `workspaces:AssociateConnectionAlias`および のアクセス許可が必要です`workspaces:DisassociateConnectionAlias`。

```
{
  "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の関連付けまたは関連付け解除を行う IAMポリシーを作成する場合は、 でアカウント ID を指定することはできませんARN。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"
      ]
    }
  ]
}
```

アカウントが関連付けまたは関連付け解除する接続エイリアスを所有しているARN場合にのみ、 でアカウント ID を指定できます。

IAM の使用方法の詳細については、「の Identity and Access Management WorkSpaces」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FQDNとして を使用しなくなった場合は、潜在的なセキュリティ問題を防ぐために、次の予防措置を講じる必要があります。

- ディレクトリのリージョン固有の登録コード (などWSpdx+ABC12D) を WorkSpaces ユーザーに発行 WorkSpaces し、 を登録コードFQDNとして使用しないように指示してください。
- このドメインをまだ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、DNSTXTレコードを更新してこのドメインを削除してください。このドメインをDNSTXTレコードから削除

し、 WorkSpaces ユーザーが を登録コードFQDNとして使用しようとすると、接続試行は無害に失敗します。

- このドメインを所有しなくなった場合、 WorkSpaces ユーザーはリージョン固有の登録コードを使用する必要があります。登録コードFQDNとして を引き続き使用しようとすると、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 個人用のマルチリージョンレジリエンス

Amazon WorkSpaces Multi-Region Resilience (MRR) を使用すると、中断したイベントが原因でプライマリリージョンに到達できない場合に、ユーザーをセカンダリ WorkSpaces リージョンにリダイレクトできます。スタンバイへのログ記録時に登録コードを切り替える必要はありませんWorkSpaces。スタンバイ WorkSpaces は、スタンバイデプロイの作成と管理を合理化する 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、スタンバイを作成するプライマリリージョン WorkSpace の を選択しますWorkSpace 。システムは、プライマリ WorkSpace バンドルイメージをセカンダリリージョンに自動的にミラーリングします。その後、セカンダリリージョン WorkSpace に新しいスタンバイを自動的にプロビジョニングします。

Amazon WorkSpaces マルチリージョンレジリエンスは、DNSヘルスチェックとフェイルオーバー機能を活用するクロスリージョンリダイレクトに基づいて構築されています。これにより、完全修飾ドメイン名 (FQDN) WorkSpaces を登録コードとして使用できます。ユーザーが にログインすると WorkSpaces、 のドメインネームシステム (DNS) ポリシーに基づいて、サポートされているWorkSpaces リージョン間でリダイレクトできますFQDN。Amazon Route 53 を使用する場合は、クロスリージョンリダイレクト戦略を策定する際に Amazon CloudWatch アラームをモニタリングするヘルスチェックを使用することをお勧めします WorkSpaces。詳細については、「Amazon Route 53 デベロッパーガイド」の「Amazon Route 53 ヘルスチェックの作成」およびDNS「フェイルオーバーの設定」を参照してください。

データレプリケーションは、プライマリリージョンからセカンダリリージョンにデータを一方向レプリケート WorkSpaces するスタンバイのアドオン機能です。データレプリケーションを有効にすると、システムボリュームとユーザーボリュームのEBSスナップショットが 12 時間ごとに作成されます。マルチリージョンレジリエンス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、セカンダリリージョンの更新に使用されます WorkSpace。

内容

- 前提条件

- 制限
- マルチリージョンレジリエンススタンバイを設定する WorkSpace
- スタンバイを作成する WorkSpace
- スタンバイを管理する WorkSpace
- スタンバイを削除する WorkSpace
- スタンバイ用の一方向データレプリケーション WorkSpaces
- Amazon EC2容量を復旧用に予約する計画を立てる

前提条件

- スタンバイを作成する前に、プライマリリージョンのユーザー WorkSpaces 用に を作成する必要があります WorkSpaces。作成の詳細については WorkSpaces、「」を参照してください WorkSpaces Personal のディレクトリを作成する。
- スタンバイ時にデータレプリケーションを有効にするには WorkSpaces、セルフマネージド Active Directory または AWS Managed Microsoft AD のいずれかをスタンバイリージョンにレプリケートするように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。
- プライマリの ENA、NVMe、PV ドライバーなどのネットワーク依存関係ドライバーを必ず更新してください WorkSpaces。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、「Windows インスタンス用の Elastic Network Adapter (ENA) ドライバー をインストールまたはアップグレードする」および「Windows インスタンスでの PV ドライバーのアップグレード」を参照してください。 AWS NVMe ドライバー
- EC2Config、EC2Launch、および EC2Launch V2 エージェントは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、「UpdateEC2Config」およびEC2Launch「」を参照してください。
- 適切なデータレプリケーションを行うには、プライマリリージョンとセカンダリリージョンの Active Directory が FQDN、OU、およびユーザー と同期していることを確認しますSID。
- スタンバイのデフォルトのクォータ (制限) WorkSpaces は 0 です。スタンバイを作成する前に、サービスクォータの引き上げをリクエストする必要があります WorkSpace。詳細については、「Amazon WorkSpaces クォータ」を参照してください。
- カスタマーマネージドキーを使用してプライマリとスタンバイの両方を暗号化していることを確認します WorkSpaces。単一リージョンキーまたはマルチリージョンキーを使用して、プライマリとスタンバイを暗号化できます WorkSpaces。

制限

- スタンバイはプライマリのバンドルイメージ WorkSpaces のみをコピーします WorkSpaces が、プライマリからシステムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) はコピーしません WorkSpaces。システムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) をプライマリから WorkSpaces スタンバイにコピーするには WorkSpaces、データレプリケーションを有効にする必要があります。
- スタンバイを直接変更、再構築、復元、または移行することはできません WorkSpace。
- クロスリージョンリダイレクトのフェイルオーバーはDNS、設定によって制御されます。自動フェイルオーバーシナリオを実装するには、クロスリージョンリダイレクトと組み合わせて別のメカニズムを使用する必要があります。例えば、Amazon Route 53 フェイルオーバーDNSルーティングポリシーと、プライマリリージョンの CloudWatch アラームをモニタリングする Route 53 ヘルスチェックを組み合わせることができます。プライマリリージョンの CloudWatch アラームが呼び出されると、DNSフェイルオーバールーティングポリシーは、フェイルオーバーリージョンで WorkSpaces 設定した に WorkSpaces ユーザーをリダイレクトします。
- データレプリケーションは、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 フェイルオーバー中は、12 ~ 24 時間の間にデータとアプリケーションにアクセスできます。停止後、セカンダリで作成したデータを手動でバックアップ WorkSpace し、ログアウトします。プライマリからデータにアクセスできるように、作業はネットワークドライブなどの外部ドライブに保存することをお勧めします WorkSpace。
- データレプリケーションは Simple AD AWS をサポートしていません。
- スタンバイ時にデータレプリケーションを有効にすると WorkSpaces、プライマリ WorkSpaces (ルートボリュームとシステムボリュームの両方) のEBSスナップショットが 12 時間ごとに作成されます。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。その結果、特定の の最初のレプリケーション WorkSpace は、それ以降のレプリケーションよりも時間がかかります。スナップショットは の内部スケジュールで開始 WorkSpaces され、タイミングを制御することはできません。
- プライマリ WorkSpace とスタンバイの WorkSpace 結合が同じドメインを使用している場合は、ドメインコントローラーとの接続が失われないように WorkSpace 、特定の時点でプライマリ WorkSpace またはスタンバイのいずれかにのみ接続することをお勧めします。
- マルチリージョンレプリケーション AWS Managed Microsoft AD 用に を設定する場合、プライマリリージョンのディレクトリのみを登録して使用できます WorkSpaces。ディレクトリをレプリケートされたリージョンに登録して使用しようとすると WorkSpaces、失敗します。を使用したマ

ルチリージョンレプリケーション AWS Managed Microsoft AD は、レプリケートされたリージョン WorkSpaces 内の での使用はサポートされていません。

- クロスリージョンリダイレクトをすでに設定していて、スタンバイを使用せずにプライマリリージョンとセカンダリリージョン WorkSpaces の両方で作成されている場合は WorkSpaces、セカンダリリージョン WorkSpace の既存の を直接スタンバイに変換することはできません WorkSpace 。代わりに、セカンダリリージョン WorkSpace で をシャットダウンし、スタンバイを作成するプライマリリージョン WorkSpace で を選択し WorkSpace 、スタンバイを使用してスタンバイ WorkSpaces を作成する必要があります WorkSpace。
- 停止後、セカンダリで作成したデータを手動でバックアップ WorkSpace し、ログアウトします。プライマリからデータにアクセスできるように、作業内容をネットワークドライブなどの外部ドライブに保存することをお勧めします WorkSpace。
- WorkSpaces マルチリージョンレジリエンスは現在、次のリージョンで使用できます。
  - 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
  - 欧州 (フランクフルト) リージョン
  - 欧州 (アイルランド) リージョン
- WorkSpaces マルチリージョンレジリエンスは、Linux、macOS、および Windows WorkSpaces クライアントアプリケーションのバージョン 3.0.9 以降でのみサポートされています。ウェブアクセスでマルチリージョンレジリエンスを使用することもできます。
- WorkSpaces マルチリージョンレジリエンスは、Windows と Bring-Your-Own-License (BYOL) をサポートしています WorkSpaces。Amazon Linux 2、Ubuntu WorkSpaces、Rocky Linux、Red Hat Enterprise Linux、または GPU対応 WorkSpaces (Graphics、GraphicsPro、Graphics.g4dn、.g4dn など) をサポートしていません GraphicsPro。
- フェイルオーバーまたはフェイルバックが完了したら、15～30 分待ってから に接続します WorkSpace。

マルチリージョンレジリエンススタンバイを設定する WorkSpace

マルチリージョンレジリエンススタンバイを設定するには WorkSpace

1. プライマリリージョンとセカンダリリージョンの両方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 ディレクトリで同じユーザー名を使用していることを確認してください。

Active Directory ユーザーデータを同期させるには、AD Connector を使用して、ユーザー WorkSpaces 用に設定した各リージョンで同じ Active Directory を指すことをお勧めします。ディレクトリの作成の詳細については、「ディレクトリの登録 WorkSpaces」を参照してください。

> **Important**
>
> マルチリージョンレプリケーション用に AWS Managed Microsoft AD ディレクトリを設定する場合、プライマリリージョンのディレクトリのみを登録して使用できます WorkSpaces。で使用するレプリケートされたリージョンにディレクトリを登録しようとすると失敗 WorkSpaces します。を使用したマルチリージョンレプリケーション AWS Managed Microsoft AD は、レプリケートされたリージョン WorkSpaces 内の での使用はサポートされていません。

2. プライマリリージョンのユーザー WorkSpaces 用に を作成します。作成の詳細については WorkSpaces、「起動 WorkSpaces」を参照してください。
3. セカンダリリージョン WorkSpace にスタンバイを作成します。スタンバイの作成の詳細については WorkSpace、「スタンバイの作成 WorkSpace」を参照してください。
4. 接続文字列 (FQDN) を作成し、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 のクロスリージョンリダイレクト WorkSpacesの手順のステップ 1～3 に従います。
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組み合わせて機能し、必要に応じて WorkSpaces ユーザーをリダイレクトします。
6. クロスリージョンリダイレクトの設定が完了したら、FQDN接続文字列を含む E メールをユーザーに送信する必要があります。詳細については、「ステップ 5: 接続文字列を WorkSpaces ユーザーに送信する」を参照してください。 WorkSpaces ユーザーが、プライマリリージョンのリージョンFQDNベースの登録コード (WSpdx+ などABC12D) ではなく、 ベースの登録コードを使用していることを確認します。

> **Important**
>
> - Active Directory でユーザーを作成する代わりに WorkSpaces コンソールでユーザーを作成すると、新しい を起動するたびに、 はリージョンベースの登録コードを含む招待メールをユーザー WorkSpaces に自動的に送信します WorkSpace。つまり、セカンダリリージョンのユーザー WorkSpaces 用に を設定すると、ユーザーもこれらのセカンダリの E メールを自動的に受信します WorkSpaces。リージョンベースの登録コードを含む E メールを無視するようにユーザーに指示する必要があります。
> - リージョン固有の登録コードは有効ですが、クロスリージョンリダイレクトが機能するには、ユーザーはFQDN代わりに を登録コードとして使用する必要があります。

スタンバイを作成する WorkSpace

スタンバイを作成する前に WorkSpace、プライマリリージョンとセカンダリリージョンの両方にユーザーディレクトリを作成する、プライマリリージョンの WorkSpaces ユーザー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、サービスクォータによるスタンバイ WorkSpaces 制限の引き上げのリクエストなど、前提条件を満たしていることを確認してください。

スタンバイを作成するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで、WorkSpaces を選択します。
4. スタンバイ WorkSpace を作成する を選択します WorkSpace 。
5. アクション を選択し、スタンバイの作成 WorkSpace を選択します。
6. スタンバイを作成するセカンダリリージョンを選択し WorkSpace、次へを選択します。
7. セカンダリリージョンのユーザーディレクトリを選択し、[Next] (次へ) を選択します。
8. (オプション) 暗号化キーを追加し、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に入力されています。ただし、独自の暗号化キーで置き換えることもできます。
> - データレプリケーションのステータスの更新には数分かかります。
> - スタンバイ WorkSpace がプライマリのスナップショットで正常に更新されると WorkSpace、スナップショットのタイムスタンプはリカバリスナップショットで確認できます。

9. スタンバイの設定を確認し WorkSpaces 、作成を選択します。

> **Note**
>
> - スタンバイに関する情報を表示するには WorkSpaces、プライマリ WorkSpace の詳細ページに移動します。
> - スタンバイはプライマリのバンドルイメージ WorkSpace のみをコピーします WorkSpace が、プライマリからシステムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) はコピーしません WorkSpaces。デフォルトでは、データレプリケーションはオフになっています。システムボリューム (ドライブ C) またはユーザーボリューム (ドライブ D) をプライマリ から WorkSpaces スタンバイ にコピーするには WorkSpaces、データレプリケーションを有効にする必要があります。

スタンバイを管理する WorkSpace

スタンバイを直接変更、再構築、復元、または移行することはできません WorkSpace。

スタンバイのデータレプリケーションを有効にするには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. プライマリリージョンに移動し、プライマリ WorkSpace ID を選択します。
3. 「スタンバイ WorkSpace 」セクションまでスクロールし、「スタンバイの編集 WorkSpace」を選択します。

4. [データレプリケーションを有効にする] を選択します。次に、チェックボックスをオンにして、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**
>
> - スタンバイは休止 WorkSpaces できません。スタンバイを停止しても WorkSpace、保存されていない作業は保持されません。スタンバイを終了する前に、必ず作業を保存することをお勧めします WorkSpaces。
> - スタンバイ時にデータレプリケーションを有効にするには WorkSpaces、セルフマネージド Active Directory または AWS Managed Microsoft AD のいずれかをスタンバイリージョンにレプリケートするように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 および AWS Directory Services でビジネス継続性を構築する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 がプライマリのスナップショットで正常に更新されると WorkSpace、スナップショットのタイムスタンプはリカバリスナップショットで確認できます。

スタンバイを削除する WorkSpace

スタンバイは、通常の を終了するの WorkSpace と同じ方法で終了できます WorkSpace。

スタンバイを削除するには WorkSpace

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. コンソールの右上で、 のプライマリ AWS リージョンを選択します WorkSpaces。
3. ナビゲーションペインで、WorkSpaces を選択します。
4. スタンバイを選択し WorkSpace 、削除を選択します。スタンバイの削除には約 5 分かかります WorkSpace。削除中、スタンバイのステータス WorkSpace は終了に設定されます。削除が完了すると、スタンバイはコンソールから WorkSpace 消えます。

> **Note**
>
> スタンバイの削除 WorkSpace は永続的なアクションであり、元に戻すことはできません。スタンバイ WorkSpace ユーザーのデータは保持されず、破棄されます。ユーザーデータのバックアップについては、 AWS サポートにお問い合わせください。

スタンバイ用の一方向データレプリケーション WorkSpaces

マルチリージョンレジリエンスでデータレプリケーションを有効にすると、プライマリリージョンからセカンダリリージョンにデータをレプリケートできます。定常状態では、マルチリージョンレジリエンスは 12 時間 WorkSpaces ごとにプライマリのシステム (C ドライブ) とデータ (D ドライブ) のスナップショットをキャプチャします。これらのスナップショットはセカンダリリージョンに転送され、スタンバイの更新に使用されます WorkSpaces。デフォルトでは、スタンバイ時のデータレプリケーションは無効になっています WorkSpaces。

スタンバイでデータレプリケーションを有効にすると WorkSpaces、特定のデータボリュームの初期スナップショットは完了し、それ以降のスナップショットは増分になります。その結果、特定の の最初のレプリケーション WorkSpace は、それ以降のレプリケーションよりも時間がかかります。スナップショットは 内の事前定義された間隔でトリガー WorkSpaces され、ユーザーがタイミングを制御することはできません。

フェイルオーバー中、ユーザーがセカンダリリージョンにリダイレクトされると、12 時間から 24 時間経過した WorkSpaces データおよびアプリケーションでスタンバイにアクセスできます。ユーザーがスタンバイを使用している間 WorkSpaces、マルチリージョンレジリエンスは、スタンバイ WorkSpaces からログアウトしたり、プライマリリージョンのスナップショット WorkSpaces でスタンバイを更新したりすることを強制しません。

停止後、ユーザーはスタンバイからログアウト WorkSpaces する前に、セカンダリで作成したデータを手動でバックアップする必要があります WorkSpaces。再度ログインすると、プライマリリージョンとそのプライマリリージョンに誘導されます WorkSpaces。

Amazon EC2容量を復旧用に予約する計画を立てる

Amazon Multi-Region Resilience(MRR) は、デフォルトで Amazon EC2 オンデマンドプールに依存します。特定の Amazon EC2インスタンスタイプが復旧をサポートできない場合、 MRR は使用可能なインスタンスタイプが見つかるまでインスタンスのスケールアップを自動的に試行しますが、極端な状況では、インスタンスが常に利用できるとは限りません。最も重要なインスタンスタイプの可用

性を向上させるには WorkSpaces、 AWS サポートにお問い合わせください。キャパシティプランニングのサポートを提供します。

WorkSpaces Personal の問題のトラブルシューティング

以下の情報は、 に関する問題のトラブルシューティングに役立ちます WorkSpaces。

高度なログ記録の有効化

ユーザーが経験する可能性のある問題のトラブルシューティングに役立つように、任意の Amazon WorkSpaces クライアントで高度なログ記録を有効にできます。

高度なログ記録では、診断情報とデバッグレベルの詳細 (詳細なパフォーマンスデータなど) を含むログファイルが生成されます。1.0 以降および 2.0 以降のクライアントの場合、これらの高度なログファイルは のデータベースに自動的にアップロードされます AWS。

> **Note**
>
> 高度なログファイル AWS 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 Support。詳細については、AWS Support センターを参照してください。

Web Access で高度なログ記録を有効にするには

Web Access で高度なログ記録を有効にするには

1. Amazon WorkSpaces Web Access クライアントを開きます。
2. WorkSpaces サインインページの上部で、診断ログ記録を選択します。
3. ポップアップダイアログボックスで、[診断ログ] が有効になっていることを確認します。
4. [ログレベル] で [高度なログ記録] を選択します。

Google Chrome、Microsoft Edge、および Firefox でログファイルにアクセスするには

1. ブラウザでコンテキスト (右クリック) メニューを開くか、キーボードの Ctrl + Shift + I (Mac の場合は command + option + I) を押して、開発者ツールパネルを開きます。
2. 開発者ツールパネルで、[コンソール] タブを選択してログファイルを見つけます。

Safari でログファイルにアクセスするには

1. [Safari]、[設定] の順に選択します。
2. [設定] セクションで、[詳細] を選択します。
3. [メニューバーに "開発" メニューを表示] を選択します。
4. メニューバーの [開発] タブから、[開発] > [Web インスペクターを表示] を選択します。
5. Safari の [Web インスペクター] パネルで、[コンソール] タブを選択してログファイルを見つけます。

4.0 以上のクライアントで高度なログ記録を有効にするには

Windows クライアントのログは、次の場所に保存されています。

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. コマンドプロンプトアプリを開きます。
3. `-l3` フラグを使用して WorkSpaces クライアントを起動します。

   ```
   c:

   cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > WorkSpaces がすべてのユーザーではなく 1 人のユーザーにインストールされている場合は、次のコマンドを使用します。
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

macOS クライアントのログは次の場所に保存されます。

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

macOS クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   open -a workspaces --args -l3
   ```

Android くらいで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. Android クライアントメニューを開きます。
3. [Support] (サポート) を選択します。
4. [Logging settings] (ログ記録設定) を選択します。
5. [Enable advanced logging] (高度なログ記録の有効化) を選択します。

高度なログを有効にした後に Android クライアントのログを取得するには

- [Extract log] (ログの抽出) をクリックして、圧縮したログをローカルに保存します。

Linux クライアントのログは、次の場所に保存されます。

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

Linux クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

3.0 以上のクライアントで高度なログ記録を有効にするには

Windows クライアントのログは、次の場所に保存されています。

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

Windows クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. コマンドプロンプトアプリを開きます。
3. `-l3` フラグを使用して WorkSpaces クライアントを起動します。

   ```
   c:

   cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

   workspaces.exe -l3
   ```

   > **Note**
   >
   > WorkSpaces がすべてのユーザーではなく 1 人のユーザーにインストールされている場合は、次のコマンドを使用します。
   >
   > ```
   > c:
   > cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
   > workspaces.exe -l3
   > ```

macOS クライアントのログは次の場所に保存されます。

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

macOS クライアントで高度なログ記録を有効にするには

1. Amazon WorkSpaces クライアントを閉じます。
2. ターミナルを開きます。
3. 以下のコマンドを実行します。

   ```
   open -a workspaces --args -l3
   ```

Android くらいで高度な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、 に関する特定の問題のトラブルシューティングに役立ちます WorkSpaces。

問題

- ユーザー名に無効な文字 WorkSpace があるため、Amazon Linux を作成できません
- Amazon Linux のシェルを変更 WorkSpace 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
- 接続されたディレクトリ WorkSpaces での の起動が失敗することが多い
- 起動が内部エラーで WorkSpaces 失敗する
- ディレクトリを登録しようとすると、登録は失敗し、ディレクトリは ERROR状態のままになります。
- ユーザーがインタラクティブなログオンバナー WorkSpace で Windows に接続できない
- ユーザーが Windows に接続できない WorkSpace
- ユーザーが WorkSpaces Web Access WorkSpaces から にログオンしようとすると問題が発生する
- Amazon WorkSpaces クライアントは、ログイン画面に戻る前に、しばらく灰色の「ロード中...」画面を表示します。他のエラーメッセージは表示されない。
- ユーザーにWorkSpace 「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。
- ユーザーに「このデバイスは へのアクセスを許可されていません WorkSpace。Please contact your administrator for assistance.」というメッセージが表示される。
- ユーザーが 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。」 に接続しようとする場合 DCV WorkSpace
- WorkSpaces クライアントはユーザーにネットワークエラーを与えますが、デバイスで他のネットワーク対応アプリを使用できる
- WorkSpace ユーザーには、「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が「指定された証明書はタイムスタンプのため無効です」というエラーを受信しています

- USB プリンターやその他のUSB周辺機器がPCoIPゼロクライアントで機能しない
- ユーザーが Windows または macOS クライアントアプリケーションの更新をスキップしても、最新バージョンをインストールするように求められない
- ユーザーが Chromebook に Android クライアントアプリケーションをインストールできない
- ユーザーに招待 E メールまたはパスワードリセット E メールが届かない
- クライアントのログイン画面でユーザーに [パスワードを忘れた場合] が表示されません。
- Windows にアプリケーションをインストールしようとすると、「システム管理者がこのインストールを禁止するポリシーを設定しています」というメッセージが表示される WorkSpace
- ディレクトリ WorkSpaces にインターネットに接続できない
- インターネットアクセスを失 WorkSpace 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「使用不可」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「レコード」エラーが表示される
- Windows がアイドル状態のままになるとスリープ状態 WorkSpace になる
- の 1 つの状態 WorkSpaces が である UNHEALTHY
- WorkSpace が予期せずクラッシュまたは再起動しています
- 同じユーザー名に複数の がありますが WorkSpace、ユーザーは の 1 つのみにログインできます。 WorkSpaces
- Amazon での Docker の使用に問題がある WorkSpaces
- 一部のAPI通話に ThrottlingException エラーが表示される
- バックグラウンドで実行させると切断され WorkSpace 続ける
- SAML 2.0 フェデレーションは機能しません。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。
- ユーザーは 60 分ごとに WorkSpaces セッションから切断されます。
- ユーザーが 2SAML.0 ID プロバイダー (IdP) によって開始されたフローを使用してフェデレーションする場合、または IdP にフェデレーションした後にユーザーがクライアントからサインインしようとするたびに WorkSpaces 、クライアントアプリケーションの追加のインスタンスが起動すると、リダイレクトURIエラーが発生します。
- ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインイン WorkSpaceしようとすると、「Something went wrong: An error occurred while launching your」というメッセージが表示されます。

- ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインインしようとすると、「タグを検証できません」というメッセージが表示されます。
- 「The client and the server cannot communicate, because they do not possess a common algorithm」(クライアントとサーバーは共通のアルゴリズムを所有していないため、通信できません) というメッセージがユーザーに表示されます。
- マイクまたはウェブカメラが Windows で動作していません WorkSpaces。
- ユーザーは証明書ベースの認証を使用してログインできず、デスクトップセッションに接続するときに 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が、提供 WorkSpaces していない操作を実行しようとしています。
- サポートされていない WorkSpaces リージョンで作成された既存の AWS Managed Directory WorkSpaces で を起動したい。
- 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ます。設定されているきめ細かなパスワードポリシー (FFGP) の設定は無視されます AWS Managed Microsoft AD。
- ユーザーに「これは Web Access OS/platform is not authorized to access your WorkSpace" when trying to access the Windows/Linux WorkSpace を使用しています
- 停止状態の に接続した後、ユーザーの AutoStop WorkSpace が異常と WorkSpace 表示される

ユーザー名に無効な文字 WorkSpace があるため、Amazon Linux を作成できません

Amazon Linux の場合 WorkSpaces、ユーザー名：

- 最大 20 文字を含めることができます。
- UTF-8 で表現できる文字、スペース、数字を含めることができます
- 次の特殊文字を含めることができます: _.-#
- ダッシュ記号 (-) をユーザー名の 1 文字目として使用することはできません。

> **Note**
>
> これらの制限は Windows には適用されません WorkSpaces。Windows では、ユーザー名のすべての文字に対して @ 記号と - 記号 WorkSpaces がサポートされています。

Amazon Linux のシェルを変更 WorkSpace 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 のデフォルトシェルを上書きするには WorkSpaces、「」を参照してくださいAmazon Linux のデフォルトシェルを上書きする WorkSpaces。

Amazon Linux WorkSpaces が起動しない

2020 年 7 月 20 日以降、Amazon Linux WorkSpaces は新しいライセンス証明書を使用します。これらの新しい証明書は、 PCoIP エージェントのバージョン 2.14.1.1、2.14.7、2.14.9、および 20.10.6 以降と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。 には、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の向上が含まれています。7 月 20 日までにこれらのアップグレードを行わないと、Linux のセッションプロビジョニング WorkSpaces は失敗し、エンドユーザーは に接続できなくなります WorkSpaces。

PCoIP エージェントを最新バージョンにアップグレードするには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、WorkSpaces を選択します。
3. Linux を選択し WorkSpace、アクション、再起動を選択して再起動 WorkSpacesします。WorkSpace ステータスが の場合はSTOPPED、アクション、開始 WorkSpaces、ステータスがになるまで待ってAVAILABLEから再起動する必要があります。
4. が再起動し、ステータス WorkSpace が になったらAVAILABLE、このアップグレードの実行ADMIN_MAINTENANCE中に のステータス WorkSpace を に変更することをお勧めします。完了したら、 のステータス WorkSpace を に変更しますAVAILABLE。ADMIN_MAINTENANCE モードの詳細については、「手動メンテナンス」を参照してください。

   のステータスを WorkSpace に変更するにはADMIN_MAINTENANCE、次の手順を実行します。

   a. WorkSpace を選択し、アクション、変更 WorkSpaceを選択します。
   b. [Modify State (状態の変更)] を選択します。
   c. 目的の状態 で、ADMIN_MAINTENANCE を選択します。
   d. Modify を選択します。
5. WorkSpace を介して Linux に接続しますSSH。詳細については、「Personal WorkSpaces で Linux WorkSpaces SSHの接続を有効にする」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. から切断 WorkSpace し、再度再起動します。
9. で のステータスを WorkSpace ADMIN_MAINTENANCE に設定する場合はStep 4、 を繰り返しStep 4て、意図された状態を に設定しますAVAILABLE。

PCoIP エージェントのアップグレード後も Linux の起動に WorkSpace 失敗した場合は、 AWS サポートにお問い合わせください。

接続されたディレクトリ WorkSpaces での の起動が失敗することが多い

オンプレミスディレクトリ内の 2 つのDNSサーバーまたはドメインコントローラーが、ディレクトリへの接続時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。この接続を確認するには、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インスタンスをディレクトリに結合します。

起動が内部エラーで WorkSpaces 失敗する

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が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、サブネットアクション、自動割り当て IP 設定の変更を選択します。この設定が有効になっている場合、パフォーマンスバンドルまたはグラフィックスバンドル WorkSpaces を使用して を起動することはできません。代わりに、この設定を無効にし、インスタンスの起動時に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、登録は失敗し、ディレクトリは ERROR状態のままになります。

この問題は、マルチリージョンレプリケーション用に設定された AWS Managed Microsoft AD ディレクトリを登録しようとしている場合に発生する可能性があります。プライマリリージョンのディレクトリは Amazon で使用するために正常に登録できますが WorkSpaces、レプリケートされたリージョンにディレクトリを登録しようとすると失敗します。 AWS Managed Microsoft AD 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 WorkSpaces 内の Amazon での使用はサポートされていません。

ユーザーがインタラクティブなログオンバナー WorkSpace で Windows に接続できない

インタラクティブなログオンメッセージを実装してログオンバナーを表示すると、ユーザーは Windows にアクセスできなくなります WorkSpaces。現在、インタラクティブの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。 WorkSpaces グループInteractive logon: Message text for users attempting to log onポリシーが適用されていない組織単位 (OU) に を移動します。ログオンメッセージは でサポートされておりDCV WorkSpaces、ユーザーはログオンバナーを受け入れた後で再度ログインする必要があります。

ユーザーが Windows に接続できない WorkSpace

ユーザーが Windows に接続しようとすると、次のエラーが表示されます WorkSpaces。

```
"An error occurred while launching your WorkSpace. Please try again."
```

このエラー WorkSpace は、 が を使用して Windows デスクトップをロードできない場合によく発生しますPCoIP。以下をチェックしてください:

- このメッセージは、Windows のPCoIP標準エージェントサービスが実行されていない場合に表示されます。を使用して接続RDP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するように設定されていること、管理インターフェイス (eth0) 経由で通信できることを検証します。

- PCoIP エージェントをアンインストールした場合は、Amazon WorkSpaces コンソール WorkSpace から を再起動して自動的に再インストールします。

- また、WorkSpacesセキュリティグループがアウトバウンドトラフィックを制限するように変更された場合、長時間の遅延後に Amazon WorkSpaces クライアントでこのエラーが表示されることがあります。送信トラフィックを制限すると、Windows はディレクトリコントローラーと通信してログインできなくなります。セキュリティグループが、プライマリネットワークインターフェイスを介して必要なすべてのポートで ディレクトリコントローラーと通信 WorkSpaces することをに許可していることを確認します。

このエラーの別の原因として、ユーザー権利の割り当てグループポリシーに関連がある場合があります。次のグループポリシーが正しく設定されていない場合、ユーザーは Windows にアクセスできなくなります WorkSpaces。

コンピュータ構成\Windows Settings\Security Settings\Local Policies\User Rights Assignment

- 正しくないポリシー:

  ポリシー: ネットワークからこのコンピュータにアクセスする

  設定: *Domain name*\ドメインコンピュータ

  獲得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: *Domain name*\ドメインユーザー

  獲得GPO: ファイルアクセスを許可する

> **Note**
>
> このポリシー設定は、ドメインコンピュータの代わりにドメインユーザーに適用する必要があります。

詳細については、Microsoft Windows のドキュメントの「ネットワークセキュリティポリシーの設定からこのコンピュータにアクセスする」および「セキュリティポリシー設定を構成する」を参照してください。

ユーザーが WorkSpaces Web Access WorkSpaces から にログオンしようとすると問題が発生する

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

Web Access ユーザーが にログオンできるようにするには WorkSpaces、グループポリシー設定と 3 つのセキュリティポリシー設定を設定する必要があります。これらの設定が正しく設定されていない場合、ユーザーが にログオンしようとすると、ログオン時間が長くなり、画面が黒くなることがあります WorkSpaces。これらの設定を構成するには、「WorkSpaces Personal の WorkSpaces ウェブアクセス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 Bring Your Own License (BYOL) に接続できなくなります WorkSpaces。

Amazon WorkSpaces クライアントは、ログイン画面に戻る前に、しばらく灰色の「ロード中...」画面を表示します。他のエラーメッセージは表示されない。

この動作は通常、 WorkSpaces クライアントがポート 443 経由で認証できるが、ポート 4172 (PCoIP) またはポート 4195 () 経由でストリーミング接続を確立できないことを示しますDCV。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、ポート 4172 または 4195 (TCP および) 経由のアクセスを妨げているクライアント側のファイアウォールまたはプロキシですUDP。このヘルスチェックが失敗した場合は、ローカルのファイアウォール設定を確認してください。

ネットワークチェックに合格すると、 のネットワーク設定に問題がある可能性があります WorkSpace。たとえば、Windows ファイアウォールルールは、管理インターフェイスのポート UDP 4172 または 4195 をブロックする場合があります。 リモートデスクトッププロトコル (RDP) クライアント WorkSpace を使用して に接続し、 WorkSpace が必要なポート要件を満たしていることを確認します。

ユーザーにWorkSpace 「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。

このエラーは通常、 SkyLightWorkSpacesConfigService サービスがヘルスチェックに応答していないことを示します。

を再起動または開始したばかりの場合は WorkSpace、数分待ってからもう一度試してください。

WorkSpace がしばらく実行されていても、このエラーが表示される場合は、 を使用して接続 RDPし、 SkyLightWorkSpacesConfigService サービスが以下であることを確認します。

- 実行中である。
- 自動的に開始するように設定されている。
- 管理インターフェイス (eth0) を介して通信できる。
- サードパーティー製のウイルス対策ソフトウェアによってブロックされていない。

ユーザーに「このデバイスは へのアクセスを許可されていません WorkSpace。Please contact your administrator for assistance.」というメッセージが表示される。

このエラーは、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。

- IP アクセスコントロールグループは WorkSpace ディレクトリで設定されますが、クライアントの IP アドレスは許可リストに登録されません。

  ディレクトリの設定を確認します。ユーザーが接続しているパブリック IP アドレスが へのアクセスを許可していることを確認します WorkSpace。

- [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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
  2. ナビゲーションペインで [ディレクトリ] を選択します。
  3. 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 の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. [Save] を選択します。

- デバイスタイプにはアクセス権が付与されません WorkSpaces。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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
  2. ナビゲーションペインで [ディレクトリ] を選択します。
  3. 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 アクセスを許可する次のいずれかのデバイスタイプから確認します。
     - ChromeOS
     - iOS
     - Linux
     - Web Access
     - ゼロクライアント
  6. [Save] 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。」 に接続しようとする場合 DCV WorkSpace

このエラーが発生したが、ユーザーに接続の問題が発生していない場合は、ネットワークのファイアウォールでポート 4195 が開いていることを確認してください。 WorkSpaces を使用する場合 DCV、クライアントセッションのストリーミングに使用されるポートが 4172 から 4195 に変更されました。

WorkSpaces クライアントはユーザーにネットワークエラーを与えますが、デバイスで他のネットワーク対応アプリを使用できる

WorkSpaces クライアントアプリケーションは、 AWSクラウド内のリソースへのアクセスに依存しており、少なくとも 1 Mbps のダウンロード帯域幅を提供する接続が必要です。デバイスにネットワークへの断続的な接続がある場合、 WorkSpaces クライアントアプリケーションはネットワークの問題を報告する可能性があります。

WorkSpaces は、2018 年 5 月現在、Amazon Trust Services によって発行されたデジタル証明書の使用を強制します。Amazon Trust Services は、 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 に接続できず WorkSpaces 、クライアントはネットワークエラーを表示します。

証明書の失敗による接続の問題を認識するには

- PCoIP ゼロクライアント — 次のエラーメッセージが表示されます。

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- その他のクライアント – ヘルスチェックは、インターネットの赤い三角形の警告が表示されて失敗します。

証明書の失敗を解決するには

- Windows クライアントアプリケーション
- PCoIP ゼロクライアント

- その他のクライアントアプリケーション

Windows クライアントアプリケーション

証明書が失敗した場合は、次のいずれかの解決策を使用します。

解決策 1: クライアントアプリケーションを更新する

https://clients.amazonworkspaces.com/ から最新の Windows クライアントアプリケーション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. Starfield 証明書を DER形式 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) で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。[完了] を選択します。[OK] を選択します。
6. [証明書 (ローカル コンピュータ)] を展開し、[信頼されたルート証明機関] を選択します。[アクション]、[すべてのタスク]、[インポート] の順に選択します。
7. ウィザードに従って、ダウンロードした証明書をインポートします。
8. WorkSpaces クライアントアプリケーションを終了して再起動します。

解決策 3: グループポリシーを使用して Amazon Trust Services を信頼された CA としてデプロイする

グループポリシーを使用して、ドメインの信頼されたルートに Starfield CAs 証明書を追加します。詳細については、「Use Policy to Distribute Certificates」を参照してください。

PCoIP ゼロクライアント

ファームウェアバージョン 6.0 以降 WorkSpace を使用して に直接接続するには、Amazon Trust Services によって発行された証明書をダウンロードしてインストールします。

Amazon Trust Services を信頼されたルート CA として追加するには

1. https://certs.secureserver.net/repository/ を開きます。
2. [Starfield Certificate Chain] で、サムプリント 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 の証明書をダウンロードします。
3. 証明書をゼロクライアントにアップロードします。詳細については、Teradici ドキュメントの「Uploading Certificates」を参照してください。

その他のクライアントアプリケーション

Amazon Trust Services から、Starfield 証明書 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92) を追加します。ルート CA の追加方法の詳細については、以下のドキュメントを参照してください。

- Android: 証明書の追加と削除
- Chrome OS: Chrome 端末でのクライアント証明書の管理
- macOS および iOS: Installing a CA's Root Certificate on Your Test Device

WorkSpace ユーザーには、「デバイスは登録サービスに接続できません。ネットワーク設定を確認してください」というエラーが表示されます。

登録サービスの障害が発生すると、 WorkSpace 接続ヘルスチェックページに「デバイスが WorkSpaces 登録サービスに接続できません。デバイスを に登録することはできません WorkSpaces。ネットワーク設定を確認してください」というエラーメッセージが表示されることがあります。

このエラーは、 WorkSpaces クライアントアプリケーションが登録サービスに到達できない場合に発生します。通常、これは WorkSpaces ディレクトリが削除されたときに発生します。このエラーを解決するには、登録コードが有効で、 AWS クラウドで実行中のディレクトリに対応していることを確認してください。

PCoIP ゼロクライアントユーザーが「指定された証明書はタイムスタンプのため無効です」というエラーを受信しています

Teradici で Network Time Protocol (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発生する可能性があります。をセットアップするにはNTP、「」を参照してくださいWorkSpaces Personal で PCoIP ゼロクライアントを設定する。

USB プリンターやその他のUSB周辺機器がPCoIPゼロクライアントで機能しない

PCoIP エージェントのバージョン 20.10.4 以降、Amazon は Windows レジストリを介したUSB リダイレクトをデフォルトで WorkSpaces 無効にします。このレジストリ設定は、ユーザーがPCoIPゼロクライアントデバイスを使用して に接続する場合のUSB周辺機器の動作に影響します WorkSpaces。

WorkSpaces がバージョン 20.10.4 以降のPCoIPエージェントを使用している場合、USBリダイレクトを有効にするまで、USB周辺機器はPCoIPゼロクライアントデバイスで動作しません。

> **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 WorkSpaces を使用して、これらのレジストリの変更を にプッシュアウトすることをお勧めします。詳細については、「Teradiciのマニュアル」からエージェントの設定および環境の設定を参照してください。

1. 次のレジストリキーの値を 1 (有効) に設定します。

   KeyPath = HKEYLOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
2. 次のレジストリキーの値を 1 (有効) に設定します。

KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP
\pcoip_admin_defaults

KeyName = pcoip.enable_usb

KeyType = DWORD

KeyValue = 1

3. まだ行っていない場合は、 からログアウト WorkSpaceしてから再度ログインします。これで USBデバイスが動作するはずです。

ユーザーが Windows または macOS クライアントアプリケーションの更新をスキップしても、最新バージョンをインストールするように求められない

ユーザーが Amazon WorkSpaces Windows クライアントアプリケーションの更新をスキップすると、SkipThisVersionレジストリキーが設定され、クライアントの新しいバージョンがリリースされたときにクライアントを更新するように求められなくなります。最新バージョンに更新するには、「Amazon 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。次の PowerShell コマンドを実行することもできます。

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

ユーザーが Amazon WorkSpaces macOS クライアントアプリケーションの更新をスキップすると、SUSkippedVersion設定が設定されます。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、クライアントの更新を求めるプロンプトが表示されなくなります。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 Chromebook WorkSpaces 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しているため、Chromebook WorkSpaces クライアントアプリケーションにはそれ以上の更新はなく、その使用はサポートされていません。

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

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、「Android for Chromebook for WorkSpaces Personal をセットアップする」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 WorkSpaces されたドメインを使用して作成された の招待メールまたはパスワードリセットメールは、ユーザーに自動的には送信されません。また、ユーザーが既に Active Directory に存在する場合も、招待メールは自動的に送信されません。

これらのユーザーに招待 E メールを手動で送信するには、「招待 E メールの送信」を参照してください 。

ユーザーパスワードをリセットするには、「WorkSpaces 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。(WorkSpaces クライアントアプリケーションログイン画面のパスワードを忘れた場合？ オプションは使用できません。) ユーザーパスワードをリセットする方法については、WorkSpaces Personal で Active Directory 管理ツールを設定する を参照してください。

Windows にアプリケーションをインストールしようとすると、「システム管理者がこのインストールを禁止するポリシーを設定しています」というメッセージが表示される WorkSpace

この問題に対処するには、Windows インストーラのグループポリシー設定を変更します。このポリシーをディレクトリ WorkSpaces 内の複数の にデプロイするには、ドメイン結合EC2インスタンスから WorkSpaces 組織単位 (OU) にリンクされている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管理ツールを開き、 WorkSpaces マシンアカウントの WorkSpaces グループポリシーオブジェクトに移動して選択します。メインメニューの [Action]、[Edit] を選択します。
3. グループポリシー管理エディタで、[Computer Configuration (コンピュータの構成)]、[Policies (ポリシー)]、[Administrative Templates (管理用テンプレート)]、[Classic Administrative Templates (従来の管理用テンプレート)]、[Windows Components (Windows コンポーネント)]、[Windows Installer (Windows インストーラ)] の順に選択します。
4. [Turn Off Windows Installer (Windows インストーラをオフ)] 設定を開きます。
5. [Turn Off Windows Installer (Windows インストーラをオフ)] ダイアログボックスで、[Not Configured (未構成)] を [Enabled (有効)] に変更し、[Disable Windows Installer (Windows インストーラを無効にする] を [Never (しない)] に設定します。
6. [OK] を選択します。
7. グループポリシーの変更を適用するには、次のいずれかを実行します。
   - を再起動します WorkSpace （ WorkSpaces コンソールで を選択し WorkSpace、アクション、再起動 WorkSpacesを選択します ）。
   - 管理コマンドプロンプトから、gpupdate /force と入力します。

ディレクトリ WorkSpaces にインターネットに接続できない

WorkSpaces デフォルトでは、 はインターネットと通信できません。明示的にインターネットアクセスを許可する必要があります。詳細については、「WorkSpaces Personal でのインターネットアクセス」を参照してください。

インターネットアクセスを失 WorkSpace った

WorkSpace がインターネットにアクセスできなくなり、 WorkSpace を使用して に接続RDPできない場合、この問題はおそらく のパブリック IP アドレスが失われたことが原因です WorkSpace。ディレクトリレベルで Elastic IP アドレスの自動割り当てを有効にしている場合、Elastic IP アドレス (Amazon が提供するプールから) は、起動 WorkSpace 時に に割り当てられます。ただし、所有している Elastic IP アドレスを に関連付け WorkSpace、後でその Elastic IP アドレスを から関連付

け解除すると WorkSpace、 はパブリック IP アドレス WorkSpace を失い、Amazon が提供するプールから新しい IP アドレスを自動的に取得しません。

Amazon が提供するプールから新しいパブリック IP アドレスを に関連付けるには WorkSpace、 を再構築 WorkSpaceする必要があります。を再構築しない場合は WorkSpace、所有する別の Elastic IP アドレスを に関連付ける必要があります WorkSpace。

WorkSpace の起動後に 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 に割り当てられると WorkSpace、 は同じパブリック IP アドレス WorkSpace を保持します (WorkSpace が再構築されない限り、新しいパブリック IP アドレスを取得します)。

オンプレミスディレクトリに接続しようとすると、DNS「使用不可」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、TCPUDPポート 53 経由でオンプレミス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とオンプレミスのファイアウォールで、このポートを介した TCPおよびUDP通信が許可され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TCPUDPポートを介してオンプレミスの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とオンプレミスのファイアウォールで、次のポートを介した TCPおよび UDP 通信が許可され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「レコード」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。このエラーは、サービスがディレクトリへの接続時に指定したDNSサーバーからこれらのレコードを取得できない場合に表示されます。DNS サーバーにこれらのSRVレコードが含まれていることを確認します。詳細については、「Microsoft のSRVリソースレコード」を参照してください TechNet。

Windows がアイドル状態のままになるとスリープ状態 WorkSpace になる

この問題を解決するには、 に接続 WorkSpace し、次の手順を使用して電源プランを高パフォーマンスに変更します。

1. から WorkSpaceコントロールパネルを開き、ハードウェアを選択するか、ハードウェアとサウンドを選択します (Windows のバージョンによって名前が異なる場合があります)。
2. [Power Options (電源オプション)] で [Choose a power plan (電源プランを選択)] を選択します。
3. [Choose or customize a power plan] (電力プランの選択あるいはカスタマイズ) ペインで [High performance] (高パフォーマンス) 電力プランを選択し、[Change plan settings] (プラン設定の変更)を選択します。
   - オプションで、[High performance](高パフォーマンス) 電力プランの選択が無効になっている場合は、[現在利用できない設定を変更する] を選択してから、[高パフォーマンス] 電力プランを選択します。
   - そのファイルに[高パフォーマンス]プランが非表示になっている場合は、[追加プランを表示]の右側にある矢印を選択して表示するか、もしくは左のナビゲーションで[電源プランを作成する]から[高パフォーマンス]を選択し、電源プランに名前を付けたうえで、[次へ] を選択します。
4. [プランの設定を変更する:高パフォーマンス]ページでは、[ディスプレイをオフにする]および (利用可能な場合) [コンピュータをスリープ状態にする]などについて[Never](決してしない) を選択してあることを確認してください。

5. 高パフォーマンスプランに変更した場合は、[変更の保存] を選択します。(または新しいプランを作成するのであれば[作成]を選択します)。

上記の手順で問題を解決できない場合は、次の操作を行います。

1. から WorkSpaceコントロールパネルを開き、ハードウェアを選択するか、ハードウェアとサウンドを選択します (Windows のバージョンによって名前が異なる場合があります) 。
2. [Power Options (電源オプション)] で [Choose a power plan (電源プランを選択)] を選択します。
3. [Choose or customize a power plan] (電力プランの選択あるいはカスタマイズ) ペインで、[High performance] (高パフォーマンス) 電源プランの右側にある [Change plan settings] (プラン設定の変更) リンクを選択して、[Change advanced power settings] (高度な電源設定の変更) リンクを選択します。
4. 設定リストの [Power Options (電源オプション)] ダイアログボックスで、[Hard disk (ハードディスク)] の左側にあるプラス記号を選択して関連する設定を表示します。
5. [Plugged in (プラグイン)] の [Turn off hard disk after (経過後にハードディスクを切断する)] 値が、[On battery (バッテリー使用時)] よりも大きいことを確認します (デフォルト値は 20 分)。
6. PCI Express の左側にあるプラス記号を選択し、Link State Power Management でも同じ操作を行います。
7. [Link State Power Management (ステート電力管理リンク)] 設定が [オフ] であることを確認します。
8. [OK] (あるいは、設定を変更した場合には [適用]) を選択して、ダイアログボックスを閉じます。
9. 設定を変更した場合には、[Change settings for the plan (プランの設定変更)] ペインで [変更の保存] を選択します。

の 1 つの状態 WorkSpaces が である UNHEALTHY

WorkSpaces サービスは定期的にステータスリクエストを に送信します WorkSpace。 WorkSpace はUNHEALTHY、これらのリクエストに応答できない場合にマークされます。この問題に対する一般的な原因は次のとおりです。

- 上のアプリケーション WorkSpace がネットワークポートをブロックしているため、 WorkSpace がステータスリクエストに応答できません。
- CPU 使用率が高い WorkSpace と、 がステータスリクエストにタイムリーに応答できなくなります。

- のコンピュータ名が変更され WorkSpace ました。これにより、 WorkSpaces と の間で安全なチャネルが確立されなくなります WorkSpace。

次の方法を使用して、この状況を修正するよう試みることができます。

- WorkSpaces コンソール WorkSpace から を再起動します。
- 次の手順 WorkSpace を使用して異常のある に接続します。これはトラブルシューティングの目的にのみ使用してください。

  1. 異常がある と同じディレクトリ WorkSpace 内の運用 に接続します WorkSpace。
  2. オペレーションから WorkSpace、リモートデスクトッププロトコル (RDP) を使用して、異常のある の IP アドレス WorkSpace を使用して異常のある に接続します WorkSpace。問題の範囲によっては、異常のある に接続できない場合があります WorkSpace。
  3. 異常な場合は WorkSpace、ポートの最小要件が満たされていることを確認します。
- SkyLightWorkSpacesConfigService サービスがヘルスチェックに応答できることを確認します。この問題のトラブルシューティングについては、「ユーザーにWorkSpace 「ステータス: 異常」というメッセージが表示されます。に接続できませんでした WorkSpace。Please try again in a few minutes.」というメッセージが表示される。」を参照してください。
- WorkSpaces コンソール WorkSpace から を再構築します。を再構築 WorkSpace するとデータが失われる可能性があるため、このオプションは、他のすべての問題修正の試みが失敗した場合にのみ使用してください。

WorkSpace が予期せずクラッシュまたは再起動しています

用に WorkSpace 設定された PCoIPが繰り返しクラッシュまたは再起動していて、エラーログまたはクラッシュダンプが spacedeskHookKmode.sysまたは の問題を示している場合spacedeskHookUmode.dll、または次のエラーメッセージが表示されている場合は、 へのウェブアクセスを無効にする必要がある場合があります WorkSpace。

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - これらのトラブルシューティング手順は、 用に WorkSpaces 設定された には適用されませんDCV。これらは、 用に WorkSpaces 設定された にのみ適用されますPCoIP。
> - Web Access を無効にするのは、ユーザーに Web Access の使用を許可しない場合だけです。

へのウェブアクセスを無効にするには WorkSpace、 WorkSpaces ディレクトリでウェブアクセスを無効にして、 を再起動する必要があります WorkSpace。

同じユーザー名に複数の がありますが WorkSpace、ユーザーは の 1 つのみにログインできます。 WorkSpaces

まず を削除せずに Active Directory (AD) のユーザーを削除し、そのユーザーを Active Directory に再度追加してその WorkSpace ユーザーの新しい を作成する WorkSpace と、同じユーザー名が同じディレクトリ WorkSpaces に 2 つの を持つようになります。ただし、ユーザーが元の に接続しようとすると WorkSpace、次のエラーが表示されます。

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

さらに、Amazon WorkSpaces コンソールでユーザー名を検索すると WorkSpace、両方 WorkSpaces がまだ存在する場合でも、新しい のみが返されます。(ユーザー名の代わりに WorkSpace ID を検索 WorkSpace することで、元の を見つけることができます)。

この動作は、Active Directory のユーザーの名前を最初に削除せずに変更した場合にも発生する可能性があります WorkSpace。次に、ユーザー名を元のユーザー名に戻し、 WorkSpace ユーザーの新しい を作成すると、同じユーザー名が ディレクトリ WorkSpaces に 2 つ含まれます。

この問題は、Active Directory がユーザー名ではなくユーザーのセキュリティ識別子 (SID) を使用してユーザーを一意に識別するため発生します。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SID、ユーザーに新しい が割り当てられます。ユーザー名の検索中、Amazon WorkSpaces コンソールは SIDを使用して Active Directory で一致を検索します。また、Amazon WorkSpaces クライアントは を使用してSID、接続先のユーザーを識別します WorkSpaces。

この問題を解決するには、以下のいずれかの操作を行います。

- ユーザーが削除されて Active Directory で再作成されたためにこの問題が発生した場合は、Active Directory のごみ箱機能を有効にすると、削除された元のユーザーオブジェクトを復元できる可能性があります。元のユーザーオブジェクトを復元できる場合は、ユーザーが元のユーザーオブジェクトに接続できることを確認します WorkSpace。可能な場合は、手動でバックアップし、新しいから元の WorkSpace（ 必要に応じて) WorkSpace にユーザーデータを転送した後に、新しい を削除 WorkSpaceできます。
- 元のユーザーオブジェクトを復元できない場合は、ユーザーの元のオブジェクトを削除します WorkSpace。ユーザーは に接続し、 WorkSpace 代わりに新しい を使用できます。必ず、元の から新しい WorkSpace にユーザーデータを手動でバックアップして転送してください WorkSpace。

> **Warning**
>
> の削除 WorkSpace は永続的なアクションであり、元に戻すことはできません。WorkSpace ユーザーのデータは保持されず、破棄されます。ユーザーデータのバックアップに関するヘルプについては、 AWS サポートにお問い合わせください。

Amazon での Docker の使用に問題がある WorkSpaces

Windows WorkSpaces

ネストされた仮想化 (Docker の使用を含む) は Windows ではサポートされていません WorkSpaces。詳細については、「Docker ドキュメント」を参照してください。

Linux WorkSpaces

Linux で Docker を使用するには WorkSpaces、Docker で使用されるCIDRブロックが、 に関連付けられた 2 つの Elastic Network Interface (ENIs) で使用されるCIDRブロックと重複していないことを確認します WorkSpace。Linux での Docker の使用で問題が発生した場合は WorkSpaces、Docker にお問い合わせください。

一部のAPI通話に ThrottlingException エラーが表示される

呼び出しの WorkSpaces APIデフォルトの許容レートは、1 秒あたり 2 回のAPI呼び出しの一定のレートで、最大許容「バースト」レートは 1 秒あたり 5 回のAPI呼び出しです。次の表は、APIリクエストに対するバーストレート制限の仕組みを示しています。

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。つまり、3 つのAPI呼び出しのいずれかがスロットリングされます。1 つの調整された呼び出しは、短い遅延後に応答します。
6	0	1	5 秒目からの呼び出しの 1 つが 6 秒目で再試行されるため、6 秒目の追加の呼び出しは 1 つだけです。これは、1 秒あたり 2 回の呼び出しが一定のレート制限であるためです。
7	0	3	キューにスロットリングされたAPI呼び出しがなくなったため、レート制限は引き続き増加し、バーストレート制限の 5 コールまで増加します。
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。

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
9	0	5	8 秒目には呼び出しが発行されませんが、レート制限は 5 つを超えることはありません。

バックグラウンドで実行させると切断され WorkSpace 続ける

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 フェデレーションは機能しません。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。

これは、2SAML.0 フェデレーションIAMロール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 Amazon リソースネーム () からストリーミングするアクセス許可が含まれていないために発生する可能性がありますARN。IAM ロールは、 WorkSpaces ディレクトリにアクセスするフェデレーティッドユーザーによって引き受けられます。ロールのアクセス許可を編集して ディレクトリを含めARN、ユーザーが ディレクトリ WorkSpace に を持っていることを確認します。詳細については、「 SAML2.0 Authentication and Troubleshooting SAML 2.0 Federation with AWS」を参照してください。

ユーザーは 60 分ごとに WorkSpaces セッションから切断されます。

ID プロバイダー (IdP) に応じて WorkSpaces、SAML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、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、必要に応じて 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 2SAML.0 ID プロバイダー (IdP) によって開始されたフローを使用してフェデレーションする場合、または IdP にフェデレーションした後にユーザーがクライアントからサインインしようとするたびに WorkSpaces 、クライアントアプリケーションの追加のインスタンスが起動すると、リダイレクトURIエラーが発生します。

このエラーは、リレーステートURLが有効ではないために発生します。IdP フェデレーション設定のリレーステートが正しいこと、および WorkSpaces ディレクトリプロパティの IdP フェデレーションに対してユーザーアクセスURLとリレーステートのパラメータ名が正しく設定されていることを確認します。それらが有効で、問題が解決しない場合は、 AWS サポートにお問い合わせください。詳細については、「SAML のセットアップ」を参照してください。

ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインイン WorkSpaceしようとすると、「Something went wrong: An error occurred while launching your」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 値は WorkSpaces ユーザー名と一致する必要があり、通常は Active Directory ユーザーの sAMAccountName 属性と同じです。さらに、 属性が に設定されている `PrincipalTag:Email` Attribute 要素は、 WorkSpaces ディレクトリで定義されている WorkSpaces ユーザーの E メールアドレスと一致する`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`必要があります。詳細については、「SAML のセットアップ」を参照してください。

ユーザーが IdP にフェデレーションした後に WorkSpaces クライアントアプリケーションにサインインしようとすると、「タグを検証できません」というメッセージが表示されます。

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`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`。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および でのタグ付けのルール 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、 1.2 TLS を有効にしない場合に発生する可能性があります。

マイクまたはウェブカメラが Windows で動作していません WorkSpaces。

[Start] (スタート) メニューを開いてプライバシー設定を確認してください

- [Start] (スタート) > [Settings] (設定) > [Privacy] (プライバシー) > [Camera] (カメラ)
- [Start] (スタート) > [Settings] (設定)> [Privacy] (プライバシー) > [Microphone] (マイク)

オフになっている場合は、オンにします。

または、 WorkSpaces 管理者はグループポリシーオブジェクト (GPO) を作成して、必要に応じてマイクやウェブカメラを有効にすることもできます。

ユーザーは証明書ベースの認証を使用してログインできず、デスクトップセッションに接続するときに 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 クライアントはサポートされていません。証明書ベースの認証は、最新の Windows クライアントアプリケーションを使用するDCVバンドル WorkSpaces の WorkSpaces Windows でサポートされています。
- WorkSpaces ディレクトリで証明書ベースの認証を有効にした後、 を再起動 WorkSpaces する必要があります。
- WorkSpaces が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 (24 時間) 前にキャッシュをクリア Support するには、 にお問い合わせください。詳細については、Support センターを参照してください。
- `UserPrincipalName` SAML 属性の userPrincipalName 形式が正しくフォーマットされていないか、ユーザーの実際のドメインに解決されません。詳細については、「前提条件」のステップ 1 を参照してください。
- SAML アサーションの (オプション) `ObjectSid` 属性が、SAML_Subject で指定されたユーザーの Active Directory セキュリティ識別子 (SID) と一致しません`NameID`。SAML フェデレーションで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ます。
- スマートカードログオンのデフォルトの Active Directory 設定を変更したり、スマートカードがスマートカードリーダーから取り外された場合にアクションを実行したりするグループポリシー設定があります。これらの設定により、上記のエラー以外にも予期しない動作が発生する可能性があります。証明書ベースの認証では、仮想スマートカードがインスタンスのオペレーティングシステムに提示され、ログオンの完了後にそれが削除されます。「Primary Group Policy settings for smart cards」(スマートカードのプライマリグループポリシー設定) と「Additional smart card Group Policy settings and registry keys」(その他のスマートカードのグループポリシー設定とレジストリキー) (スマートカード取り出し時の動作を含む) を参照してください。
- プライベート CA のCRLディストリビューションポイントはオンラインではなく、 WorkSpaces またはドメインコントローラーから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CAsに古いものがあるかどうかを確認するには、CA `PKIVIEW.msc`でを実行して確認します。古い がある場合はCAs、`PKIVIEW.mscmmc` 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。

その他のトラブルシューティング手順には、 WorkSpaces インスタンスの Windows イベントログの確認が含まれます。ログオンの失敗を確認する一般的なイベントは、Windows セキュリティログの「イベント 4625: アカウントがログオンに失敗しました」です。

問題が解決しない場合は、 にお問い合わせください Support。詳細については、Support センターを参照してください。

Windows インストールメディアを必要とするが、提供 WorkSpaces していない操作を実行しようとしています。

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、EC2必要に応じて Amazon が提供する Windows Server OS インストールメディアEBSスナップショットを使用できます。

これらのスナップショットから EBSボリュームを作成し、Amazon にアタッチしてEC2、必要に応じてファイルを WorkSpace に転送します。BYOL で Windows 10 を使用して WorkSpaces いて、インストールメディアが必要な場合は、独自のインストールメディアを準備する必要があります。詳細については、「インストールメディアを使用した Windows コンポーネントの追加」を参照してください。EBS ボリュームを に直接アタッチすることはできないため WorkSpace、Amazon EC2インスタンスにアタッチしてファイルをコピーする必要があります。

サポートされていない WorkSpaces リージョンで作成された既存の AWS Managed Directory WorkSpaces で を起動したい。

現在 でサポートされていないリージョンのディレクトリ WorkSpaces を使用して Amazon を起動するには WorkSpaces、以下の手順に従います。

> **Note**
>
> AWS Command Line Interface コマンドの実行中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VPC内の別の と仮想プライベートクラウド (VPC) ピアリングを作成する

1. 別のリージョンVPCの とのVPCピアリング接続を作成します。詳細については、「Create with VPCs in the same account and different Regions」を参照してください。
2. VPC ピアリング接続を受け入れます。詳細については、VPC「ピア接続を受け入れる」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 を使用してVPCピアリング接続を表示できますAPI。

ステップ 2: 両方のリージョンでVPCピアリング用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 VPCを介したピアとの通信を有効にしますIPv6。詳細については、VPC「ピアリング接続のルートテーブルを更新する」を参照してください。

ステップ 3: AD Connector を作成して Amazon を登録する WorkSpaces

1. AD Connector の前提条件を確認するには、「AD Connector の前提条件」を参照してください。
2. 既存のディレクトリを AD Connector と接続します。詳細については、「AD Connector を作成する」を参照してください。
3. AD Connectorのステータスが [アクティブ] に変わったら、AWS Directory Service コンソールを開き、ディレクトリ ID のハイパーリンクを選択します。
4. AWS アプリケーションとサービスの場合は、Amazon WorkSpaces を選択して、このディレクトリ WorkSpaces で のアクセスを有効にします。
5. ディレクトリを に登録します WorkSpaces。詳細については、「 ディレクトリの登録 WorkSpaces」を参照してください。

Amazon Linux 2 で Firefox をアップデートしたいと考えています。

ステップ 1: 自動更新が有効になっていることを確認する

自動更新が有効になっていることを確認するには、 `systemctl status *os-update-mgmt.timer | grep enabled`で コマンドを実行します WorkSpace。出力に、`enabled` という単語を含む行が 2 行あるはずです。

ステップ 2: 更新を開始する

Firefox は通常、メンテナンスウィンドウ中に、Amazon Linux 2 WorkSpaces でシステム内の他のすべてのソフトウェアパッケージとともに自動的に更新されます。ただし、これは WorkSpaces 使用している のタイプによって異なります。

- の場合 AlwaysOn WorkSpaces、毎週のメンテナンスウィンドウは日曜日の 00:00 から 04:00 のタイムゾーンになります WorkSpace。
- For AutoStop WorkSpaces. は、その月の第 3 月曜日から最大 2 週間、メンテナンスウィンドウは、 の AWS リージョンのタイムゾーンで毎日午前 0 時から午前 5 時まで開かれます WorkSpace。

メンテナンスウィンドウの詳細については、WorkSpace「メンテナンス」を参照してください。

を再起動 WorkSpaceし、15 分後に再接続することで、即時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パッケージバージョンの 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yumdownloader firefoxで コマンドを実行することで、Amazon Linux 2 リポジトリから必要なRPMパッケージをダウンロードすることもできます。次に、リポジトリを にサイドロードします。ここでは WorkSpaces、 などの標準YUMコマンドを使用してリポジトリをインストールできますsudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm。

> **Note**
>
> 正確なファイル名は、パッケージのバージョンによって変わります。

ステップ 3: Firefox リポジトリが使用されていることを確認する

Amazon Linux Extras は、Amazon Linux 2 の Firefox 更新を自動的に提供します WorkSpaces。2023 年 7 月 31 日以降に WorkSpaces 作成された Amazon Linux 2 では、Firefox Extra リポジトリが既に有効になっています。 WorkSpace が Firefox Extra リポジトリを使用していることを確認するには、次のコマンドを実行します。

```
yum repolist | grep amzn2extra-firefox
```

コマンド出力は、Firefox Extra リポジトリが使用されている場合、amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10 と類似したものになります。Firefox Extra リポジトリが使用されていない場合は、空になります。Firefox Extra リポジトリが使用されていない場合は、次のコマンドを使用して手動でアクティブ化を試みることができます。

```
sudo amazon-linux-extras install firefox
```

Firefox Extra リポジトリのアクティベーションが引き続き失敗する場合は、インターネットアクセスを確認し、VPCエンドポイントが設定されていないことを確認します。Amazon Linux 2 WorkSpaces via YUMリポジトリの Firefox 更新を引き続き受信するには、 WorkSpaces が Amazon Linux 2 リポジトリに到達できることを確認します。インターネットに接続することなく Amazon Linux 2 リポジトリにアクセスする方法の詳細については、こちらのナレッジセンター記事を参照してください。

ユーザーは、 WorkSpaces クライアントを使用してパスワードをリセットできます。設定されているきめ細かなパスワードポリシー (FFGP) の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。

組織で強制する必要がある場合はFFGP WorkSpaces、Active Directory 管理者に連絡して、WorkSpaces クライアントではなく Active Directory から直接ユーザーのパスワードをリセットしてください。

ユーザーに「これは Web Access OS/platform is not authorized to access your WorkSpace" when trying to access the Windows/Linux WorkSpace を使用しています

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は、 WorkSpaces Web Access と互換性がありません。 WorkSpace ディレクトリのその他のプラットフォーム設定でウェブアクセスを有効にしていることを確認してください。のウェブアクセスを有効にする方法の詳細については、 WorkSpace「」を参照してください WorkSpaces Personal の WorkSpaces ウェブアクセスを有効にして設定する。

停止状態の に接続した後、ユーザーの AutoStop WorkSpace が異常と WorkSpace 表示される

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。たとえば、 WorkSpace に 1.1 NPCAP 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。

DCV WorkSpaces Personal のホストエージェントバージョン

DCV ホストエージェントは、 内で実行されるホストエージェントです WorkSpace。のピクセルをクライアントアプリケーション WorkSpace にストリーミングし、双方向のオーディオとビデオ、印刷などのセッション内機能が含まれています。の詳細についてはDCV、「Amazon のプロトコル WorkSpaces」を参照してください。

ホストエージェントソフトウェアは常に最新バージョンに更新しておくことをお勧めします。を手動で再起動 WorkSpaces して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 デフォルトのメンテナンスウィンドウ中に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「メンテナンス」を参照してください。これらの機能には、最新の WorkSpaces クライアントバージョンが必要です。最新のクライアントバージョンの詳細については、WorkSpaces「 クライアント」を参照してください。

次の表に、 WorkSpaces Personal のDCVホストエージェントの各バージョンの変更を示します。

リリース	日付	変更
• 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	• ストリーミングプロトコル (WSP) WorkSpaces の名前を Amazon に変更しましたDCV。 • "" アプリケーションを使用しているお客様向けのDCVエージェントのオーディオダックの問題を修正しました。

リリース	日付	変更
		• 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 SmartCard ログインの問題を修正しました。 • Chrome ブラウザでの最初のログイン試行時の WebAuthn リダイレクトの問題を修正しました。 • 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 Identity Center (IdC) との統合のサポートが追加されました。 • パフォーマンス向上とバグ修正が行われています。
• 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。 • Amazon Connect のウェブRTCリダイレクトサポートが追加されました。 • 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。 • 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。 • アイドル切断タイムアウトを設定する新しいグループポリシー設定を追加しました。 • ユーザーが表示設定を変更したときに WorkSpaces が切断され、白画面が表示される問題を修正しました。 • パフォーマンス向上とバグ修正が行われています。
• 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。 • 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 Google Chrome または Microsoft Edge ブラウザで実行されているウェブアプリケーションからのセッション内 WebAuthn リダイレクトリクエストのサポートが追加されました。この機能は、ユーザーにDCV WebAuthn リダイレクト拡張機能を有効にするよう求める 1 回限りのブラウザプロンプトを追加します。Windows WorkSpaces および WorkSpaces ネイティブクライアントでのみサポートされています。 • ログイン時に白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。 • 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。 • 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 以降の間接ディスプレイドライバー (IDD) のサポートが追加されました。これにより、CPU消費が減少し、ストリーミングパフォーマンスが向上します。 • IDD ドライバーを有効または無効にする新しいグループポリシー設定を追加しました。 • クリップボードイメージの透過性に関連するバグを修正しました。 • 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。 • 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 VSyncに のサポートが追加されました。 • 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VSync。 • 再接続と信頼性の問題を改善しました。 • パフォーマンス向上とバグ修正が行われています。

リリース	日付	変更
• Amazon Linux WorkSpaces - 2.0.0.1086 • Ubuntu WorkSpaces - 2.1.0.1086	2023 年 8 月 18 日	• タイムゾーンのリダイレクトを有効または無効にするための新しい設定を追加しました。 • ログオンタイムアウトを延長し、設定オプションを追加しました。 • 中断後の再接続を迅速に行うことができるようにゲートウェイが改善されました。 • パフォーマンス向上とバグ修正が行われています。
• Amazon Linux WorkSpaces - 2.0.0.907	2023 年 6 月 30 日	• DCV 拡張機能のサポートが追加されSDK、 ISV固有の統合が可能になりました。 • ログアウトするとユーザーのセッションが終了するように切断動作を変更しました。 • タイムゾーンのリダイレクトのサポートを追加しました。 • ログオンタイムアウトを延長し、設定オプションを追加しました。 • アップグレードの問題を修正しました。 • パフォーマンス向上とバグ修正が行われています。
• Windows WorkSpaces - 2.0.0.829	2023 年 6 月 8 日	• ログアウトするとユーザーのセッションが終了するように切断動作を変更しました。 • A/V 同期と日本語キーボードに関するバグを修正しました。 • 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。 • DCV 拡張機能のサポートが追加されSDK、 ISV固有の統合が可能になりました。 • タイムゾーンのリダイレクトのサポートを追加しました。 • アップグレードの問題を修正しました。
• Windows WorkSpaces - 2.0.0.799	2023 年 5 月 8 日	• イメージ品質とパフォーマンスの最適化により、 UDPベースのQUICトランスポートを強化しました。 • DCV 拡張機能のサポートが追加されSDK、 ISV固有の統合が可能になりました。 • 拡張機能 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SDK。 • 韓国語、日本語、およびドイツ語のキーボードレイアウトを改善しました。 • セッションフリーズの問題、ハードウェアアクセラレーション、プリンタのリダイレクト、ログの冗長性、および target-fps グループポリシー設定に関連するバグを修正しました。

Note

- ホストエージェントのバージョンを確認する方法については、「 の最新バージョンでサポートされているクライアントおよびホストオペレーティングシステムDCV」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、「 が既にある場合はDCV WorkSpace、どのように更新すればよいですか？」を参照してください。
- 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、DCV 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」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」の WorkSpaces 「Windows クライアントアプリケーション」セクションの「リリースノート」を参照してください。

WorkSpaces プールの使用と管理

WorkSpaces プールは、エフェメラルインフラストラクチャでホストされている高度にキュレーションされたデスクトップ環境にアクセスする必要があるユーザー向けに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 プールの および アベイラビリティーゾーン
- WorkSpaces プールのディレクトリを管理する
- WorkSpaces プールのネットワークとアクセス
- WorkSpaces プールを作成する
- WorkSpaces プールの管理
- WorkSpaces プールでの Active Directory の使用
- WorkSpaces プールのバンドルとイメージ
- WorkSpaces Pools のモニタリング
- WorkSpaces プールの永続的ストレージの有効化と管理
- WorkSpaces プール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 のトラブルシューティング通知コード

AWS リージョン WorkSpaces プールの および アベイラビリティーゾーン

WorkSpaces プールは以下で利用できます 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 workspaces-fips.us-east-1.amazonaws.com	HTTPS HTTPS	use1-az2、use1-az4、use1-az6	
米国西部 (オレゴン)	us-west-2	workspaces.us-west-2.amazonaws.com workspaces-fips.us-west-2.amazonaws.com	HTTPS 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
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 workspaces-fips.us-gov-east-1.amazonaws.com	HTTPS HTTPS	usgw1-az1、usgw1-az2、usgw1-az3
AWS GovCloud (米国西部)	us-gov-west-1	workspaces.us-gov-west-1.amazonaws.com workspaces-fips.us-gov-west-1.amazonaws.com	HTTPS HTTPS	usge1-az1、usge1-az2、usge1-az3

WorkSpaces プールのディレクトリを管理する

WorkSpaces プールは ディレクトリを使用して、 およびユーザーの情報を保存 WorkSpaces および管理します。このセクションでは、 WorkSpaces プール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

- 2.0 SAML を設定し、 WorkSpaces プールディレクトリを作成する
- WorkSpaces プールのディレクトリの詳細を更新する
- WorkSpaces プールディレクトリの登録を解除する

2.0 SAML を設定し、 WorkSpaces プールディレクトリを作成する

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 プール WorkSpaces 内の SAML 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 2.0 ID SAML プロバイダー (IdP) を設定し、有効にします AWS。これにより、フェデレーティッドユーザーに WorkSpace プールディレクトリへのアクセスが許可されます。リレーステートは、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 AWS。

> **Important**
>
> WorkSpaces プールは IP ベースの 2.0 SAML 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
- ステップ 2: 前提条件を完了させる
- ステップ 3: で SAML ID プロバイダーを作成する IAM
- ステップ 4: WorkSpace プールディレクトリを作成する
- ステップ 5: 2.0 SAML フェデレーションIAMロールを作成する
- ステップ 6: 2.0 ID SAML プロバイダーを設定する
- 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
- 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
- ステップ 9: WorkSpace プールディレクトリで SAML 2.0 との統合を有効にする
- トラブルシューティング
- WorkSpaces プールディレクトリの Active Directory の詳細を指定する

ステップ 1: 要件を考慮する

WorkSpaces Pools ディレクトリSAMLに を設定する場合、次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 高速セットアップを使用するか、 WorkSpace を使用して を以前に起動したときに自動的に作成されます AWS Management Console。これは、ユー

ザーに代わって特定の AWS リソースにアクセスする許可を Amazon WorkSpaces に付与します。ロールが既に存在する場合は、管理ポリシーをアタッチする必要がある場合があります。 AmazonWorkSpacesPoolServiceAccessこれは、Amazon が WorkSpaces プールの AWS アカウント内の必要なリソースにアクセス WorkSpaces するために使用します。詳細については、workspaces_DefaultRole Role を作成するおよびAWS 管理ポリシー: AmazonWorkSpacesPoolServiceAccessを参照してください。

- 機能 AWS リージョン をサポートする で WorkSpaces プールの SAML 2.0 認証を設定できます。詳細については、「AWS リージョン WorkSpaces プールの および アベイラビリティーゾーン」を参照してください。
- で SAML2.0 認証を使用するには WorkSpaces、IdP はディープリンクターゲットリソースまたはリレーステートエンドポイント SSOで開始された未承諾 IdP をサポートする必要がありますURL。これ IdPs をサポートする の例には、ADFS、Azure AD、"" Single Sign-On、Okta PingFederate、 などがあります PingOne。詳細については、IdP のユーザードキュメントを参照してください。
- SAML 2.0 認証は、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 Client Download 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 プールディレクトリへの SAML 2.0 IdP 接続を設定する前に、次の前提条件を完了してください。

- 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、 にアクセスIAMするための IdP と の統合が含まれます AWS Management Console。
- 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。この署名付き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。このファイルを、後でIAMコンソールからアクセスできる場所に保存します。
- WorkSpaces コンソールを使用して WorkSpaces プールディレクトリを作成します。詳細については、「 WorkSpaces プールでの 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の WorkSpaces プールを作成します。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: で SAML ID プロバイダーを作成する IAM

開始するには、 で SAML IdP を作成する必要がありますIAM。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 プロバイダーの作成と管理」を参照してください。SAML IdPs での の使用の詳細については AWS GovCloud (US) Regions、 AWS GovCloud (US) ユーザーガイドAWS Identity and Access Managementの「」を参照してください。

ステップ 4: WorkSpace プール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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [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. アプリケーションに必要なネットワークリソースにアクセスできる VPCと 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. でネットワークリンクの作成を WorkSpaces に許可するセキュリティグループを選択しますVPC。セキュリティグループは、 から WorkSpaces 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VPC。例えば、セキュリティグループがすべてのインバウンドHTTPS接続を制限している場合、ウェブポータルにアクセスするユーザーは からHTTPSウェブサイトをロードできません WorkSpaces。

8. [Active Directory 設定] セクションはオプションです。ただし、 WorkSpaces プールで AD を使用する予定がある場合は、プールディレクトリの作成時に Active Directory (AD) WorkSpaces の詳細を指定する必要があります。 WorkSpaces プールディレクトリの作成後に Active Directory Config を編集することはできません。 WorkSpaces プールディレクトリの AD の詳細を指定する方法の詳細については、「」を参照してください WorkSpaces プールディレクトリの Active Directory の詳細を指定する。そのトピックで説明されているプロセスを完了したら、このトピックに戻り、 WorkSpaces プールディレクトリの作成を完了する必要があります。

   WorkSpaces プールで AD を使用する予定がない場合は、Active Directory Config セクションをスキップできます。

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。新しいロールを作成するには、新しいIAMロールの作成を選択します。

    アカウントから WorkSpace プールディレクトリに IAMロールを適用すると、 AWS 認証情報を手動で管理しなくても、 WorkSpace プール WorkSpace 内の からリクエストを行うことができます AWS API。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の作成」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: 2.0 SAML フェデレーションIAMロールを作成する

IAM コンソールで 2.0 SAML フェデレーションIAMロールを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで [ロール] を選択します。
3. [Create role] を選択します。
4. 信頼されたエンティティタイプの SAML 2.0 フェデレーションを選択します。
5. 2.0 SAML ベースのプロバイダーの場合は、「」で作成した ID プロバイダーを選択しますIAM。詳細については、「 で SAML ID プロバイダーを作成するIAM」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。この値は、 の値を持つ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`persistent`。SAML:sub_type が永続的である場合、IdP は特定のユーザーからのすべてのSAMLリクエストで `NameID`要素に同じ一意の値を送信します。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] を選択します。
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. [信頼ポリシーを編集] を選択します。
16. 信頼ポリシーの編集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] を選択します。
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、 を選択しますJSON。
21. ポリシーエディタの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 プールディレクトリを作成した AWS リージョンのコードに置き換えます。
    - *<account-id>* を AWS アカウント ID に置き換えます。
    - *<directory-id>* を、前に作成したディレクトリの ID に置き換えます。これは コンソールで WorkSpaces取得できます。

    のリソースでは AWS GovCloud (US) Regions、 に次の形式を使用しますARN: `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. [Next (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: 2.0 ID SAML プロバイダーを設定する

2.0 SAML IdP によっては、サービスプロバイダー AWS として信頼するように IdP を手動で更新する必要がある場合があります。これを行うには、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。

場合によっては IdPs、更新がすでに設定されている可能性があります。すでに設定されている場合は、この手順を省略できます。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。一部のプロバイダーでは、ダッシュボードにURLXMLファイルの を入力するオプションがあり、IdP がファイルを取得してインストールします。それ以外の場合は、 からファイルをダウンロードしURL、ダッシュボードにアップロードする必要があります。

> **Important**
>
> 現時点では、IdP で設定したアプリケーションへのアクセス WorkSpacesを IdP のユーザーに許可することもできます。ディレクトリの WorkSpaces アプリケーションへのアクセスが許可されているユーザーには、 WorkSpace自動的に が作成されません。同様に、 が WorkSpace 作成されたユーザーには、 WorkSpaces アプリケーションへのアクセスは自動的に許可されません。SAML 2.0 認証 WorkSpace を使用して 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 が認証レスポンスの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 Subject NameID — サインインしてい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**
>
> ドメイン結合 WorkSpaces プールの場合、ユーザーのNameID値は、 を使用する domain\username形式sAMAccountName、 を使用する username@domain.com形式userPrincipalName、または のみの形式で指定する必要がありますuserName。sAMAccountName 形式を使用している場合は、NetBIOS 名または完全修飾ドメイン名 () を使用してドメインを指定できますFQDN。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 プールでの 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 に設定**persistent**) — IdP が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するpersistentように 値を設定します。ステップ 5: 2.0 SAML フェデレーションIAMロールを作成する 「」セクションで説明されているようにpersistent、 が SAMLsub_type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てください。
- **Attribute Name** 属性が https://aws.amazon.com/SAML/Attributes/Role に設定された 要素 — この要素には、ユーザーが IdP によってマッピングされる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。ロールと IdP は、 のカンマ区切りのペアとして指定されますARNs。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/ に設定された 要素 RoleSessionName — この要素には、 に発行される AWS 一時的な認証情報の識別子を提供するAttributeValue要素が 1 つ含まれていますSSO。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 () ですUPN。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 Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email に設定された 要素 — この要素には、ユーザーの E メールアドレスを提供する AttributeValue 要素が 1 つ含まれています。値は、 WorkSpaces ディレクトリで定義されている WorkSpaces ユーザーの E メールアドレスと一致する必要があります。タグ値には、文字、数字、スペース、および特殊文字 (_ . : / = + - @) の組み合わせを含めることができます。詳細については、「 AWS

Identity and Access Management ユーザーガイド」の「IAMおよび でのタグ付けのルール AWS STS」を参照してください。

- （オプション）**Attribute Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag：UserPrincipalName — この要素には、サインインしているuserPrincipalNameユーザーの Active Directory を提供する 1 つの AttributeValue 要素が含まれています。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と WorkSpaces 個人」を参照してください。
- （オプション）**Attribute Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag：ObjectSid（オプション）に設定された 要素 — 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) を提供する 1 つの AttributeValue 要素が含まれます。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 個人」を参照してください。
- （オプション）**Attribute Name** 属性が https://aws.amazon.com/SAML/Attributes/PrincipalTag:Domain に設定されている 要素 — この要素には、サインインするユーザーに Active Directory のDNS完全修飾ドメイン名 (FQDN) を提供する 1 つの AttributeValue 要素が含まれています。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 Name** 属性が https://aws.amazon.com/SAML/Attributes/ に設定されている 要素SessionDuration — この要素には、再認証が必要になる前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のままにできる最大時間を指定する 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。詳細については、「 AWS Identity and Access Management ユーザーガイドSAML SessionDurationAttribute」の「」を参照してください。

> **Note**
>
> SessionDuration はオプションの属性ですが、SAMLレスポンスに含めることをお勧めします。この属性を指定しない場合、セッション期間はデフォルト値の 3600秒 (60 分) に設定されます。 WorkSpaces デスクトップセッションは、セッション期間が終了すると切断されます。

これらの要素を設定する方法の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「認証レスポンスのSAMLアサーションの設定」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 プールディレクトリのリレーステート 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URL。による認証に成功すると AWS、ユーザーは WorkSpaces プール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認証レスポンスでリレーステートとして定義されます。

リレーステートURL形式は次のとおりです。

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

次の表に、2.0 WorkSpaces SAML 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 プール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
米国西部 (オレゴン) リージョン	workspaces.euc-sso.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

リージョン	リレーステートのエンドポイント
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
AWS GovCloud （ 米国西部 ）	workspaces.euc-sso.us-gov-west-1amazonaws-us-gov..com **Note** SAML IdPs での の使用の詳細については AWS GovCloud (US) Regions、AWS GovCloud （ 米国) ユーザーガイドの「Amazon WorkSpaces」を参照してください。

リージョン	リレーステートのエンドポイント
AWS GovCloud （ 米国東部 ）	workspaces.euc-sso.us-gov-east-1amazonaws-us-gov..com **Note** SAML IdPs での の使用の詳細については AWS GovCloud (US) Regions、AWS GovCloud （ 米国) 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 プールディレクトリで SAML 2.0 との統合を有効にする

WorkSpaces プールディレクトリSAMLの 2.0 認証を有効にするには、次の手順を実行します。

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [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. 編集 SAML 2.0 ID プロバイダーを選択します。
7. 「」ともSSO呼ばれるユーザーアクセス URLの場合URL、プレースホルダー値を IdP から SSOURL提供された 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。

   次の表は、アプリケーションのさまざまな ID プロバイダーに固有のユーザーアクセスURLsとディープリンクパラメータ名の一覧です。

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/idpinitia`

ID プロバイダー	パラメータ	ユーザーアクセス URL
		tedsignon.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
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>*

ID プロバイダー	パラメータ	ユーザーアクセス URL
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId= <sp-id>`
PingOne エンタープライズ向け	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid= <app-id>&idpid=<idp-id>`

9. [Save] を選択します。

> **Important**
>
> ユーザーから 2.0 SAML 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 を使用して終了することもできますAPI。

トラブルシューティング

以下の情報は、 WorkSpaces プール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。

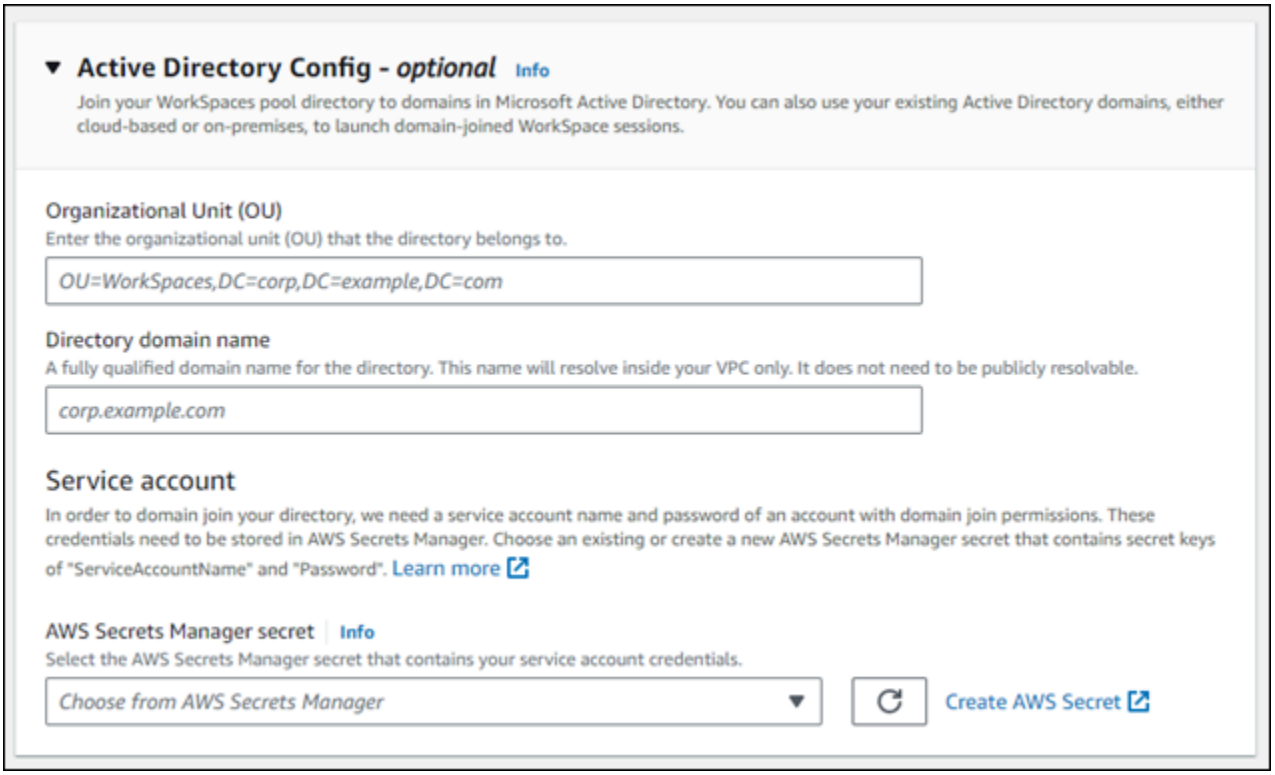
SAML 認証の完了後に WorkSpaces Pools クライアントで「ログインできません」というメッセージが表示される

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 E メール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 プールディレクトリの Active Directory の詳細を指定する

このトピックでは、 WorkSpaces コンソールの WorkSpaces 「プールの作成」ディレクトリページ内で Active Directory (AD) の詳細を指定する方法について説明します。 WorkSpaces プールディレクトリを作成するときに、 WorkSpaces プールで AD を使用する予定がある場合は、AD の詳細を指

定する必要があります。 WorkSpaces プールディレクトリの作成後に Active Directory Config を編集することはできません。以下は、 WorkSpaces プールの作成ディレクトリページの Active Directory Config セクションの例です。



> **Note**
>
> WorkSpaces プールディレクトリを作成する完全なプロセスについては、2.0 SAML を設定し、 WorkSpaces プールディレクトリを作成する「」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 プールディレクトリを作成するプロセス全体のステップのサブセットのみを示しています。

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

次の手順を実行して、 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します。

1. 組織単位には、プールが属する OU を入力します。 WorkSpace マシンアカウントは、WorkSpaces プール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 名を指定した場合、Active Directory ドメインに再参加しようとすると、 WorkSpaces はコンピュータオブジェクトを正しくサイクルできず、ドメイン再参加は機能しません。

2. ディレクトリドメイン名には、Active Directory ドメインの完全修飾ドメイン名 (FQDN) を入力します (例:)`corp.example.com`。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 プールディレクトリを Microsoft Active Directory のドメインに結合できます。また、クラウドベースのドメインまたはオンプレミスの既存の Active Directory ドメインを使用して、ドメイン結合を起動することもできます WorkSpaces。
   - また AWS Directory Service for Microsoft Active Directory、Active Directory ドメインの作成に AWS Managed Microsoft ADを使用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。
   - Active Directory ドメイン WorkSpaces に参加することで、次のことができます。
     - 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。
     - グループポリシー管理コンソール (GPMC) で使用可能な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します。
     - 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。
     - 企業のコンプライアンスとセキュリティポリシーを WorkSpaces ストリーミングインスタンスに適用します。

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

WorkSpaces プールの Active Directory (AD) をディレクトリ作成プロセスの一部として設定する場合は、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。これには、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。これは、 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を示します。

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. [完了] を選択します。

   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. で AWS Secrets Manager コンソールを開きますhttps://console.aws.amazon.com/secretsmanager/。
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 プールディレクトリの 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 「プールの作成」ディレクトリページの「Active Directory Config」セクション内のすべてのフィールドに入力できたので、 WorkSpaces プールディレクトリの作成を続行できます。「ステップ 4: WorkSpace プール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 プールのディレクトリの詳細を更新する

WorkSpaces プール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 プールに追加の認証オプションを設定できます。プールには 2.0 SAML 認証が必要です。

2.0 ID SAML プロバイダー認証を有効にして設定するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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. 編集 SAML 2.0 ID プロバイダーを選択します。
6. Enable SAML 2.0 authentication 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を入力して、フェデレーティッドサインイン中に WorkSpaces Pools クライアントに指示します。
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. [Save] 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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. ドロップダウンから AWS Certificate Manager （ ACM) プライベート認証機関 (CA) を選択します。
8. [Save] を選択します。

セキュリティグループ

ディレクトリの WorkSpaces プールにセキュリティグループを適用します。

WorkSpaces プールのセキュリティグループを設定するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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、Secrets Manager シー AWS 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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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 を選択したら、既存の を再構築 WorkSpaces して OU を更新します。詳細については、「 WorkSpaces Personal WorkSpace で を再構築する」を参照してください

6. [Save] 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

ユーザーがプールされたデバイス WorkSpace とローカルデバイス間で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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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. [Save] を選択します。

IAM ロール

WorkSpaces プール用の IAMロールを選択します。

IAM ロールを選択するには

1. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 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ロールの作成を選択します。
6. [Save] を選択します。

[タグ]

WorkSpaces プールに新しいタグを追加する

新しいタグを追加するには

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

3. 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 プールのネットワークとアクセス

以下のトピックでは、ユーザーが WorkSpaces プールに接続し、 WorkSpaces プールがネットワークリソースとインターネットにアクセスできるようにする方法について説明します。

内容

- WorkSpaces プールのインターネットアクセス
- WorkSpaces プールVPCの を設定する
- WorkSpaces プール機能に Amazon S3 VPCエンドポイントを使用する
- WorkSpaces プールVPCの への接続
- WorkSpaces プールへのユーザー接続

WorkSpaces プールのインターネットアクセス

WorkSpaces プール WorkSpaces の に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 人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、プライベートサブネットとNATゲートウェイVPCを使用して を設定します。
- デプロイでサポートされる同時ユーザー数が 100 人未満の場合は、パブリックサブネットVPCを使用して新規または既存のユーザーを設定できます。
- デプロイでサポートされる同時ユーザー数が 100 人未満で、 WorkSpaces プールを初めて使用し、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、および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とNATゲートウェイVPCを使用して 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、 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VPC。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。

さらに、インターネットアクセスを有効にするためにデフォルトのインターネットアクセスオプションを使用する設定とは異なり、NAT設定は WorkSpaces プール WorkSpaces の 100 個に制限されません。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VPCで使用する新しい を作成して設定するか、既存の にNATゲートウェイを追加できますVPC。

- パブリックサブネットVPCを使用して新規または既存の を設定する — この設定では、パブリックサブネットで WorkSpaces プールを起動します。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 を作成するVPCか、既存のものを設定できます。

  > **Note**
  >
  > パブリックサブネットVPCを使用して新規または既存の を設定すると、 WorkSpaces プールでは最大 100 WorkSpaces がサポートされます。デプロイで 100 人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。

- デフォルトの VPC、パブリックサブネット、およびセキュリティグループを使用する — WorkSpaces プールを初めて使用し、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 プールを起動できます。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VPCsは、2013-12-04 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、 にアタッチされている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VPCも含まれています。

> **Note**
>
> デフォルトの VPC、パブリックサブネット、およびセキュリティグループを使用する場合、 WorkSpaces プールでは最大 100 WorkSpaces がサポートされます。デプロイで 100 人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 プールVPCの を設定する

WorkSpaces プールを設定するときは、仮想プライベートクラウド (VPC) と、 を起動するサブネットを少なくとも 1 つ指定する必要があります WorkSpaces。VPC は、Amazon Web Services 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。サブネットは、VPC の IP アドレスの範囲です。

WorkSpaces プールVPCの を設定するときは、パブリックサブネットまたはプライベートサブネット、または両方のタイプのサブネットの組み合わせを指定できます。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

- VPC WorkSpaces プールの設定に関する推奨事項
- プライベートサブネットとNATゲートウェイVPCを使用して を設定する
- パブリックサブネットVPCを使用して新規または既存の を設定する
- デフォルトの VPC、パブリックサブネット、およびセキュリティグループを使用する

VPC WorkSpaces プールの設定に関する推奨事項

WorkSpaces プールを作成するときは、 VPCと、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VPCすることで、 に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。さらに、効果的な WorkSpaces プールスケーリングをサポートする環境を設定するのに役立ちます。効果的な WorkSpaces プールスケーリングを使用すると、不要なリソースの使用量や関連コストを回避しながら、現在および予想される WorkSpaces ユーザーの需要を満たすことができます。

全体的なVPC設定

- VPC 設定が WorkSpaces プールのスケーリングニーズをサポートできることを確認します。

  WorkSpaces プールのスケーリングの計画を立てるときは、1 人のユーザーが 1 人必要であることに注意してください WorkSpaces。したがって、 WorkSpaces 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。このため、使用するインスタンスタイプごとに、 WorkSpaces がサポートVPCできる の数が、同じインスタンスタイプの予想される同時ユーザー数よりも多いことを確認してください。

- WorkSpaces プールアカウントのクォータ (制限とも呼ばれます) が、予想される需要をサポート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、 の Service Quotas コンソールを使用できますhttps://console.aws.amazon.com/servicequotas/。デフォルトの WorkSpaces プールクォータの詳細については、「」を参照してくださいAmazon WorkSpaces クォータ。

- WorkSpaces プール WorkSpaces の 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VPCを使用して 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 WorkSpaces の 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、インターネットがそれらとの接続を開始することはできません WorkSpaces。さらに、インターネットアクセスを有効にするためにデフォルトのインターネットアクセスオプションを使用する設定とは異なり、NAT設定は 100 を超える をサポートしています WorkSpaces。詳細については、「プライベートサブネットとNATゲートウェイVPCを使用して 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 プールは、 WorkSpaces プールの最大希望する容量と同じ数の 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。

  数千など、非常に大規模なデプロイの容量を計画する場合は WorkSpaces、同じリージョンでも使用されている Amazon EC2インスタンスの数を考慮してください。

サブネット

- に複数のプライベートサブネットを設定する場合はVPC、それぞれを別のアベイラビリティーゾーンに設定します。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 プールは 2 番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「」および「 のサブネットサイズ設定IPv4」を参照してください。
- VPC で を使用している場合はNAT、インターネットアクセス用のNATゲートウェイで少なくとも 1 つのパブリックサブネットを設定します。できれば 2 つに設定します。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。

  大規模な WorkSpaces プールのデプロイで耐障害性を高め、容量不足エラーが発生する可能性を減らすには、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、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、 に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VPCを使用すると、 WorkSpaces プール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または Amazon 、ライセンスサーバーFSx、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とNATゲートウェイVPCを使用して を設定する

WorkSpaces プール WorkSpaces の にインターネットへのアクセスを提供する場合は、 VPCに 2 つのプライベートサブネット WorkSpaces とパブリックサブネットのNATゲートウェイを設定することをお勧めします。NAT ゲートウェイVPCで使用する新しい を作成して設定するか、既存の にNATゲートウェイを追加できますVPC。その他のVPC設定の推奨事項については、「」を参照してくださいVPC WorkSpaces プールの設定に関する推奨事項。

NAT ゲートウェイは、プライベートサブネット WorkSpaces の 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サービスとの接続を開始できないようにします WorkSpaces。さらに、インターネットアクセスを有効にするためにデフォルトのインターネットアクセスオプションを使用する設定とは異なり WorkSpaces、この設定は 100 に制限されません WorkSpaces。

NAT ゲートウェイとこの設定の使用の詳細については、「Amazon VPCユーザーガイドNAT」の「パブリックサブネットVPCとプライベートサブネット (NAT) を使用したゲートウェイと」を参照してください。

内容

- 新しい を作成して設定する VPC
- 既存の にNATゲートウェイを追加する VPC
- WorkSpaces プールのインターネットアクセスを有効にする

新しい を作成して設定する VPC

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VPCを持つ 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、 のパブリックサブネットに自動的に作成されますVPC。

ウィザードを使用して初期設定を作成したらVPC、2 番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「パブリックサブネットとプライベートサブネット (NAT) を使用する」を参照してください。

> **Note**
>
> が既にある場合はVPC、既存の にNATゲートウェイを追加する VPC代わりに「」のステップを完了してください。

内容

- ステップ 1: Elastic IP アドレスの割り当て
- ステップ 2: 新しい を作成する VPC
- ステップ 3: 2 番目のプライベートサブネットの追加
- 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

ステップ 1: Elastic IP アドレスの割り当て

を作成する前にVPC、 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。で使用する Elastic IP アドレスを最初に割り当ててからVPC、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 アドレス」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。詳細については、Amazon EC2料金ページの「Elastic IP アドレス」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. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. ナビゲーションペインのネットワークとセキュリティで、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 IPs ペインの右上で、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 を作成する VPC

次の手順を実行して、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VPCを持つ新しい を作成します。

新しい を作成するには VPC

1. で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
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 を選択します。
4. ステップ 1: VPC設定を選択し、VPCパブリックサブネットとプライベートサブネットで を選択し、選択を選択します。
5. 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VPCで、 VPC を次のように設定します。
   - IPv4 CIDR ブロックには、 の IPv4CIDRブロックを指定しますVPC。
   - IPv6 CIDR ブロックの場合は、デフォルト値のIPv6CIDR「ブロックなし」のままにします。
   - VPC 名前には、 の一意の名前を入力しますVPC。
6. パブリックサブネットを次のように設定します。
   - パブリックサブネットの IPv4 CIDRで、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。
   - プライベートサブネットの IPv4 でCIDR、サブネットの CIDRブロックを指定します。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、 の Amazon VPCコンソールを使用して作成しますhttps://console.aws.amazon.com/vpc/。
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. サービスで、「s3」で終わるリスト内のエントリ (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) を選択します。
   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. DNS ホスト名を有効にする では、デフォルト値の Yes 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. [作成]VPC を選択します。
13. のセットアップには数分かかることに注意してくださいVPC。VPC を作成したら、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 を作成する VPC) では、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VPCを持つ 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、[Subnets (サブネット)] を選択します。
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. でVPC、前のステップでVPC作成した 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 ブロックには、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。例えば、最初のプライベートサブネットのIPv4CIDRブロック範囲が の場合`10.0.1.0/24`、新しいプライベートサブネット`10.0.2.0/24`に の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

を作成して設定したらVPC、次のステップを実行してルートテーブルの名前を指定し、以下を確認します。

- 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、インターネットトラフィックをインターネットゲートウェイにポイントする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がNATゲートウェイを指すように設定されています。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引き続き選択した状態で、ルートタブで、ローカルトラフィック用のルートが 1 つあり、他のすべてのトラフィックを のインターネットゲートウェイに

送信する別のルートがあることを確認しますVPC。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IPv4CIDRブロック (10.0.0/20 など)	ローカル	パブリックサブネットIPv4CIDRブロック内のIPv4アドレス宛てのリソースからのすべてのトラフィックは、 内でローカルにルーティングされますVPC。
他のすべてのIPv4アドレス宛てのトラフィック (例: 0.0.0.0/0	アウトバウンド (igw-*ID*)	他のすべてのIPv4アドレス宛てのトラフィックは、VPCウィザードによって作成されたインターネットゲートウェイ (によって識別されますigw-*ID*) 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IPv4CIDRブロック (10.0.0/20 など)	ローカル	パブリックサブネットIPv4CIDRブロック内のIPv4アドレス宛てのリソースからのすべてのトラフィックは、 内でローカルにルーティングされますVPC。

送信先	ターゲット	説明
他のすべてのIPv4アドレス宛てのトラフィック (例: 0.0.0.0/0	アウトバウンド (nat-*ID*)	他のすべてのIPv4アドレス宛てのトラフィックは、NATゲートウェイ (で識別) にルーティングされますnat-*ID*。
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) [pl-*ID* (com.amazonaws. *region*.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 (で識別) にルーティングされますvpce-*ID*。

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 プール WorkSpaces の がインターネットにアクセスできるようにするには、「」の手順を実行します WorkSpaces プールのインターネットアクセスを有効にする。

既存の にNATゲートウェイを追加する VPC

をすでに設定している場合はVPC、次のステップを実行してゲートウェイNATを に追加します VPC。新しい VPC を作成する必要がある場合は、「新しい を作成して設定する VPC」を参照してください。

既存の にNATゲートウェイを追加するには VPC

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NAT「ゲートウェイの作成」の手順を完了します。
2. に少なくとも 1 つのプライベートサブネットVPC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ているルートテーブルを更新して、インターネットにバインドされたトラフィックをNATゲートウェイにポイントします。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。これを行うには、「Amazon VPC ユーザーガイド」の「ルートテーブルの更新」の手順を完了します。

次のステップ

WorkSpaces プール WorkSpaces の がインターネットにアクセスできるようにするには、「」の手順を実行します WorkSpaces プールのインターネットアクセスを有効にする。

WorkSpaces プール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 で使用可能になったらVPC、 WorkSpaces プールのインターネットアクセスを有効にできます。 WorkSpaces プール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。ディレクトリを作成するときに、NATゲートウェイVPCを持つ 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。にプライベートサブネットがまだない場合はVPC、2 番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 プールを起動し、プール WorkSpace 内の に接続してインターネットを参照することで、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VPCを使用して新規または既存の 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、各 AWS リージョンにはデフォルトのVPCパブリックサブネットを含むデフォルトがあります。ただし、独自のデフォルト以外の を作成VPCしたり、 WorkSpaces プールディレクトリVPCで使用する既存の を設定したりできます。このトピックでは、 WorkSpaces プールで使用するデフォルト以外のVPC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 および パブリックサブネットを設定したら、デフォルト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 プール WorkSpaces 内の 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 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ている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でインターネット接続を有効にします。Elastic IP アドレスは、インターネットから到達可能なパブリックIPv4アドレスです。このため、代わりにNATゲートウェイを使用して、

WorkSpaces プール WorkSpaces の へのインターネットアクセスを提供することをお勧めします。さらに、デフォルト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 WorkSpaces がサポートされます。デプロイで 100 人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とNATゲートウェイVPCを使用して を設定するのステップ を参照してください。その他のVPC設定の推奨事項については、「」を参照してくださいVPC WorkSpaces プールの設定に関する推奨事項。

内容

- ステップ 1: パブリックサブネットVPCを使用して を設定する
- ステップ 2: WorkSpaces プールのデフォルトのインターネットアクセスを有効にする

ステップ 1: パブリックサブネットVPCを使用して を設定する

次のいずれかの方法を使用して、パブリックサブネットVPCでデフォルト以外の独自の を設定できます。

- 1 つのパブリックサブネットVPCで新しい を作成する
- 既存の を設定する VPC

1 つのパブリックサブネットVPCで新しい を作成する

VPC ウィザードを使用して新しい を作成するとVPC、ウィザードはパブリックサブネットに関連付けられたインターネットゲートウェイとカスタムルートテーブルを作成します。ルートテーブルは、外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VPC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VPC」の「単一のパブリックサブネットを使用する」を参照してください。

1. Amazon VPCユーザーガイドの「ステップ 1: VPCを作成する」のステップを完了して、 を作成しますVPC。
2. WorkSpaces がインターネットにアクセスできるようにするには、「」の手順を実行しますステップ 2: WorkSpaces プールのデフォルトのインターネットアクセスを有効にする。

既存の を設定する VPC

パブリックサブネットVPCを持たない既存の を使用する場合は、新しいパブリックサブネットを追加できます。パブリックサブネットに加えて、 にインターネットゲートウェイをアタッチVPCし、

外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VPC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、「 でサブネットを作成するVPC」の手順を実行します。 WorkSpaces プールで使用するVPC予定の既存の を使用します。

   アドレスIPv6指定をサポートするように が設定されている場合VPCは、IPv6CIDR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 にアタッチするにはVPC、「インターネットゲートウェイの作成とアタッチ」の手順を実行します。
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、送信先 にIPv4形式 () を使用します`0.0.0.0/0`。
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、「」の手順を実行しますステップ 2: WorkSpaces プールのデフォルトのインターネットアクセスを有効にする。

ステップ 2: WorkSpaces プールのデフォルトのインターネットアクセスを有効にする

WorkSpaces プール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。ディレクトリを作成するときに、パブリックサブネットVPCを持つ 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 プールを起動し、プール WorkSpace 内の に接続してインターネットを参照することで、インターネット接続をテストできます。

デフォルトの VPC、パブリックサブネット、およびセキュリティグループを使用する

Amazon Web Services アカウントが 2013-12-04 以降に作成された場合、各 AWS リージョンVPCにデフォルト 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、 にアタッチされている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VPCも含まれています。 WorkSpaces プールを初めて使用し、 サービスの使用を開始する場合は、 WorkSpaces プールの作成時にデフォルト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 2013-12-04 より前に作成されている場合は、WorkSpaces プールで使用する新しいアカウントを作成するVPCか、既存のアカウントを設定する必要があります。 WorkSpaces プール用の 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VPCを使用して、 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とNATゲートウェイVPCを使用して 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VPCでデフォルト以外の 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VPCを使用して新規または既存の を設定する」を参照してください。

WorkSpaces プール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VPC時にデフォルトを選択します。デフォルトVPC名は、 の形式を使用しますvpc-*vpc-id* (No_default_value_Name)。

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 block*) | Default in、 の形式を使用しますavailability-zone。

WorkSpaces プールを起動し、プール WorkSpace 内の に接続してインターネットを参照することで、インターネット接続をテストできます。

WorkSpaces プール機能に Amazon S3 VPCエンドポイントを使用する

WorkSpaces プールディレクトリの WorkSpaces プールまたはホームフォルダのアプリケーション設定の永続化を有効にすると、 はディレクトリにVPC指定した WorkSpaces 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。プライベート S3 エンドポイントへの WorkSpaces プールアクセスを有効にするには、Amazon S3 のVPCエンドポイントに次のカスタムポリシーをアタッチします。プライベート Amazon S3 エンドポイントの詳細については、VPC「Amazon VPCユーザーガイド」のAmazon S3のエンドポイント」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 プールVPCの 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 プール接続を有効にするには、WorkSpaces 次のように を設定します。

ネットワークインターフェイス

WorkSpaces プール WorkSpaces の各 には、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、 内のリソースとインターネットへの接続を提供し、 を WorkSpaces 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、安全な WorkSpaces プール管理ネットワークに接続されています。これは、ユーザーのデバイス WorkSpace への のインタラクティブなストリーミング、および WorkSpaces プールによる の管理を許可するために使用されます WorkSpace。

WorkSpaces プールは、管理ネットワークインターフェイスの 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。この範囲は、競合を引き起こし、 が到達不能になる可能性があるため、 には使用しないでください。VPCCIDRまた、この範囲VPCを持つ別の VPCとピア接続 WorkSpaces しないでください。また、 にアタッチされているネットワークインターフェイスを変更または削除しないでください。これにより WorkSpace、 WorkSpaceにアクセスできなくなる可能性があります。

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 の管理ネットワークインターフェイスで開いている必要があります WorkSpaces。

- ポート 8300 TCPへのインバウンド。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 8000 および 8443 TCPのインバウンド。これらは の管理に使用されます WorkSpaces。
- ポート 8300 UDPへのインバウンド。これは、 を介したストリーミング接続の確立に使用されますUDP。

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。

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

を無効にしないでくださいIPv6。を無効にするとIPv6、 WorkSpaces プールが正しく機能しません。Windows IPv6用 の設定については、「上級ユーザー向けの Windows IPv6 での の設定に関するガイダンス」を参照してください。

> **Note**
>
> WorkSpaces プールは、 内のDNSサーバーに依存しVPC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 プール管理のネットワークインターフェイスが管理サーバーと通信できるようになります。
> Simple AD で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。ドメインコントローラーはNXDOMAINレスポンスを提供しないため、 WorkSpaces プールでは使用できません。

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「セキュリティグループルール」を参照してください。
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
  - UDP 4195

- WorkSpaces をディレクトリに結合する場合、 WorkSpaces プールVPCとディレクトリコントローラーの間で次のポートが開いている必要があります。
  - TCP/UDP53 - 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/UDP445 - SMB
  - TCP 1024-65535 - の動的ポート RPC

  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。
- EC2 メタデータサービスへのアクセスを許可するには、すべての でポート 80 (HTTP) が IP アドレスに対して開かれ`169.254.169.254`ている WorkSpaces 必要があります。IP アドレス範囲`169.254.0.0/16`は、管理トラフィックの WorkSpaces プールサービスの使用の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 プールへのユーザー接続

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 WorkSpaces プール内の に接続できます。

デフォルトでは、 WorkSpaces プールはパブリックインターネット経由で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 プールが機能するために必要なウェブアセットを配信するには、インターネット接続が必要です。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**
>
> ユーザー認証の場合、 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、「2.0 SAML を設定し、 WorkSpaces プールディレクトリを作成する」を参照してください。

以下のトピックでは、 WorkSpaces プール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 プールユーザーデバイスの IP アドレスとポート要件
- 許可されたドメイン

推奨帯域幅

WorkSpaces プール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ことを確認してください。

WorkSpaces プールは NICE Desktop Cloud Visualization (DCV) を使用して、ユーザーがさまざまなネットワーク条件でアプリケーションに安全にアクセスしてストリーミングできるようにします。帯域幅の消費量を減らすために、 NICEDCVは H.264 ベースのビデオ圧縮とエンコーディングを使用します。ストリーミングセッション中、アプリケーションのビジュアル出力は圧縮され、 を介して 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HTTPS。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。ユーザーがストリーミングアプリケーションを操作すると、NICEDCVプロトコルは入力をキャプチャし、 経由でストリーミングアプリケーションに送り返しますHTTPS。

このプロセス中、ネットワーク条件は常に測定され、情報は WorkSpaces プールに送り返されます。 WorkSpaces プールは、ビデオとオーディオのエンコードをリアルタイムで変更することで、変化するネットワーク条件に動的に対応し、さまざまなアプリケーションやネットワーク条件に対応する高品質のストリームを生成します。

WorkSpaces プールストリーミングセッションに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。

次の表は、一般的なワークロードに基づく WorkSpaces プールストリーミングセッションの推奨ネットワーク帯域幅とレイテンシーに関するガイダンスを示しています。

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 プールユーザーデバイスの IP アドレスとポート要件

WorkSpaces プールユーザーのデバイスは、インターネットエンドポイントを使用するとき、およびドメイン名解決にDNSサーバーを使用している場合はポート 53 (TCP) で、ポート 443 () とポート 4195 (UDP) へのアウトバウンドアクセスを必要としますUDP。

- ポート 443 は WorkSpaces 、プールユーザーのデバイスとインターネットエンドポイントを使用する WorkSpaces ときの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 WorkSpaces 、プールユーザーのデバイスとインターネットエンドポイントを使用する WorkSpaces ときのUDPHTTPS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ています。 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 プールユーザーのデバイスとDNSサーバー間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、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 プールユーザーが にアクセスするには WorkSpaces、ユーザーが へのアクセスを開始するネットワーク上のさまざまなドメインを許可する必要があります WorkSpaces。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。このページでは、 WorkSpaces Personal には適用されるが、 WorkSpaces プール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、「2.0 SAML を設定し、 WorkSpaces プール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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。

2. ナビゲーションペインで、WorkSpaces、プールを選択します。
3. WorkSpaces プールの作成を選択します。
4. オンボーディング (オプション) で、ユースケースに基づいてレコメンデーションオプションを選択して、 WorkSpace 使用する のタイプに関するレコメンデーションを取得できます。WorkSpaces プールの使用がわかっている場合は、このステップをスキップできます。
5. 設定 WorkSpacesで、次の詳細を入力します。

   - [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、使用するバンドルタイプを以下から選択します WorkSpaces。
     - ベース WorkSpaces バンドルを使用する - ドロップダウンからバンドルのいずれかを選択します。選択したバンドルタイプの詳細を確認するには、[バンドルの詳細] を選択します。プールに提供されるバンドルを比較するには、[すべてのバンドルを比較] を選択します。
     - 独自のカスタムバンドルを使用 - 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 用のカスタム WorkSpaces イメージとバンドルを作成する」を参照してください。
   - [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 プールコンソールで設定できる最大セッション時間は 5760 分 (96 時間) です。 WorkSpaces プールを使用して設定できる最大セッション期間は 432,000 秒 (120 時間) APICLI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 プールのディレクトリを管理する」を参照してください。
7. WorkSpace プールの作成を選択します。

WorkSpaces プールの管理

WorkSpaces プールは、指定したイメージ WorkSpaces を実行する で構成されます。

内容

- WorkSpaces プールの実行モード
- WorkSpaces プールバンドル
- プールの変更
- プールを削除する
- WorkSpaces プールの自動スケーリング

WorkSpaces プールの実行モード

WorkSpaces は、ユーザーがアプリケーションとデスクトップをストリーミングしている場合にのみ実行されます。まだユーザーに割り当てられ WorkSpaces ていない は、ユーザーがストリーミングする前にプロビジョニング WorkSpaces する必要があります。 WorkSpaces プロビジョニングされた の数は、自動スケーリングルールによって管理されます。

ユーザーがアプリケーションまたはデスクトップを選択すると、1～2 分の待機時間後にそれらのストリーミングが開始されます。ユーザーにまだ割り当てられていない の停止 WorkSpaces されたインスタンス料金と、ユーザーに WorkSpaces 割り当てられている の実行中のインスタンス料金が請求されます。

WorkSpaces プールバンドル

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、ソフトウェアリソースの組み合わせです。を起動するときは WorkSpace、ニーズに合ったバンドルを

選択します。で使用できるデフォルトのバンドル WorkSpaces は、パブリックバンドルと呼ばれます。で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。

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 プールを作成したら、以下を変更できます。

- ディレクトリ ID (WorkSpaces プール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 プールを変更するには

1. ナビゲーションペインで、WorkSpaces、プールを選択します。
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、プールを選択します。
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 プール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 プールスケーリングの計画を立てるときは、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 を使用しますAPI。Auto Scaling が WorkSpaces プールと正しく連携するには、Application Auto Scaling に、プールを記述

および更新し、Amazon CloudWatch アラームを記述するアクセス許可と、ユーザー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 プールの Auto Scaling の理解と使用に役立つ情報を提供します。

内容

- スケーリングの概念
- コンソールを使用したプールスケーリングの管理
- を使用したプールスケーリングの管理 AWS CLI
- 追加リソース

スケーリングの概念

WorkSpaces プールのスケーリングは、Application Auto Scaling によって提供されます。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 プールで Auto Scaling を効果的に使用するには、次の用語と概念を理解する必要があります。

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

プールの作成中、またはプールタブを使用していつでも、 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。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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで、[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。

を使用したプールスケーリングの管理 AWS CLI

AWS Command Line Interface () 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AWS CLI。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、 を使用します AWS CLI。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。そのためには、次の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

この例では AWS CLI、使用率 >= 75% の場合、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"}
```

次に、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。-- alarm-actions パラメータには、前のコマンドでARN返されたポリシーを使用できます。

```
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

この例では AWS CLI、プールがInsufficientCapacityErrorエラーを返す場合にプールを 1 ずつ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"}
```

次に、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。--alarm-actions パラメータには、前のコマンドでARN返されたポリシーを使用できます。

```
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"}
```

次に、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。--alarm-actions パラメータには、前のコマンドでARN返されたポリシーを使用できます。

```
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 PutScheduledActionAPI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、 コマンドを使用して現在のプール容量を WorkSpaces describe-workspaces-pools AWS CLI一覧表示できます。

```
aws workspaces describe-workspaces-pools --name PoolId
```

現在のプール容量は、次の出力 (JSON 形式で表示) のようになります。

```
{
    "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。例えば、次のコマンドは、毎日午前 9:00 に最小容量を 3 に変更し、最大容量を 5 に変更しますUTC。

> **Note**
>
> cron 式の場合、 でアクションを実行するタイミングを指定しますUTC。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
```

プール容量を変更するスケジュールされたアクションが正常に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 プールの容量使用率を 75% に維持しようと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 のコマンドまたはAPIアクションの使用の詳細については、以下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
- 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 プールでの Active Directory の使用

WorkSpaces プール WorkSpaces の Windows を Microsoft Active Directory のドメインに結合し、クラウドベースのドメインまたはオンプレミスの既存の Active Directory ドメインを使用して、ドメイン結合ストリーミングインスタンスを起動できます。また 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、そのドメインを使用して WorkSpaces プール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 プールを Active Directory ドメインに結合することで、次のことができます。

- 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。
- グループポリシー管理コンソール (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します。
- 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 プール WorkSpaces の にエンタープライズコンプライアンスポリシーとセキュリティポリシーを適用します。

内容

- アクティブディレクトリドメインの概要
- WorkSpaces プールで Active Directory の使用を開始する前に
- 証明書ベースの認証
- WorkSpaces プール Active Directory 管理
- 詳細情報

アクティブディレクトリドメインの概要

WorkSpaces プールで Active Directory ドメインを使用するには、それらがどのように連携するか、および完了する必要がある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 プールでドメイン結合ディレクトリを作成します。
3. 2.0 ID プロバイダーで WorkSpaces Pools SAML アプリケーションを作成し、直接または Active Directory グループを介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アサーションを投稿します。
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 プールサービスに転送します。
6. からの認証トークンを使用して AWS、 WorkSpaces Pools はユーザーを認可し、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 Poles 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 ドメインの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に求められます。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 プール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、必要なエンタイトルメントとグループポリシー設定で Active Directory を設定し、ドメイン結合 WorkSpaces プールディレクトリを作成する必要があります。

WorkSpaces プールで Active Directory の使用を開始する前に

WorkSpaces プールで Microsoft Active Directory ドメインを使用する前に、以下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 プール WorkSpaces にドメイン参加
- グループポリシー設定
- スマートカード認証

アクティブディレクトリドメイン環境

- に参加する Microsoft Active Directory ドメインが必要です WorkSpaces。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 プールで使用するドメインに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を持つ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 プールに関連付けるときは、サービスアカウント名とパスワードを指定します。 WorkSpaces Pools はこのアカウントを使用して、ディレクトリ内のコンピュータオブジェクトを作成および管理します。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。

- Active Directory ドメインを WorkSpaces プールに登録するときは、組織単位 (OU) 識別名を指定する必要があります。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 プールでは使用できません。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 プールで使用する予定のディレクトリには、 WorkSpaces が起動される仮想プライベートクラウド (FQDNs) を介して、完全修飾ドメイン名 (VPC) からアクセス可能である必要があります。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 プール WorkSpaces にドメイン参加

SAML ドメイン結合からのアプリケーションストリーミングには、2.0 ベースのユーザーフェデレーションが必要です WorkSpaces。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。必要に応じて、このセクションで説明されているように設定を更新して、 WorkSpaces プールがドメインユーザーの認証とログインをブロックしないようにします。そうしないと、ユーザーが WorkSpaces ログインを試みても成功しない可能性があります。「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。
- コンピュータ設定 > 管理テンプレート > システム > ログオン > 認証情報プロバイダー を除外 — 以下CLSIDが表示されてい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 プールは、Active Directory ドメインパスワード、または WorkSpaces プール WorkSpaces の への Windows サインイン用の共通アクセスカード (CAC) や個人 ID 検証 (PIV) スマートカードなどのスマートカードの使用をサポートします。サードパーティー認証機関 (CAs) 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 Active Directory 環境を設定する方法については、Microsoft ドキュメントの「サードパーティー認証機関との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 プールでは、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。

- 2.0 ID プロバイダーに依存してユーザーを認証し、Active Directory SAML のユーザーと一致する SAMLアサーションを提供します。
- 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。
- 2SAML.0 ID プロバイダーを使用してパスワードレス認証フローを有効にします。

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 や下位 などのプライベート認証機関 (CA) 階層を作成できますCAs。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 プール WorkSpace 内の各 WorkSpaces のセッション予約時に、Pools がユーザーの証明書を自動的にリクエストします。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結合 WorkSpaces プール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
- 証明書ベースの認証の管理
- クロスアカウントPCA共有を有効にする

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. 証明書ベースの認証を使用するように 2.0 SAML 統合で WorkSpaces Pools ディレクトリを設定します。詳細については、「2.0 SAML を設定し、 WorkSpaces プール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 アサーションで `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. (オプション) SAMLアサーションで `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 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NameID。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。
4. 2.0 SAML 設定で使用するIAMロール信頼ポリシーに アクセス`sts:TagSession`許可を追加します。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: 2.0 SAML 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 Private 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 、Private 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、次の AWS Private 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ディストリビューション

   > **Note**
   >
   > 証明書ベースの認証では、 WorkSpaces プール WorkSpaces の とドメインコントローラーの両方からオンラインCRLディストリビューションポイントにアクセスする必要があります。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」の「証明書失効リスト (CRL) の計画」を参照してください。

6. プライベート CA に、 WorkSpaces プール証明書ベースの認証で使用する CA を指定する という権限を持つキー`euc-private-ca`をタグ付けします。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 Private 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 Certificate Services 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VPCの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、TCPポート 135、およびポート 49152 ~ 65535 へのアクセスをセキュリティグループに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これ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 でCLI、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。グループポリシーと Microsoft PKI Health Tool (PKIView) を使用して CA を発行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 プール WorkSpaces に発行されるまでに数分かかる場合があります。

> **Note**
>
> Active Directory は、ドメインに参加するときに WorkSpaces 、プール WorkSpaces 内の の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 サポートドキュメントのKB5「014754 — Windows ドメインコントローラーでの証明書ベースの認証の変更」を参照してください。 AWS Managed Microsoft AD を使用している場合は、「ディレクトリのセキュリティ設定の構成」を参照してください。

証明書ベースの認証

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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [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. [Save] 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。ドメインに参加している を使用して WorkSpaces プールディレクトリに対して SAML2.0 で認証する場合 WorkSpaces、ドメインパスワードの入力を求めるプロンプトは表示されなくなります。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 プール証明書ベースの認証 AWS Private Certificate Authority 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。これらの証明書は有効期間が短くなります。 WorkSpaces プールは、新しいセッションごとに新しい証明書を自動的に発行します。または、期間が長いセッションの場合は 24 時間ごとに新しい証明書を発行します。 WorkSpaces プールセッションは、これらのエンドユーザー証明書の使用を管理します。セッションを終了すると、 WorkSpaces プール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す必要はなく、 に表示されませんCRL。

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 CloudTrail 、 WorkSpaces プールによるプライベート CA へのAPI呼び出しを記録できます。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「 の使用 CloudTrail」を参照してください。CloudTrail イベント履歴では、 WorkSpaces プールのEcmAssumeRoleSessionユーザー名によって作成された acm-pca.amazonaws.com イベントソースから GetCertificateおよび IssueCertificateイベント名を表示できます。これらのイベントは、 WorkSpaces プール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「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

クロスアカウントPCA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では、集中型 CA を使用するアクセス許可を他のアカウントに付与できます。CA は、AWS Resource Access Manager (RAM) を使用してアクセス許可を管理することで、証明書を生成および発行できます。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 クロスアカウント共有は、同じ 内の AppStream 2.0 証明書ベースの認証 (CBA) で使用できます AWS リージョン。

WorkSpaces プールで共有 Private CA リソースを使用するにはCBA、次のステップを実行します。

1. 一元化された CBAで のプライベート CA を設定します 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 プールリソース AWS アカウント が を利用するリソースと共有しますCBA。これを行うには、「 を使用して AWS RAM ACM Private CA クロスアカウントを共有する方法」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 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APIs。

   共有を設定するときは、 AWS Resource Access Manager リソースアカウントの Private 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 プールサービスロールで使用されるPCAテンプレートと一致します。

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、 WorkSpaces プールディレクトリCBAの ARNにプライベート CA を関連付けます。現時点では、 WorkSpaces プールコンソールは共有プライベート CA の選択をサポートしていませんARNs。詳細については、「Amazon WorkSpaces Service API Reference」を参照してください。

WorkSpaces プール Active Directory 管理

WorkSpaces プールで Active Directory をセットアップして使用するには、以下の管理タスクが必要です。

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
- ドメイン信頼を使用するように WorkSpaces プールを設定する

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 プールが Active Directory コンピュータオブジェクトオペレーションを実行できるようにするには、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。

- ドメインに参加しているコンピュータまたはEC2インスタンスへのアクセスを取得します。
- Active Directory ユーザーとコンピュータの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。
- 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. これらのアクセス許可を必要とする追加の に対して、ステップ 2 ~ 9 OUs 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。このアカウントには、WorkSpaces を ディレクトリに接続するための十分な権限があります。 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

Active Directory ドメインを WorkSpaces プールに登録するときは、組織単位 (OU) 識別名を指定する必要があります。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 プールでは使用できません。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。

- ドメインに参加しているコンピュータまたはEC2インスタンスへのアクセスを取得します。
- Active Directory ユーザーとコンピュータの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。
- 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. 左側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) メニューを開き、プロパティを選択します。
4. [Attribute Editor] を選択します。
5. 属性で、 で表示distinguishedName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。ドメインユーザーにローカル管理者権限を付与すると、そのユーザーは にアプリケーションをインストールし、 WorkSpaces プールにカスタムイメージを作成できます。

内容

- グループポリシー設定を使用する
- でローカル管理者グループ WorkSpace を使用してイメージを作成する

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。

- ドメインに参加しているコンピュータまたはEC2インスタンスへのアクセスを取得します。
- グループポリシー管理コンソール (GPMC) 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。
- グループポリシーオブジェクト () を作成する権限を持つドメインユーザーとしてログインしますGPOs。適切な GPOsへのリンクOUs。

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、「」と入力しgpmc.msc、 を押しますENTER。
2. 左側のコンソールツリーで、新しい を作成するか、既存の GPOを使用する OU を選択しGPO、次のいずれかを実行します。

    - コンテキスト (右クリック) メニューを開き、このドメインGPOで を作成するを選択し、ここでリンクGPOして、新しい を作成します。名前には、この のわかりやすい名前を指定しますGPO。

- 既存の を選択しますGPO。

3. のコンテキストメニューを開きGPO、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. これをGPO他の に適用するにはOUs、追加の OU を選択し、コンテキストメニューを開いて、既存の をリンクGPO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名前を使用して、スクロールして を見つけGPO、OK を選択します。
11. この設定が必要な追加の に対して、ステップ 9 と 10 OUs 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. を再び閉じるには、OK を選択しますGPMC。

新しい設定を に適用するにはGPO、実行中の Image Builder またはフリートを停止して再起動する必要があります。ステップ 8 で指定した Active Directory ユーザーとグループには、 GPO がリンクされている OU 内の Image Builder とフリートに対するローカル管理者権限が自動的に付与されます。

でローカル管理者グループ WorkSpace 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. イメージの構築 WorkSpace に使用する に接続します。が実行され、ドメインに参加している WorkSpace 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 に対するローカル管理者権限があるかどうかをテストするには WorkSpaces、管理者コマンド、ユーザーの切り替えを選択し、関連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 プールは、ユーザーが指定した時間アイドル状態になった後にストリーミングセッションをロックGPMCするように で設定した設定に依存します。を使用するにはGPMC、まず次の操作を行う必要があります。

- ドメインに参加しているコンピュータまたはEC2インスタンスへのアクセスを取得します。
- 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。
- を作成する権限を持つドメインユーザーとしてログインしますGPOs。適切な GPOsへのリンク OUs。

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、「」と入力しgpmc.msc、 を押しますENTER。
2. 左側のコンソールツリーで、新しい を作成するか、既存の GPOを使用する OU を選択し GPO、次のいずれかを実行します。

- コンテキスト (右クリック) メニューを開き、このドメインGPOで を作成するを選択し、ここでリンクGPOして、新しい を作成します。名前には、この のわかりやすい名前を指定しますGPO。
- 既存の を選択しますGPO。

3. のコンテキストメニューを開きGPO、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。

ドメイン信頼を使用するように WorkSpaces プールを設定する

WorkSpaces プールは、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 1 つのドメインに存在し、ユーザーオブジェクトが別のドメインに存在する 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オペレーションに使用されるドメインサービスアカウントは、 WorkSpaces Pools コンピュータオブジェクトと同じドメインに存在す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 プール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 プール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、ソフトウェアリソースの組み合わせです。を起動するときは WorkSpace、ニーズに合ったバンドルを選択します。で使用できるデフォルトのバンドル WorkSpaces は、パブリックバンドルと呼ばれます。で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。

Windows を起動 WorkSpace してカスタマイズした場合は、その Windows からカスタムイメージを作成して WorkSpaces プールで WorkSpace 使用できます。Linux は WorkSpaces プールではサポートされていません。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

カスタムイメージを作成したら、カスタム WorkSpace イメージと、選択した基盤となるコンピューティングおよびストレージ設定を組み合わせたカスタムバンドルを構築できます。その後、新しい WorkSpaces プール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 WorkSpaces 内の新しい の設定 (ハードウェアとソフトウェア) が一貫していることを確認できます。

ソフトウェア更新を実行したり、 に追加のソフトウェアをインストールしたりする必要がある場合は WorkSpaces、カスタムバンドルを更新して、それを使用して を再構築できます WorkSpaces。

WorkSpaces プールは、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
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する保証はなく、 AWS サポートによってもサポートされません。

トピック

- WorkSpaces Pools のバンドルオプション
- WorkSpaces プールのカスタムイメージとバンドルを作成する
- WorkSpaces プールのカスタムイメージと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
- Email(メール)

このバンドルは、音声およびビデオ会議、画面共有、言語処理、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

Performance バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- インスタントメッセージング
- Email(メール)
- スプレッドシート
- オーディオ処理
- コースウェア

このバンドルは、ビデオ会議、画面共有、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

Power バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- インスタントメッセージング
- スプレッドシート
- オーディオ処理
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入
- 音声会議とビデオ会議

このバンドルは、画面共有、ソフトウェア開発ツール、ビジネスインテリジェンスアプリケーション、およびグラフィックアプリケーションにはお勧めしません。

PowerPro バンドル

このバンドルは、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- インスタントメッセージング
- スプレッドシート
- オーディオ処理
- ソフトウェア開発 (統合開発環境 (IDE))
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- 音声会議とビデオ会議

このバンドルは、機械学習モデルのトレーニング、およびグラフィックアプリケーションにはお勧めしません。

Graphics.g4dn バンドル

このバンドルは、WorkSpaces の高いレベルのグラフィックパフォーマンスと、中程度のレベルの CPU パフォーマンスおよびメモリを提供し、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- スプレッドシート
- インスタントメッセージング
- オーディオ会議
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入

- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- グラフィックスデザイン
- CAD/CAM (コンピューター支援設計/コンピューター支援製造)

このバンドルは、音声会議やビデオ会議、3D レンダリング、実写のようなリアルなデザイン、および機械学習モデルのトレーニングにはお勧めしません。

GraphicsPro.g4dn バンドル

このバンドルは、WorkSpaces の高いレベルのグラフィックパフォーマンス、CPU パフォーマンス、およびメモリを提供し、以下に最適です。

- ウェブブラウジング
- 言語処理
- Email(メール)
- スプレッドシート
- インスタントメッセージング
- オーディオ会議
- ソフトウェア開発 (統合開発環境 (IDE))
- 中級レベルのデータ処理への参入
- データウェアハウス
- ビジネスインテリジェンスアプリケーション
- グラフィックスデザイン
- CAD/CAM (コンピューター支援設計/コンピューター支援製造)
- 動画トランスコーディング
- 3D レンダリング
- 実写のようなリアルなデザイン
- ゲームストリーミング
- 機械学習 (ML) モデルのトレーニングと ML 推論

このバンドルは、音声会議やビデオ会議にはお勧めしません。

WorkSpaces プールのカスタムイメージとバンドルを作成する

WorkSpaces プールは Windows イメージとバンドルのみをサポートします。Windows または を起動 WorkSpace し、カスタマイズした場合は、そこからカスタムイメージとカスタムバンドルを作成できます WorkSpace。

カスタムイメージには、 の OS、ソフトウェア、および設定のみが含まれます WorkSpace。カスタムバンドルは、そのカスタムイメージと、 を起動 WorkSpace できるハードウェアの両方の組み合わせです。

カスタムイメージを作成したら、カスタムイメージと、選択した基盤となるコンピューティングおよびストレージ設定を組み合わせたカスタムバンドルを構築できます。その後、新しい を起動するときにこのカスタムバンドルを指定 WorkSpaces して、新しい の設定 (ハードウェアとソフトウェア) WorkSpaces が一貫していることを確認できます。

バンドルごとに異なるコンピューティングオプションとストレージオプションを選択することで、同じカスタムイメージを使用してさまざまなカスタムバンドルを作成できます。

> **Important**
>
> - 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 料金表」を参照してください。

内容

- Windows カスタムイメージを作成するための要件
- ベストプラクティス
- (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
- ステップ 2: Image Checker を実行する
- ステップ 3: カスタムイメージとカスタムバンドルを作成する
- Windows WorkSpaces カスタムイメージに含まれているもの

Windows カスタムイメージを作成するための要件

> **Note**
>
> 現在、Windows では 1 GB を 1,073,741,824 バイトと定義しています。のイメージを作成するには、C ドライブで 12,884,901,888 バイト (または 12 GiB) を超える空きがあり、ユーザープロファイルが 10,737,418,240 バイト (または 10 GiB) 未満であることを確認する必要があります WorkSpace。

- のステータスは Available WorkSpace で、変更ステータスは None である必要があります。
- WorkSpaces イメージ上のすべてのアプリケーションとユーザープロファイルは、Microsoft Sysprep と互換性がある必要があります。
- イメージに含めるすべてのアプリケーションは、C ドライブにインストールする必要があります。
- で実行されているすべてのアプリケーションサービスは、ドメインユーザー認証情報の代わりにローカルシステムアカウント WorkSpace を使用する必要があります。たとえば、Microsoft SQL Server Express のインストールをドメインユーザーの認証情報で実行することはできません。
- は暗号化 WorkSpace しないでください。暗号化された からのイメージの作成 WorkSpace は現在サポートされていません。
- 以下のコンポーネントがイメージに必要です。これらのコンポーネントがないと、イメージから起動 WorkSpaces した が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 エージェントとドライバー
  - STXHD エージェントとドライバー
  - AWS および WorkSpaces 証明書
  - Skylight エージェント
- WorkSpaces プールは、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

からイメージを作成する前に WorkSpace、次の操作を行います。

- 本番環境に接続VPCされていない別の を使用します。
- プライベートサブネット WorkSpace に をデプロイし、アウトバウンドトラフィックにNATインスタンスを使用します。
- 小さい Simple AD ディレクトリを使用します。
- ソースの最小ボリュームサイズを使用し WorkSpace、カスタムバンドルを作成するときに必要に応じてボリュームサイズを調整します。
- すべてのオペレーティングシステムの更新 (Windows 機能/バージョンの更新を除く) とすべてのアプリケーションの更新を にインストールします WorkSpace。
- バンドルに含めるべきではないキャッシュされたデータ (ブラウザ履歴、キャッシュファイル、ブラウザ Cookie など) WorkSpace を から削除します。
- バンドルに含めるべきではない から設定を削除します (E WorkSpace メールプロファイルなど)。
- を使用して動的 IP アドレス設定に切り替えますDHCP。
- リージョンで許可されている WorkSpace イメージのクォータを超えていないことを確認してください。デフォルトでは、リージョンごとに 40 個の WorkSpace イメージが許可されます。このクォータに達した場合、新しいイメージを作成しようとすると失敗します。クォータの引き上げをリクエストするには、WorkSpaces の制限フォームを使用します。
- 暗号化された からイメージを作成しようとしていないことを確認します WorkSpace。暗号化された からのイメージの作成 WorkSpace は現在サポートされていません。
- でウイルス対策ソフトウェアを実行している場合は WorkSpace、イメージの作成中に無効にします。
- でファイアウォールが有効になっている場合は WorkSpace、必要なポートがブロックされていないことを確認してください。詳細については、「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 の場合 WorkSpaces、イメージの作成前にグループポリシーオブジェクト (GPOs) を設定しないでください。
- Windows の場合は WorkSpaces、イメージを作成する前にデフォルトのユーザープロファイル (`C:\Users\Default`) をカスタマイズしないでください。を使用してユーザープロファイルをカスタマイズしGPOs、イメージの作成後に適用することをお勧めします。 は簡単に変更または口ー

ルバックGPOsできるため、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。

- の ENA、NVMe、PV ドライバーなどのネットワーク依存関係ドライバーを必ず更新してください WorkSpaces。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、「Windows インスタンス用の Elastic Network Adapter (ENA) ドライバー をインストールまたはアップグレードする」および「Windows インスタンスでの PV ドライバーのアップグレード」を参照してください。 AWS NVMe ドライバー
- EC2Config、EC2Launch、および EC2Launch V2 エージェントは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と の更新EC2Launch」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 WorkSpaces 起動された では、デフォルトのコンピュータ名形式を使用する代わりに、コンピュータ名形式にカスタムプレフィックスを指定できます。デフォルトでは、Windows 10 のコンピュータ名の形式 WorkSpaces は DESKTOP-XXXXXで WorkSpaces、Windows 11 のコンピュータ名の形式は ですWORKSPA-XXXXX。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 WorkSpace 使用している で、メモ帳または別のテキストエディタC:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xmlで を開きます。Unattend.xml ファイルの操作の詳細については、Microsoft のドキュメントの「応答ファイル (unattend.xml)」をご参照ください。

   の Windows File Explorer からC:ドライブにアクセスするには WorkSpace、アドレスバーC:\にと入力します。

2. <settings pass="specialize"> セクションで、<ComputerName> がアスタリスク (*) に設定されていることを確認します。<ComputerName> が他の値に設定されている場合、カスタムコンピュータ名の設定は無視されます。<ComputerName> 設定の詳細については、Microsoft ドキュメントの ComputerName「」を参照してください。

3. <settings pass="specialize"> セクションで、<RegisteredOrganization> および <RegisteredOwner> を任意の値に設定します。

   Sysprep では、<RegisteredOwner> および <RegisteredOrganization> に指定した値が連結され、結合された文字列の最初の 7 文字を使用してコンピュータ名が作成されます。たとえば、 Amazon.comに <RegisteredOrganization>を指定し、 **EC2**に を指定した場

合<RegisteredOwner>、カスタムバンドルから WorkSpaces 作成された のコンピュータ名は で始まりますEC2AMAZ-*xxxxxxx*。

<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 がイメージ作成の要件を満た WorkSpace 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 WorkSpace に使用する で一連のテストを実行し、見つかっ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 でのみ使用できます WorkSpaces。

> **Important**
>
> - は、イメージの作成に使用する前に、Image Checker によって実行されるすべてのテストに合格 WorkSpace する必要があります。
> - Image Checker を実行する前に、最新の Windows セキュリティ更新プログラムと累積更新プログラムが にインストールされていることを確認します WorkSpace。

Image Checker を入手するには、以下のいずれかを実行します。

- を再起動します WorkSpace。Image Checker は再起動時に自動的にダウンロードされ、C:\Program Files\Amazon\ImageChecker.exe にインストールされます。
- https://tools.amazonworkspaces.com/ImageChecker.zip 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、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。

ステータスが のテストではFAILED、Info を選択して、障害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 のステータスが表示された場合はWARNING、すべての警告を修正する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、テストの失敗や警告の原因となる問題を解決し、 がすべてのテストに WorkSpace合格するまで Image Checker を実行するプロセスを繰り返します。イメージを作成する前に、すべての失敗と警告が解決されている必要があります。
5. がすべてのテストに WorkSpace 合格すると、検証成功メッセージが表示されます。これで、カスタムバンドルを作成する準備ができました。

Image Checker によって検出された問題を解決するためのヒント

Image Checker によって検出された問題を解決するための以下のヒントを参照するほか、`C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` で Image Checker のログファイルも確認してください。

PowerShell バージョン 3.0 以降がインストールされている必要があります

Microsoft Windows PowerShellの最新バージョンをインストールします。

> **Important**
>
> PowerShell の実行ポリシーは、RemoteSignedスクリプトを許可するように設定 WorkSpace する必要があります。実行ポリシーを確認するには、Get-ExecutionPolicy PowerShell command を実行します。実行ポリシーが無制限または に設定されていない場合はRemoteSigned、Set-ExecutionPolicy –ExecutionPolicy RemoteSigned コマンドを実行して実行ポリシーの値を変更します。RemoteSigned この設定により WorkSpaces、イメージの作成に必要な Amazon でのスクリプトの実行が可能になります。

C および D ドライブのみが存在できる

イメージに使用される には、 Cおよび WorkSpace Dドライブのみ存在できます。仮想ドライブを含め他のすべてのドライブを削除します。

Windows Update による保留中の再起動は検出できない

- Windows を再起動してセキュリティまたは累積更新プログラムのインストールが完了するまで、イメージ作成プロセスは実行できません。Windows を再起動してこれらの更新を適用し、保留中の他の Windows セキュリティまたは累積更新プログラムをインストールする必要がないことを確認します。
- イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows 10 システム (Windows の機能/バージョンのアップグレード) ではサポートされません。ただし、Windows の累積更新プログラムまたはセキュリティ更新プログラムは、WorkSpaces イメージ作成プロセスでサポートされています。

Sysprep ファイルは存在する必要があり、空白にすることはできない

Sysprep ファイルに問題がある場合は、 AWS Support センターに連絡して EC2Configまたは の EC2Launch修復を依頼してください。

ユーザープロファイルのサイズは 10 GB 未満であることが必要

Windows 7 の場合 WorkSpaces、ユーザープロファイル (`D:\Users\`*`username`*) の合計は 10 GB 未満である必要があります。必要に応じてファイルを削除して、ユーザープロファイルのサイズを小さくします。

ドライブ C には十分な空き容量が必要

Windows 7 では WorkSpaces、ドライブ に 12 GB 以上の空き容量が必要ですC。必要に応じてファイルを削除し、ドライブ C の空き容量を増やします。Windows 10 では WorkSpaces、FAILEDメッセージを受信し、ディスク容量が 2GB を超える場合は無視します。

ドメインアカウントで実行できるサービスがない

イメージの作成プロセスを実行するには、ドメインアカウントで 上のサービス WorkSpace を実行することはできません。すべてのサービスがローカルアカウントで実行されている必要があります。

ローカルアカウントでサービスを実行するには

1. `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` を開き、ドメインアカウントで実行されているサービスのリストを見つけます。
2. Windows の検索ボックスに「**`services.msc`**」と入力して、Windows サービスマネージャーを開きます。
3. [ログオン方法] で、ドメインアカウントで実行されているサービスを探します。([ローカルシステム]、[ローカルサービス]、または [ネットワークサービス] として実行されているサービスは、イメージの作成を妨げません)
4. ドメインアカウントで実行されているサービスを選択し、[操作]、[プロパティ] の順に選択します。
5. [ログオン] タブを開きます。[ログオン方法] で、[ローカルシステムアカウント] を選択します。
6. [OK] を選択します。

を使用するように を設定 WorkSpace する必要があります DHCP

静的 IP アドレスDHCPの代わりに を使用する WorkSpace ように、 のすべてのネットワークアダプタを設定する必要があります。

を使用するようにすべてのネットワークアダプタを設定するには DHCP

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を選択します。
8. [OK] を選択します。
9. 上のすべてのネットワークアダプタに対してこのプロセスを繰り返します WorkSpace。

リモートデスクトップサービスを有効にすることが必要

イメージ作成プロセスでは、リモートデスクトップサービスを有効にする必要があります。

リモートデスクトップサービスを有効にするには

1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[リモートデスクトップサービス] を見つけます。
3. [リモートデスクトップサービス] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] を選択します。

ユーザープロファイルが存在することが必要

イメージの作成 WorkSpace に使用する には、ユーザープロファイル () が必要です`D:\Users\`*`username`*。このテストに失敗した場合は、AWS Support センターにお問い合わせください。

環境変数のパスを適切に設定することが必要

ローカルマシンの環境変数パスに、System32 および Windows のエントリがありません PowerShell。これらのエントリは、[イメージの作成] を実行するために必要です。

環境変数のパスを設定するには

1. Windows の検索ボックスに「**environment variables**」と入力し、[システム環境変数の編集] を選択します。
2. [システムのプロパティ] ダイアログボックスで、[詳細設定] タブを開き、[環境変数] を選択します。
3. [環境変数] ダイアログボックスの [システム変数] で、[パス] エントリを選択し、[編集] を選択します。
4. [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32
   ```
5. もう一度 [新規] を選択し、以下のパスを追加します。

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```

6. [OK] を選択します。
7. を再起動します WorkSpace。

> **Tip**
>
> 環境変数のパスに項目が表示される順序が重要です。正しい順序を決定するには、 の環境変数パス WorkSpace を、新しく作成された Windows インスタンス WorkSpace または新しい Windows インスタンスのパスと比較します。

Windows モジュールインストーラーを有効にすることが必要

イメージ作成プロセスでは、Windows モジュールインストーラーサービスを有効にする必要があります。

Windows モジュールインストーラーサービスを有効にするには

1. Windows の検索ボックスに「**services.msc**」と入力して、Windows サービスマネージャーを開きます。
2. [名前] 列で、[Windows モジュールインストーラー] を見つけます。
3. [Windows モジュールインストーラー] を選択し、[操作]、[プロパティ] の順に選択します。
4. [全般] タブの [スタートアップの種類] で、[手動] または [自動] を選択します。
5. [OK] を選択します。

Amazon SSM Agent を無効にする必要があります

イメージの作成プロセスでは、Amazon SSM エージェントサービスを無効にする必要があります。

Amazon SSM エージェント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 エージェントを見つけます。
3. Amazon SSM エージェントを選択し、アクション、プロパティを選択します。
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] を選択します。

SSL3 およびTLSバージョン 1.2 を有効にする必要があります

Windows 用 SSL/TLS を設定するには、Microsoft Windows ドキュメントの「How to Enable TLS 1.2」を参照してください。

には 1 つのユーザープロファイルしか存在できません WorkSpace

イメージの作成に使用している には WorkSpace 、1 つの WorkSpaces ユーザープロファイル (`D:\Users\username`) しか使用できません。の目的のユーザーに属さないユーザープロファイルを削除します WorkSpace。

イメージ作成が機能するように、 には 3 つのユーザープロファイルしか WorkSpace 使用できません。

- (`D:\Users\username`) の対象ユーザーのユーザー WorkSpaceプロファイル
- デフォルトのユーザープロファイル (デフォルトプロファイルとも呼ばれます)
- 管理者ユーザープロファイル

追加のユーザープロファイルがある場合は、Windows コントロールパネルの詳細システムプロパティを使用して削除できます。

ユーザープロファイルを削除するには

1. 詳細システムプロパティにアクセスするには、以下のいずれかを実行します。
   - Windows + Pause Break キーを押し、[コントロールパネル] > [システムとセキュリティ] > [システム]ダイアログボックスの左側のペインで [システムの詳細設定]を選択します。
   - Windows の検索ボックスに「**`control panel`**」と入力します。コントロールパネルで、[システムとセキュリティ]、[システム] の順に選択し、[コントロールパネル] > [システムとセキュリティ] > [システム] ダイアログボックスの左側のペインで [システムの詳細設定] を選択します。
2. [システムのプロパティ] ダイアログボックスの [詳細設定] タブで、[ユーザープロファイル] の [設定] を選択します。
3. 管理者プロファイル、デフォルトプロファイル、および目的の WorkSpacesユーザーのプロファイル以外のプロファイルが一覧表示されている場合は、その追加プロファイルを選択して削除を選択します。
4. プロファイルを削除するかどうか尋ねられたら、[はい] を選択します。

5. 必要に応じて、ステップ 3 と 4 を繰り返して、 に属していない他のプロファイルを削除します WorkSpace。
6. [OK] を 2 回選択し、コントロールパネルを閉じます。
7. を再起動します WorkSpace。

AppX パッケージがステージング状態になることはない

1 つ以上の AppX パッケージがステージング状態になっています。これにより、イメージの作成中に Sysprep エラーが発生する可能性があります。

ステージングされたすべての AppX パッケージを削除するには

1. Windows の検索ボックスに「**powershell**」と入力します。[管理者として実行] を選択します。
2. 「このアプリがデバイスに変更を加えることを許可しますか?」と尋ねられたら、[はい] を選択します。
3. Windows PowerShell ウィンドウで、次のコマンドを入力してステージングされたすべての AppX パッケージを一覧表示し、それぞれの後に Enter キーを押します。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. 以下のコマンドを入力して、ステージングされたすべての AppX パッケージを削除し、Enter キーを押します。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. Image Checker を再度実行します。それでもこのテストに失敗する場合は、以下のコマンドを入力して、すべての AppX パッケージを削除し、それぞれの後に Enter キーを押します。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows が以前のバージョンからアップグレードされていないこと

イメージの作成は、あるバージョンの Windows 10 から新しいバージョンの Windows 10 にアップグレードされた Windows システム (Windows の機能/バージョンのアップグレード) ではサポートされません。

イメージを作成するには、Windows の機能/バージョンのアップグレードが完了 WorkSpace していない を使用します。

Windows リアームカウントが 0 でないこと

リアーム機能を使用すると、Windows の試用バージョンのアクティベーション期間を延長できます。イメージ作成プロセスでは、リアームカウントを 0 以外の値にする必要があります。

Windows リアームカウントを確認するには

1. Windows の [スタート] メニューで [Windows システム] を選択し、[コマンドプロンプト] を選択します。
2. [コマンドプロンプト] ウィンドウで、以下のコマンドを入力し、Enter キーを押します。

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

リアームカウントを 0 以外の値にリセットするには、Microsoft Windows ドキュメントの「Sysprep (Generalize) a Windows installation」を参照してください。

トラブルシューティングに関するその他のヒント

が Image Checker によって実行されるすべてのテストに WorkSpace 合格しても、 からイメージを作成できない場合は WorkSpace、次の点を確認してください。

- WorkSpace がドメイン吠えるグループ内のユーザーに割り当てられていないことを確認します。ドメインアカウントがあるかどうかを確認するには、次の PowerShellコマンドを実行します。

```
Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
$env:USERDOMAIN*" }
```

- 一部のグループポリシーオブジェクト (GPOs) 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リクエストされたときに、RDP証明書のサムプリントへのアクセスを制限します。イメージを作成する前に、 WorkSpace を、継承がブロックされ、GPOs適用されていない新しい組織単位 (OU) に移動します。
- 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] を選択します。

ステップ 3: カスタムイメージとカスタムバンドルを作成する

WorkSpace イメージを検証したら、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。プログラムでイメージを作成するには、CreateWorkspaceImage APIアクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceImage」の「」を参照してください。プログラムでバンドルを作成するには、 CreateWorkspaceBundleAPIアクションを使用します。詳細については、「Amazon WorkSpaces API リファレンス CreateWorkspaceBundle」の「」を参照してください。

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. にまだ接続している場合は WorkSpace、 WorkSpaces クライアントアプリケーションで Amazon WorkSpaces と Disconnect を選択して切断します。
2. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
3. ナビゲーションペインで、WorkSpaces を選択します。

4. を選択して詳細ページ WorkSpace を開き、イメージの作成を選択します。のステータス WorkSpace が Stopped の場合は、アクション、イメージの作成を選択する前に、まず開始する必要があります (アクション、開始 WorkSpacesを選択 ）。
5. 続行する前に、 を再起動 (再起動 ） WorkSpace するように求めるメッセージが表示されます。Amazon WorkSpaces ソフトウェアを再起動すると、最新バージョンに WorkSpace 更新されます。

   メッセージ WorkSpace を閉じて の手順に従って、 を再起動しますWorkSpaces Personal の WorkSpace を再起動する。完了したら、この手順の Step 4 を繰り返します。ただし、再起動メッセージが表示されたら、[次へ] を選択します。イメージを作成するには、 のステータスが Available WorkSpace で、変更ステータスが None である必要があります。
6. イメージを識別するのに役立つイメージの名前と説明を入力し、[イメージの作成] を選択します。イメージの作成中、 のステータス WorkSpace は一時停止になり、 WorkSpace は使用できなくなります。

   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。ステータスが Available に WorkSpace 変わると、イメージは完了します (これには最大 45 分かかる場合があります ）。
8. イメージを選択し、[Actions] (アクション)、[Create bundle] (バンドルの作成) を選択します。
9. バンドル名と説明を入力し、次の操作を行います。

   - バンドルハードウェアタイプで、このカスタムバンドル WorkSpaces から起動するときに使用するハードウェアを選択します。
   - ルートボリュームで使用できるデフォルトのサイズの組み合わせは、 あたり 200 GB です WorkSpace。
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ているもの

Windows からイメージを作成すると WorkSpace、Cドライブの内容全体が含まれます。

- 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 プールのカスタムイメージとバンドルを管理する

カスタムイメージとバンドルを管理するプロセスは、 WorkSpaces Personal と WorkSpaces Pool 間で同じです。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 に使用できるカスタムバンドルと WorkSpaces Pool に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基本パブリックバンドルです。 WorkSpaces プール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、「」を参照してください
>
> WorkSpace バンドルは、オペレーティングシステム、ストレージ、コンピューティング、ソフトウェアリソースの組み合わせです。を起動するときは WorkSpace、ニーズに合ったバンドルを選択します。で使用できるデフォルトのバンドル WorkSpaces は、パブリックバンドルと呼ばれます。で使用できるさまざまなパブリックバンドルの詳細については WorkSpaces、「Amazon WorkSpaces Bundles」を参照してください。
>
> 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。

。

- 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 プールはインスタンスセッションスクリプトを提供します。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。たとえば、カスタムスクリプトを使用して、ユーザーのストリーミングセッションを開始する前に WorkSpaces プール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 イメージ内で指定されます。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
- 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
- セッションスクリプトを作成および指定する
- セッションスクリプト設定ファイル

- Windows PowerShell ファイルの使用
- セッションスクリプト出力のログ記録
- セッションスクリプトで永続的ストレージを使用する
- 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

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。これにより、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 プール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 以外の値を返す場合、 はエラーメッセージをユーザーに WorkSpaces 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. ユーザーは、ドメインに参加していない WorkSpaces プール WorkSpace の に接続します。2.0 SAML を使用して接続します。
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、ユーザーのカスタマイズと Windows 設定を保存するアプリケーション設定 Virtual Hard Disk (VHD) ファイルをダウンロードしてマウントします。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 プール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 プールの永続的ストレージの有効化と管理 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。たとえば、ユーザーが WorkSpaces クライアントツールバーからセッションの終了を選択した場合や、セッションの最大許容期間に達した場合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削除される前に 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は終了します。
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と Windows 設定を保存するアプリケーション設定VHDファイルはアンマウントされ、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 は終了します。

セッションスクリプトを作成および指定する

WorkSpaces プール WorkSpaces で 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 WorkSpace を作成する Windows に接続します。
2. `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。
3. 変更が終了したら、`config.json` ファイルを保存して閉じます。
4. からイメージを作成するステップを完了します WorkSpace。詳細については、「WorkSpaces プールの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。

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。

タイプ: 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`パラメータで PowerShell ファイルへのフルパスを指定します。

```
"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を有効にすると、 WorkSpaces Pool は標準出力に書き込まれたセッションスクリプトからの出力を自動的にキャプチャします。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

永 WorkSpaces 続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。スクリプトがマウントされている永続的ストレージに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。 は WorkSpacesWindows の Windows レジストリのストレージコネクタのマウントステータスを次のキーで WorkSpaces 維持します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AppStream\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 — UserID
  - SAML — NameID。ユーザー名にスラッシュ (ドメインユーザーの などSAMAccountName) が含まれている場合、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

各ストレージコネクタレジストリキーには MountStatusDWORD値が含まれています。次の表に、の可能な値を示しますMountStatus。

> **Note**
>
> これらのレジストリキーを表示するには、Microsoft が必要です。NETイメージにインストールされているフレームワークバージョン 4.7.2 以降。

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 ログ記録を有効にすると、 WorkSpaces Pool はセッションスクリプトからの標準出力をキャプチャします。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。 AWS リージョンごとに、 WorkSpaces プールは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。これらは WorkSpaces 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ているログファイルは、Amazon S3 のSSLエンドポイントを使用して転送中に暗号化され、Amazon S3-managed暗号化キーを使用して保管時に暗号化されます。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 プールを作成する 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 `appstream-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 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すると123456789012、 WorkSpaces Pool はそのリージョンのアカウント内に表示されている名前で 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-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 を使用して、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API。 WorkSpaces Pools は、バケットの誤った削除を防止するバケットポリシーを追加します。

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 プールの名前。

<access-mode>

ユーザーの ID メソッド: または customの場合は WorkSpaces API CLI、 federated の場合は SAML、ユーザープール内のユーザーuserpoolの場合は 。

<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、ユーザー ID APIの 、 の AWS アカウント ID123456789012、および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

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。 単位: カウント 有効な統計: Average、Minimum、Maximum
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。 `ActualUserSessionCapacity = AvailableUserSessionCapacity + ActiveUserSessionCapacity` 単位: カウント 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。 `AvailableUserSessionCapacity = ActualUserSessionCapacity - ActiveUserSessionCapacity` 単位: カウント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
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。 単位: カウント 有効な統計: Average、Minimum、Maximum
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。 `UserSessionCapacityUtilization = (ActiveUserSessionCapacity / ActualUserSessionCapacity) * 100` 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。 単位: パーセント 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。 `DesiredUserSessionCapacity = ActualUserSessionCapacity + PendingUserSessionCapacity` 単位: カウント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
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。 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。 単位: カウント 有効な統計: Average、Minimum、Maximum、Sum

WorkSpaces プールの永続的ストレージの有効化と管理

WorkSpaces プールは、永続的ストレージのホームフォルダをサポートします。 WorkSpaces プール管理者として、次のタスクを実行してユーザーの永続的ストレージを有効化および管理する方法を理解する必要があります。

内容

- WorkSpaces プールユーザーのホームフォルダの有効化と管理

WorkSpaces プールユーザーのホームフォルダの有効化と管理

WorkSpaces プールの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。

ファイルとフォルダはAmazon S3のSSLエンドポイントを使用して転送中に暗号化されます。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、次のデフォルトの場所 WorkSpaces の WorkSpaces プールの に保存されます。

- シングルセッションの場合、 non-domain-joinedWindows WorkSpaces: `C:\Users\PhotonUser\My Files\Home Folder`
- ドメイン結合された Windows WorkSpaces: `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 プールユーザーのホームフォルダを有効にする
- ホームフォルダを管理する

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 プールのストリーミングセッション中、コンピューティング集約型のアプリケーションに関連する大きなファイルやディレクトリを永続的ストレージに保存するには、基本的な生産性向上アプリケーションに必要なファイルや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するファイルやディレクトリをユーザーが保存し、 WorkSpaces プール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より適した、計算負荷の高い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。

- 統合開発環境の Workspace フォルダ (IDEs)
- 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 プール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 アクションに対する正しい 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、仮想プライベートクラウド (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 プールのネットワークとアクセスおよび WorkSpaces プール機能に 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2.0 SAML を設定し、 WorkSpaces プール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、 を使用して AWS Management Console WorkSpaces 、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。

リージョンの WorkSpaces プールディレクトリのホームフォルダを AWS 初めて有効にすると、サービスは同じリージョンのアカウントに Amazon S3 バケットを作成します。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

- 「2.0 SAML を設定し、 WorkSpaces プール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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
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
- Amazon S3 バケットのストレージ
- ホームフォルダコンテンツの同期
- ホームフォルダの形式
- その他のリソース

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 はユーザーコンテンツを削除しません。

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

- 「2.0 SAML を設定し、 WorkSpaces プール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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。
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 プールは、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、 *>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 プールは、バケットの誤った削除を防止するバケットポリシーを追加します。

ホームフォルダコンテンツの同期

ホームフォルダを有効にすると、 WorkSpaces Pools 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を作成します。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 プールが Amazon S3 にホームフォルダを作成すると、そのフォルダ内のアクセスされたコンテンツが S3 バケットから にコピーされます WorkSpace。これにより、ユーザーはストリーミングセッション WorkSpace 中にプールの WorkSpaceからホームフォルダコンテンツにすばやくアクセスできます。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た変更と、ユーザーが WorkSpace プール WorkSpace 内の のホームフォルダコンテンツに加えた変更は、次のように Amazon S3 と WorkSpaces プール間で同期されます。

1. ユーザーの WorkSpaces プールストリーミングセッションの開始時に、 WorkSpaces Pools は Amazon Web Services アカウントとリージョンの Amazon S3 バケットにそのユーザー用に保存された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のコンテンツは、ストリーミング元の WorkSpaces プール WorkSpace の にも保存されます。ユーザーが のホームフォルダにアクセスすると WorkSpace、カタログ化されたファイルのリストが表示されます。
3. WorkSpaces プールは、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く WorkSpace 場合にのみ、S3 バケットから にファイルをダウンロードします。
4. WorkSpaces プールがファイルを にダウンロードすると WorkSpace、ファイルへのアクセス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すると、 WorkSpaces プールはストリーミングセッションの定期的または終了時に、ファイルの新しいバージョン WorkSpace を 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
- 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
- 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

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、数分以内にユーザーのホームフォルダ内のファイルのリストに表示

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 WorkSpace まで、ファイルは S3 バケットから 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 WorkSpace プールの のホームフォルダ WorkSpace でファイルを開き、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を新しいバージョンに置き換えた場合、ファイルの新しいバージョンはすぐに にダウンロードされません WorkSpace。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、ファイルを再度開いた後に WorkSpace のみ、S3 バケットから 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 WorkSpace プールの のホームフォルダ WorkSpace でファイルを開き、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ファイルを削除すると、そのファイルはユーザーが次のいずれかを実行 WorkSpace した後、 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の場合、ユーザーフォルダ構造は次のとおりです。

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

この場合、*user-id-SHA-256-hash*は、フェSAMLデレーションリクエストで渡されたNameIDSAML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。同じ名前で 2 つの異なるドメインに属するユーザーを区別するには、 形式でNameIDでSAMLリクエストを送信しますdomainname\username。詳細については、「2.0 SAML を設定し、 WorkSpaces プールディレクトリを作成する」を参照してください。

次のフォルダ構造の例は、米国西部 (オレゴン) リージョンの NameID SAMPLEDOMAIN\testuser、アカウント ID 123456789012 との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 (ドメイン名が例にあるため)、WorkSpaces Pools *SAMPLEDOMAIN* は文字列で使用される大文字化に基づいてハッシュ値を生成します。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。

ウェブサイトまたはオンラインで利用可能なオープンソースコーディングライブラリNameIDを使用して、 の SHA-256 ハッシュ値を生成することで、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: IAMユーザーが S3 ホームディレクトリにプログラムでアクセスできるようにする」および「コンソールでアクセスを許可する」を参照してください。
- WorkSpaces プールで使用される Amazon S3 バケットに保存されているコンテンツのファイル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 プール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 プールは、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。これらは、各 WorkSpaces プール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
- アプリケーション設定の永続化を有効にする
- ユーザーのアプリケーション設定VHDsの を管理する

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、仮想ハードディスク (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た WorkSpace プールが、デフォルトのアプリケーションと Windows 設定を含むイメージに基づいている場合、デフォルトの設定がユーザーの最初のストリーミングセッションに使用されます。

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Amazon S3SSLエンドポイントを使用して転送中に暗号化され、 AWS マネージド CMKsを使用して保管時に暗号化されます。

VHD は、 `C:\Users\%username%`と の両方で にマウント WorkSpace されます`D:\%username%`。 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 です PhotonUser。 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しているユーザーのユーザー名になります。

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。たとえば、Windows Server 2019 イメージを使用する WorkSpace プールのアプリケーション

設定の永続化を有効にした場合、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 WorkSpace プールを更新すると、以前のストリーミングセッションの設定は 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 WorkSpace プールを更新した後、ユーザーが からストリーミングセッションを起動すると WorkSpace、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ると、ユーザーが 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 WorkSpace。

> **Important**
>
> WorkSpaces プールは、 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 WorkSpace が Active Directory ドメインに参加していない場合、Windows ユーザーは ごとに PhotonUser異なります WorkSpace。DPAPI セキュリティモデルの仕組みにより、このシナリオDPAPIで 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。が WorkSpaces Active Directory ドメインに参加していて、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ユーザー名であり、ユーザーのパスワードは を使用するアプリケーションでも保持されますDPAPI。

WorkSpaces プールは、以下のフォルダを除き、すべてのファイルとフォルダをこのパスに自動的に保存します。

- 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

これらのフォルダの外部で作成されたファイルとフォルダは、 内に保存VHDされ、Amazon S3 に同期されます。プールのデフォルトのVHD最大サイズは 5 GB です。保存される のサイズVHDは、含まれるファイルとフォルダの合計サイズです。 WorkSpaces Pools はユーザーのHKEY_CURRENT_USERレジストリハイブを自動的に保存します。新規ユーザー (プロファイルが Amazon S3 に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**
>
> WorkSpace ストリーミングセッションを開始する前に、全体を にダウンロードVHDする必要があります。このため、大量のデータVHDを含む は、ストリーミングセッションの開始を遅らせる可能性があります。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ストリーミングセッションに使用する保存されたアプリケーション設定を決定します。 WorkSpaces プールは、 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ためのベストプラクティス
- アプリケーション設定の永続化を有効にする方法

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、仮想プライベートクラウド (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、「」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 WorkSpaces プールのネットワークとアクセス。

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

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 WorkSpaces、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 プール WorkSpaces 内の が接続されている VPC にある必要があります。エンドポイントへの WorkSpaces プール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。カスタムポリシーの作成方法については、「」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 WorkSpaces プールのネットワークとアクセス。プライベート Amazon S3 エンドポイントの詳細については、VPC「Amazon VPCユーザーガイド」のAmazon S3のエンドポイント」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

WorkSpaces コンソールを使用して、ディレクトリの作成中またはディレクトリの作成後に、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ファイルが保存されます。詳細については、ユーザーのアプリケーション設定VHDsの 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

- 「2.0 SAML を設定し、 WorkSpaces プール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. で WorkSpaces コンソールを開きますhttps://console.aws.amazon.com/workspaces/。

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VHDsの を管理する

内容

- Amazon S3 バケットのストレージ
- ユーザーのアプリケーション設定をリセットする
- 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
- アプリケーション設定のサイズを増やす VHD

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。各 AWS リージョンについて、 WorkSpaces Pools は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。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に設定タスクを実行する必要はありません。これらのバケットは WorkSpaces プール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ているVHDファイルは、Amazon S3 のSSLエンドポイントを使用して転送中に暗号化され、 AWS マネージドCMKsを使用して保管時に暗号化されます。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性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 の米国西部 (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 はそのリージョンのアカウント内に表示されている名前で 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VHDsされている は削除されません。設定 を完全に削除するにはVHDs、Amazon S3 コンソールまたは を使用して、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API。 WorkSpaces Pools は、バケットの誤った削除を防止するバケットポリシーを追加します。

アプリケーション設定の永続化を有効にすると、設定グループごとに一意のフォルダが作成され、設定 が保存されますVHD。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。

設定がアカウントの S3 バケットに保存されているフォルダのパスVHDは、次の構造を使用します。

```
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 プールcustomの場合は APIまたは CLI、 ユーザープールfederatedの場合は SAML、ユーザープールユーザーuserpoolの場合は 。

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、 APIまたは CLIのユーザー ID、 の AWS アカウント IDtestuser@mydomain.com、およびtest-stack米国西部 (オレゴン) リージョン (us-west-2) 123456789012の設定グループ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
```

ウェブサイトまたはオンラインで利用可能な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 ハッシュ値を生成することで、ユーザーのフォルダを識別できます。

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 アカウント内の 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見つけ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すると、 WorkSpaces Pools VHD はそのユーザーの新しい設定を作成します。

ユーザーのアプリケーション設定をリセットするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. バケット名リストで、リセットVHDするアプリケーション設定を含む S3 バケットを選択します。

3. を含むフォルダを見つけますVHD。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. 名前リストで、 VHDと の横にあるチェックボックスを選択しREG、詳細 を選択し、削除 を選択します。
5. オブジェクトの削除ダイアログボックスで、 VHDと REGがリストされていることを確認し、削除を選択します。

ユーザーが次に、該当する設定グループで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。これはVHD、セッションの終了時に 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、設定 のすべてのバージョンを保存、取得、復元できますVHD。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。バージョニングが有効になっている場合、各ストリーミングセッションの後、新しいバージョンのアプリケーション設定VHDがAmazon S3 に同期されます。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発生した場合は、以前のバージョンの に戻すことができますVHD。

> **Note**
>
> アプリケーション設定の各バージョンVHDは個別のオブジェクトとして Amazon S3 に保存され、それに応じて課金されます。

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でオブジェクトのバージョニングを有効にするには VHD

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 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を含む S3 VHD 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を期限切れにするにはVHDs、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を元に戻すには VHD

該当する S3 バケットVHDから の新しいバージョンを削除VHDすることで、ユーザーのアプリケーション設定の以前のバージョンに戻すことができます。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. バケット名リストで、元に戻すユーザーのアプリケーション設定VHDバージョンを含む S3 バケットを選択します。
3. を含むフォルダを見つけて選択しますVHD。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と関連するメタデータファイルが表示されます。
4. VHD およびメタデータファイルバージョンのリストを表示するには、表示を選択します。
5. VHD 元に戻す のバージョンを見つけます。
6. 名前リストで、 の新しいバージョン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選択し、その他を選択してから、削除を選択します。
7. VHD を元に戻すアプリケーション設定と関連するメタデータファイルが、これらのファイルの最新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のサイズを増やす VHD

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に追加のスペースが必要な場合は、該当するアプリケーション設定を Windows コンピュータVHDにダウンロードして展開できます。次に、S3 バケットVHD内の現在の を大きい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**
>
> 仮想ハードディスク (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クリアします。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のサイズを増やすには VHD

> **Note**
>
> ユーザーがアプリケーションをストリーミングする前に、フル をダウンロードVHDする必要があります。アプリケーション設定のサイズを大きくすると、ユーザーがアプリケーションストリーミングセッションを開始するのにかかる時間が長くなるVHD可能性があります。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. バケット名リストで、VHD展開するアプリケーション設定を含む S3 バケットを選択します。
3. を含むフォルダを見つけて選択しますVHD。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と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たらブラウザを閉じないでください。後でブラウザを再度使用して、展開された をアップロードしますVHD。
5. Diskpart を使用して のサイズを 7 GB VHDに増やすには、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。

   ```
   diskpart
   ```

   ```
   select vdisk file="C:\path\to\application\settings\profile.vhdx"
   ```

   ```
   expand vdisk maximum=7000
   ```
6. 次に、次の Diskpart コマンドを入力して、 を検索してアタッチしVHD、ボリュームのリストを表示します。

```
elect vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
attach vdisk
```

```
list volume
```

出力で、「」というラベルの付いたボリューム番号を書き留めますAwsEucUsers。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. 次のコマンドを入力して、 のパーティションのサイズが想定どおりにVHD増加したことを確認します (この例では 7 GB)。

```
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 をデタッチVHDし、アップロードできるようにします。

```
detach vdisk
```

11. Amazon S3 コンソールでブラウザに戻り、アップロード、ファイルの追加を選択し、拡大線 を選択しますVHD。
12. [アップロード] を選択します。

VHD をアップロードした後、次にユーザーが、該当する設定グループで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ストリーミングするときに、より大きな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が有効期限切れになっています。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表示される場合は、AWS Support までお問い合わせください。詳細については、AWS Supportセンターを参照してください。

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表示される場合は、AWS Support までお問い合わせください。詳細については、AWS Supportセンターを参照してください。

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表示される場合は、AWS Support までお問い合わせください。詳細については、AWS Supportセンターを参照してください。

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。

解決方法: AWS Support に連絡してサポートを受けてください。詳細については、AWS Supportセンターを参照してください。

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

AWS では、クラウドのセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された AWS のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

セキュリティは、AWS とお客様とが共有する責務です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ - AWS は、AWS Cloud で AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWSは、使用するサービスを安全に提供します。AWSコンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。WorkSpaces に適用するコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の AWS サービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS のサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、WorkSpaces を使用する際に共有責任モデルを適用する方法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすように WorkSpaces を設定する方法を説明します。また、WorkSpaces リソースのモニタリングや保護に役立つ、他の AWS サービスの使用方法についても説明します。

内容

- Amazon でのデータ保護 WorkSpaces
- の Identity and Access Management WorkSpaces
- Amazon WorkSpaces のコンプライアンスの検証
- Amazon WorkSpaces の耐障害性
- Amazon のインフラストラクチャセキュリティ WorkSpaces
- WorkSpaces に関する更新管理

Amazon でのデータ保護 WorkSpaces

Amazon でのデータ保護には、 AWS の責任共有モデルが適用されます WorkSpaces。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。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FAQ」を参照してください。欧州におけるデータ保護の詳細については、 AWS セキュリティブログの AWS 責任共有モデルとGDPRブログ投稿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 () 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IAM。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。1TLS.2 が必要で、1.3 TLS をお勧めします。
- API とユーザーアクティビティのログ記録を でセットアップします 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 などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、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、、WorkSpaces または を使用して または他の AWS のサービス を操作する場合も同様ですAPI AWS CLI 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。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

WorkSpaces とFIPSエンドポイントの暗号化の詳細については、「」を参照してください WorkSpaces Personal の FedRAMP 認可または DoD SRG コンプライアンスを設定する。

保管中の暗号化

AWS KMS キー WorkSpaces を使用して、 のストレージボリュームを暗号化できます AWS Key Management Service。詳細については、「 WorkSpaces Personal WorkSpaces で暗号化」を参照してください。

暗号化されたボリューム WorkSpaces で を作成すると、 は Amazon Elastic Block Store (Amazon EBS) WorkSpaces を使用してそれらのボリュームを作成および管理します。 EBS は、業界標準の AES-256 アルゴリズムを使用してデータキーでボリュームを暗号化します。詳細については、「Amazon ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。 EC2

転送中の暗号化

の場合PCoIP、転送中のデータは 1.2 TLS 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、ストリーミングピクセルにAES暗号化されたUDPトラフィックを使用します。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、暗号化のデフォルトは 128 ビットです。このデフォルトは、Windows PCoIPのセキュリティ設定グループポリシーの設定を使用するか、Amazon Linux の `pcoip-agent.conf` ファイルPCoIPのセキュリティ設定を変更することで WorkSpaces、256 ビットに変更できます WorkSpaces。

Amazon のグループポリシー管理の詳細については WorkSpaces、PCoIP セキュリティ設定を構成する「」の「」を参照してくださいPersonal WorkSpaces で Windows WorkSpaces を管理する。`pcoip-agent.conf` ファイルの変更の詳細については、Teradici ドキュメントのAmazon Linux でのPCoIPエージェントの動作を制御する WorkSpaces「」およびPCoIP「セキュリティ設定」を参照してください。

の場合DCV、転送中のデータのストリーミングと制御は、UDPトラフィックの 1.3 TLS 暗号化とTCPトラフィックTLSの 1.2 暗号化を使用して、AES-256 暗号で暗号化されます。

の Identity and Access Management WorkSpaces

デフォルトでは、IAMユーザーには WorkSpaces リソースとオペレーションに対するアクセス許可はありません。IAM ユーザーが WorkSpaces リソースを管理できるようにするには、明示的にアクセス許可を付与する IAMポリシーを作成し、それらのアクセス許可を必要とするIAMユーザーまたはグループにポリシーをアタッチする必要があります。

> **Note**
>
> Amazon WorkSpaces は、 WorkSpace （ インスタンスプロファイルなど) へのIAM認証情報のプロビジョニング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。
- ID プロバイダーIAMを介して で管理されるユーザー：

  ID フェデレーションのロールを作成します。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) のロールを作成する」の手順に従います。
- IAM ユーザー：
  - ユーザーが担当できるロールを作成します。「 IAMユーザーガイド」の「 IAMユーザーのロールを作成する」の手順に従います。
  - (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する。「 IAMユーザーガイド」の「ユーザーへのアクセス許可の追加 (コンソール) 」の手順に従います。

以下は、 の追加リソースですIAM。

- 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。
- の詳細についてはIAM、「 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。
- アクセスIAM許可ポリシーで使用する WorkSpaces特定のリソース、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 のアクション、リソース、および条件キー WorkSpaces」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。IAM Policy Simulator を使用して、ポリシーが特定のリクエストを許可または拒否するかどうかをテストすることもできます AWS。

内容

- ポリシーの例
- IAM ポリシーで WorkSpaces リソースを指定する
- workspaces_DefaultRole Role を作成する
- AmazonWorkSpacesPCAAccess サービスロールを作成する
- AWS の マネージドポリシー WorkSpaces
- 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

ポリシーの例

次の例は、IAMユーザーが Amazon に対して持つ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 WorkSpaces。

例 1: WorkSpaces 個人用タスクとプール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、個人用タスクとプールタスクを実行する WorkSpaces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",
                "workdocs:AddUserToGroup",
                "workdocs:DeregisterDirectory",
                "workdocs:RegisterDirectory",
                "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 個人用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 は、 `Action`および コマンドラインツールを使用するときに APIおよび `Resource`要素 WorkSpaces を完全にサポートしていますが、 WorkSpaces から Amazon 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": "*"`

次のポリシー例は、 IAMユーザーが WorkSpaces から Amazon を使用できるようにする方法を示しています AWS Management Console。

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

```
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup",
        "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 プール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 プール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: のすべての WorkSpaces タスクを実行する BYOL WorkSpaces

次のポリシーステートメントは、Bring Your Own License (BYOL) の作成に必要な Amazon タスクを含むすべての WorkSpacesEC2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WorkSpaces。

```
{
    "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",
                "workdocs:AddUserToGroup",
                "workdocs:DeregisterDirectory",
                "workdocs:RegisterDirectory"
            ],
            "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には、リソースの Amazon リソースネーム (ARN) を使用します。 WorkSpaces リソースへのアクセスを制御するには、IAMポリシーステートメントの `Action`要素で指定されたAPIアクションを使用するアクセス許可を許可または拒否します。 WorkSpaces は WorkSpaces、、バンドル、IP グループ、およびディレクトリARNs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
```

region

　があるリージョン WorkSpace （ 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

の ID WorkSpace （ 例: ws-a1bcd2efg) 。

以下は、特定の 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 WorkSpace。

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

* ワイルドカードを使用して、特定のリージョンの特定のアカウント WorkSpaces に属するすべての を指定できます。

WorkSpace プール ARN

WorkSpace プール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

があるリージョン WorkSpace （ 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) 。

以下は、特定の 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 WorkSpace。

```
"Resource":
 "arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier"
```

* ワイルドカードを使用して、特定のリージョンの特定のアカウント WorkSpaces に属するすべての 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
```

region

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
```

region

があるリージョン WorkSpace （ 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
```

region

があるリージョン WorkSpace （ 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
```

region

があるリージョン WorkSpace （ 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
```

region

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。

API リソースレベルのアクセス許可をサポートしない アクション

以下のAPIアクションARNではリソースを指定できません。

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

リソースレベルのアクセス許可をサポートしていないAPIアクションの場合は、次の例に示すリソースステートメントを指定する必要があります。

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

API 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 アクション

以下の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、ARNリソースにアカウント 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、そのアカウントが処理対象のリソースを所有しているARN場合にのみ、リソースでアカウント 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 Role を作成する

を使用してディレクトリを登録する前にAPI、 という名前のロールworkspaces_DefaultRole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、高速セットアップによって作成されるか、WorkSpace を使用して を起動した場合に作成され 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 WorkSpaces 許可を Amazon 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 role を作成するには

1. にサインイン AWS Management Console し、 で IAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
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. オプションでは、多要素認証 () を指定しないでくださいMFA。
7. [Next: Permissions] (次へ: アクセス許可) を選択します。
8. アクセス許可ポリシーをアタッチページで、 AWS 管理ポリシー AmazonWorkSpacesServiceAccess、AmazonWorkSpacesSelfServiceAccess、 を選択しますAmazonWorkSpacesPoolServiceAccess。これらのマネージドポリシーの詳細については、「AWS の マネージドポリシー WorkSpaces」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 role の概要ページで、信頼関係タブを選択します。
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 Directory 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。

を使用してサービスロールを作成するには AmazonWorkSpacesPCAAccess AWS CLI

1. 次のテキストAmazonWorkSpacesPCAAccess.jsonで という名前のJSONファイルを作成します。

```
{
    "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 の マネージドポリシー WorkSpaces

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。必要なアクセス許可のみをチームに提供する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、 AWS マネージドポリシーに新しい機能をサポートするために追加のアクセス許可を追加することがあります。この種の更新は、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、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 管理ポリシー AWS をサポートしています。たとえば、 ReadOnlyAccess AWS 管理ポリシーは、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。あるサービスで新しい機能を立ち上げる場合は、 AWS は、追加された演算とリソースに対し、読み込み専用の権限を追加します。職務機能ポリシーのリストと説明については、IAM「 ユーザーガイド」のAWS 「職務機能用の 管理ポリシー」を参照してください。

AWS 管理ポリシー： AmazonWorkSpacesAdmin

このポリシーは、Amazon WorkSpaces 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 個人用リソースと WorkSpaces プールリソースで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キーとエイリアスのリストと記述へのアクセスを許可します。

```
{
    "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 管理ポリシー: 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、次のアクセス許可が付与されます。

- `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 管理ポリシー: AmazonWorkSpacesSelfServiceAccess

このポリシーは、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するための Amazon WorkSpaces サービスへの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。

- `workspaces` - ユーザーにセルフサービス WorkSpaces 管理機能へのアクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 管理ポリシー: AmazonWorkSpacesServiceAccess

このポリシーは、 を起動するための Amazon WorkSpaces サービスへのお客様のアカウントアクセスを提供します WorkSpace。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 管理ポリシー: AmazonWorkSpacesPoolServiceAccess

このポリシーは workspaces_ で使用されます。Workspaces_ はDefaultRole、 WorkSpaces を使用して WorkSpaces プールの顧客 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 Role 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 - VPCs、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、 WorkSpaces プールに関連付けられた Amazon EC2リソースを管理するためのアクセスを許可します。
- 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

商用 には、次のポリシーJSONが適用されます 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

次のポリシーは、商用 JSONに適用されます AWS GovCloud (US) Regions。

```
{
    "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}"
                }
            }
        }
    ]
}
```

WorkSpaces AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した WorkSpaces 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。

変更	説明	日付
the section called “AmazonWorkSpacesPoolServiceAcces” - 新しいポリシーを追加しました	WorkSpaces は、Amazon EC2 VPCs および関連リソースを表示し、 WorkSpaces プールの Amazon S3 バケットを表示および管理するためのアクセス許可を付与する新しい マネージドポリシーを追加しました。	2024 年 6 月 24 日
the section called “AmazonWorkSpacesAdmin” – ポリシーを更新	WorkSpaces は WorkSpaces 、プールのいくつかのアクションを Amazon WorkSpacesAdmin 管理ポリシーに追加し、 WorkSpace プールリソースを管理するためのアクセス権を管理者に付与しました。	2024 年 6 月 24 日
the section called “AmazonWorkSpacesAdmin” – ポリシーを更新	WorkSpaces は Amazon WorkSpacesAdmin 管理ポリシーに `workspace`	2023 年 6 月 25 日

変更	説明	日付
	`s:RestoreWorkspace` アクションを追加し、 を復元するためのアクセス権を管理者に付与しました WorkSpaces。	
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 ための Private 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 が変更の追跡を開始しました	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アクセス許可セットを指定します。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 アクションおよび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や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 内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 の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] では、[WorkSpaces — WorkSpaces インスタンスがお客様に代わって AWS のサービスを呼び出すことを許可] がすで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している場合があるため、作成後はロールの名前を編集できません。
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、[Create role] (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、AWS 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 を任意の言語で使用して、プログラムで AWS の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 では、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、アプリケーションやスクリプトは、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。

AWS 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) 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

Amazon Web Services SDK for .NET バージョン 3.3.103.22 以降では、AWS Tools for PowerShell バージョン 3.3.563.1 以降を使用する必要があります。AWS Tools for PowerShell ウェブサイトから、AWS Tools for PowerShell および Amazon Web Services SDK for .NET を含む AWS Tools for Windows インストーラをダウンロードできます。

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

AWS SDK for Python を使用して Boto クライアントを作成する

```
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、さまざまな AWS コンプライアンスプログラムの一環として Amazon WorkSpaces のセキュリティとコンプライアンスを評価します。このプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムによる対象範囲内の AWS サービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

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

WorkSpaces および FedRAMP の詳細については、「 WorkSpaces Personal の FedRAMP 認可または 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。
- 「Amazon Web Services での HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ」 – このホワイトペーパーは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法を説明しています。
- AWS コンプライアンスのリソース– このワークブックおよびガイドのコレクションは、お客様の業界と拠点に適用できる場合があります。

- AWS Configデベロッパーガイドのルールでのリソースの評価 – AWS Configは、リソース設定が、社内のプラクティス、業界のガイドラインそして規制にどの程度適合しているのかを評価します。
- AWS Security Hub– AWSのこのサービスは、 AWS内でのユーザーのセキュリティ状態に関する包括的な見解を提供し、業界のセキュリティ標準、およびベストプラクティスに対するコンプライアンスを確認するために役立ちます。

Amazon WorkSpaces の耐障害性

AWS のグローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心として構築されています。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、耐障害性、および拡張性が優れています。

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

Amazon WorkSpaces は、クロスリージョンリダイレクトも提供します。これは、ドメインネームシステム (DNS) フェイルオーバールーティングポリシーと連携して、プライマリ WorkSpaces が利用できない場合に WorkSpaces ユーザーを別の AWS リージョン内の別の WorkSpaces にリダイレクトする機能です。詳細については、「 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 のインフラストラクチャセキュリティ WorkSpaces

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」の「インフラストラクチャの保護」を参照してください。 AWS

が AWS 公開したAPI呼び出しを使用して、ネットワーク WorkSpaces 経由で 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) 。1TLS.2 が必要で、1.3 TLS をお勧めします。

- DHE (エフェメラル Diffie-HellmanPFS) や (エリプティックカーブエフェメラル Diffie-Hellman) など、完全前方秘匿性 ECDHE () を持つ暗号スイート。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の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

仮想プライベートクラウド (VPC) は、 AWS クラウド内の論理的に隔離された独自のエリアにある仮想ネットワークです。の WorkSpaces プライベートサブネットに をデプロイできますVPC。詳細については、「VPC WorkSpaces 個人用の 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、 のセキュリティグループを更新するVPC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、信頼されたデバイス WorkSpace へのアクセスを制限できます。詳細については、「 WorkSpaces Personal の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 WorkSpaces 上の異なる 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、ハイパーバイザーによって割り当てられたメモリがスクラブ (ゼロに設定) されてから、新しい に割り当てられます WorkSpace。

企業ユーザーの承認

では WorkSpaces、ディレクトリは を通じて管理されます AWS Directory Service。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。

へのアクセスをさらに制御するには WorkSpaces、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を介した Amazon WorkSpaces API リクエストの実行

インターネット経由で接続するのではなく、仮想プライベートクラウド (VPC) のインターフェイスエンドポイントを介して Amazon WorkSpaces API エンドポイントに直接接続できます。VPC インターフェイスエンドポイントを使用すると、 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、 エンドポイントへの接続 WorkSpaces APIにのみ使用できます。 WorkSpaces クライアント WorkSpaces を使用して に接続するには、「」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 WorkSpaces Personal の IP アドレスとポートの要件。

Amazon WorkSpaces API エンドポイントは、 を使用する Amazon Virtual Private Cloud (Amazon VPC) インターフェイスエンドポイントをサポートしますAWS PrivateLink。各VPCエンドポイントは、VPCサブネット内のプライベート IP アドレスを持つ 1 つ以上のネットワークインターフェイス (Elastic Network Interface または とも呼ばれますENIs) 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、 を Amazon WorkSpaces API エンドポイントVPCに直接接続します。のインスタンスは、パブリック IP アドレスがなくても Amazon VPC 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 WorkSpaces を使用して Amazon AWS Management Console 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したら、 `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CLIコマンド例を使用できます。

```
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ホスト名を有効にする場合、エンドポイント を指定する必要はありませんURL。CLI と Amazon WorkSpaces API がデフォルトで使用する Amazon WorkSpaces SDK DNSホスト名 (https://api.workspaces.*Region*.amazonaws.com) は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 WorkSpacesは、Amazon と Amazon VPC 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。Amazon WorkSpaces は、 内のすべてのパブリック APIs への呼び出しをサポートしていますVPC。

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「 料金表」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。

リージョン別の Amazon WorkSpaces API エンドポイントのリストを確認するには、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、連邦情報処理標準 (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 のVPCエンドポイントポリシーを作成する WorkSpaces

Amazon の Amazon VPCエンドポイントのポリシーを作成して WorkSpaces 、以下を指定できます。

- 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「エンドポイントを使用したサービスへのアクセスの制御」を参照してください。

> **Note**
>
> VPC エンドポイントポリシーは、連邦情報処理標準 (FIPS) Amazon WorkSpaces エンドポイントではサポートされていません。

次のVPCエンドポイントポリシーの例では、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、 という名前の Amazon WorkSpaces ホストエンドポイントを呼び出すことができることを指定しますws-f9abcdefg。

```
{
     "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 ホストエンドポイントの呼び出しws-f9abcdefg。
- 指定されたリソース (WorkSpace ID: ws-f9abcdefg) 以外のリソースに対してアクションを実行する。

> **Note**
>
> この例では、ユーザーは の外部から他の Amazon WorkSpaces API アクションを実行できますVPC。内からのAPI呼び出しを制限するにはVPC、アイデンティティベースのポリシーを使用して Amazon WorkSpaces API エンドポイントへのアクセスを制御する方法の詳細については、の Identity and Access Management WorkSpaces「」を参照してください。

プライベートネットワークを に接続する VPC

を介して 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VPC、AWS Virtual Private Network （ AWS VPN) または VPCを使用してプライベートネットワークを に接続する必要があります AWS Direct Connect。詳細については、VPN「Amazon Virtual Private Cloud ユーザーガイド」の「接続」を参照してください。 Amazon Virtual Private Cloud 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 クォータ

Amazon WorkSpaces は、イメージ、バンドル、ディレクトリ WorkSpaces、接続エイリアス、IP コントロールグループなど、特定のリージョンのアカウントで使用できるさまざまなリソースを提供します。Amazon Web Services アカウントを作成すると、作成できるリソースの数が、デフォルトのクォータ (制限とも言う) として設定されます。

AWS アカウントの WorkSpaces のデフォルトのクォータは次のとおりです。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	調整可能
WorkSpaces	1	このアカウントの現在のリージョン WorkSpaces における の最大数。	あり
グラフィック WorkSpaces	0	現在のリージョン WorkSpaces におけるこのアカウントのグラフィックスの最大数。 **Note** 2023 年 11 月 30 日以降、Graphics バンドルはサポートされなくなります。WorkSpaces	あり

リソース	デフォルト	説明	調整可能
		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、「Personal WorkSpace で を移行する WorkSpaces」を参照してください。	
Graphics.g4dn WorkSpaces	0	このアカウントの現在のリージョン WorkSpaces における Graphics.g4dn の最大数。	あり
GraphicsPro WorkSpaces	0	現在のリージョン GraphicsPro WorkSpaces におけるこのアカウントのの最大数。 (GraphicsPro バンドルは 2025 年 10 月 31 日に到達 end-of-lifeします。 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。)	あり

リソース	デフォルト	説明	調整可能
GraphicsPro.g4dn WorkSpaces	0	この WorkSpaces アカウントの現在のリージョンにおける GraphicsPro.g4dn の最大数。	あり
スタンバイ WorkSpaces	5	このアカウントの現在のリージョン WorkSpaces における の最大数。	あり
バンドル	50	現在のリージョン内のこのアカウントのバンドルの最大数。このクォータはカスタムバンドルにのみ適用され、パブリックバンドルには適用されません。	いいえ
接続エイリアス	20	現在のリージョン内のこのアカウントの接続エイリアスの最大数。	いいえ
ディレクトリ	50	現在のリージョンで、このアカウント WorkSpaces で Amazon で使用するために登録できるディレクトリの最大数。	いいえ
イメージ	40	現在のリージョン内のこのアカウントのイメージの最大数。	あり

リソース	デフォルト	説明	調整可能
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
WorkSpaces プール	10	このアカウントの現在のリージョンの WorkSpaces プールの最大数。	あり
WorkSpaces プールの汎用値ストリーミングインスタンス	10	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる汎用値ストリーミングインスタンスの最大数。	あり

リソース	デフォルト	説明	調整可能
WorkSpaces プールの汎用スタンダードストリーミングインスタンス	10	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる汎用スタンダードインスタンスの最大数。	あり
プールの WorkSpaces汎用パフォーマンスストリーミングインスタンス	10	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる汎用パフォーマンスストリーミングインスタンスの最大数。	あり
WorkSpaces プールの汎用 Power ストリーミングインスタンス」	10	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる汎用 Power ストリーミングインスタンスの最大数。	あり
WorkSpaces プールの汎用 PowerPro ストリーミングインスタンス」	10	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる汎用 PowerPro ストリーミングインスタンスの最大数。	あり

リソース	デフォルト	説明	調整可能
WorkSpaces プールの Graphics.g4dn xlarge ストリーミングインスタンス	0	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる Graphics.g4dn xlarge ストリーミングインスタンスの最大数。	あり
WorkSpaces プールの Graphics.g4dn 4xlarge ストリーミングインスタンス	0	現在のリージョンで、このアカウントの WorkSpaces プールに使用できる Graphics.g4dn 4xlarge ストリーミングインスタンスの最大数。	あり

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 のサポート WorkSpaces 終了 (EOL) ポリシーは、 WorkSpaces 個人および WorkSpaces プールの 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 () の 3 つのフェーズがありますEOL。一般的なサポートフェーズは、 WorkSpaces クライアントの初回公開日に開始され、固定期間続きます。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を完全にサポートします。不具合の解決と機能リクエストは、そのメジャーバージョンおよび関連する WorkSpaces クライアントのマイナーバージョンに対して実装されます。

技術ガイダンスは、一般的なサポートフェーズの終わりからそのEOL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リクエストは、 WorkSpaces クライアントの最新バージョンに対してのみ実装されます。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、は今後公開されるバージョンリリースでその修正を 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、 WorkSpaces 最新バージョンにアップグレードするオプションがあります。

EOL メジャーバージョンの は、一般的なサポートと技術ガイダンスの両方が終了したときに発生します。EOL 日付を過ぎると、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。引き続きサポートするには、最新の WorkSpaces クライアント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EOLを避けるため、 に到達する前にサポートされている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。
>
> - 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 2024.0 ~ 2024.5
> - 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EOL日付に達する前に、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EOL日付に達する前に、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EOL日付に達する前に、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 の場合は 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 の場合は 2024.0 ~ 2024.5	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EOL日付に達する前に、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EOL日付に達する前に、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EOL日付に達する前に、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 20.04 用 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EOL日付に達する前に、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 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EOL日付に達する前に、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EOL日付に達する前に、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
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EOL日付に達する前に、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EOL日付に達する前に、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EOL日付に達する前に、必ず

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
				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EOL日付に達する前に、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	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EOL日付に達する前に、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
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 FAQs

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EOL。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 をダウンロードしてインストールします WorkSpaces。

サポートされている EOLで に到達したバージョンの WorkSpaces クライアントを使用できますか WorkSpace？

以前の解像度と機能が に達したクライアントバージョンに適用されなくなったため、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EOL、 AWS サポートチームにお問い合わせください。

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EOL。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。

に達したオペレーティングシステムでサポートされている WorkSpaces クライアントバージョンを使用していますEOL。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、 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 AWS 、 に達したオペレーティングシステムを使用する WorkSpaces クライアントにはサポートを提供しませんEOL。サポートされているオペレーティングシステムを使用して、 WorkSpaces クライアントがサポートされていることを確認します。

SDK でサポートされる 拡張機能 DCV

DCV は、幅広いワークロードやユースケースで、 WorkSpaces インスタンスへの高性能リモートアクセスを可能にします。Amazon DCV Extension を使用するとSDK、デベロッパーは次のようなエンドユーザーのDCV WorkSpaces エクスペリエンスを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 Extension の使用を開始するにはSDK、Amazon DCV Extension SDK のドキュメントを参照してください。SDK 自体は Amazon DCV Extension SDK GitHub リポジトリにあります。さらに、Amazon DCV Extension SDK サンプル GitHub リポジトリSDKに の統合例もあります。

以下は でサポートされています WorkSpaces。

- 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、iOS クライアント、ウェブアクセスはDCV拡張機能 をサポートしていませんSDK。

- WorkSpaces サポート – Windows、Linux、Ubuntu サーバー

のドキュメント履歴 WorkSpaces

次の表は、2018 年 1 月 1 日以降の WorkSpaces サービスと Amazon WorkSpaces 管理ガイドの重要な変更点を示しています。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、フィードを WorkSpaces RSSサブスクライブできます。

変更	説明	日付
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 Redirection Extension をインストールして、ウェブRTCリダイレクトを使用できます。	2024 年 8 月 1 日
WorkSpaces プールが で利用可能になりました AWS GovCloud (US) Region	WorkSpaces プールは、エフェメラルインフラストラクチャでホストされている高度にキュレーション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向けに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 7 月 23 日
WorkSpaces プールが利用可能になりました	WorkSpaces プールは、エフェメラルインフラストラクチャでホストされている高度にキュレーション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	2024 年 6 月 27 日

	ザー向けに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。	
AmazonWorkSpacesAdmin管理ポリシーの更新と新しい AmazonWorkSpacesPoolServiceAccess管理ポリシー	WorkSpaces が AmazonWorkSpacesAdmin 管理ポリシーを更新し、新しい AmazonWorkSpacesPoolServiceAccess 管理ポリシーを追加しました。	2024 年 6 月 27 日
AmazonWorkSpacesAdmin マネージドポリシーの更新	WorkSpaces は workspaces:RestoreWorkspace action を管理 AmazonWorkSpacesAdminポリシーに追加し、復元するためのアクセス権を管理者に付与しました WorkSpaces。	2023 年 7 月 17 日
SDK でサポートされる 拡張機能 DCV	Amazon DCV Extension を使用するとSDK、デベロッパーはエンドユーザーのDCV WorkSpaces エクスペリエンスをカスタマイズできます。	2023 年 5 月 25 日
DCV ホストエージェントのバージョン	のバージョン情報DCV。	2023 年 5 月 8 日
Amazon が AWS GovCloud（米国東部) で WorkSpaces 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 は、 を使用してローカルウェブカメラビデオ入力を Windows WorkSpaces デスクトップにシームレスにリダイレクトすることで、リアルタイムオーディオビデオ (AV) をサポートする WorkSpaces ようになりましたDCV。	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	Amazon WorkSpaces macOS クライアントアプリケーションを Common Access Card (CAC) および Personal Identity Verification (PIV) スマートカードで使用できるようになりました。スマートカードのサポートは、WorkSpaces の使用で利用できますDCV。	2021 年 4 月 5 日
Amazon WorkSpaces バンドル管理 APIs	Amazon APIs WorkSpaces バンドル管理が利用可能になりました。これらのAPIアクションは、 WorkSpaces バンドルの作成、削除、およびイメージの関連付けオペレーションをサポートします。	2021 年 3 月 15 日
Amazon がアジアパシフィック (ムンバイ) で WorkSpaces 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 は、(米国西部) リージョン WorkSpaces で Windows および Linux でのセッション前 AWS GovCloud (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 WorkSpaces ようになりました。	2020 年 12 月 1 日
DCV	DCV は、Graphics と を除くすべてのバンドルタイプ WorkSpaces に基づいて、ライセンス込み (Windows Server 2016) と BYOL Windows 10 ベースの両方で利用可能になりました GraphicsPro。 DCVは、 AWS GovCloud (米国西部) リージョン WorkSpaces の Linux 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。イメージが共有されると、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 を起動するためのバンドルを作成できます WorkSpaces。	2020 年 10 月 1 日

クロスリージョンリダイレクト	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する機能であるクロスリージョンリダイレクトを使用して、プライマリ WorkSpaces が使用できない場合にユーザーを代替 WorkSpaces にリダイレクトできるようになりました。	2020 年 9 月 10 日
の Microsoft Office 2016 または 2019 をサブスクライブする BYOL WorkSpaces	Bring Your Own Windows License (BYOL) で が提供する AWS Microsoft Office Professional 2016 または 2019 をサブスクライブできるようになりました WorkSpaces。	2020 年 9 月 3 日
BYOL 中国 (寧夏) でのオートメーション	Bring-Your-Own-License (BYOL) オートメーションを使用すると、中国 (寧夏) WorkSpaces の で Windows 10 デスクトップライセンスを使用するプロセスを簡素化できます。	2020 年 4 月 2 日
Image Checker	Image Checker ツールは、Windows がイメージ作成 WorkSpace 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 WorkSpace に使用する で一連のテストを実行し、見つかっ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

移行 WorkSpaces	Amazon WorkSpaces 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 WorkSpace から別のバンドルに 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 WorkSpaces から Windows 10 デスクトップエクスペリエンスに移行できます。この機能を使用して、パブリックバンドルまたはカスタムバンドル WorkSpaces から別のバンドルに移行することもできます。	2020年1月9日
PrivateLink Amazon の統合 WorkSpaces APIs	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介して Amazon WorkSpaces API エンドポイントに直接接続できます。VPC インターフェイスエンドポイントを使用すると、 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。	2019 年 11 月 25 日
Amazon 用の Linux クライアント WorkSpaces	ユーザーは Linux クライアントを使用して にアクセスできるようになりました WorkSpaces。	2019 年 11 月 25 日

Amazon が中国 (寧夏) で WorkSpaces 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
既知の最後の正常な状態 WorkSpaces への復元	復元機能を使用して、WorkSpace を既知の最後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 () に準拠するためにSRG、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 WorkSpaces ように Amazon 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
ユーザーのセルフサービス WorkSpace 管理機能	ユーザーがエクスペリエンスをより詳細に制御できるように、セルフサービス WorkSpace 管理機能を有効にできます。	2018 年 11 月 19 日

BYOL Automation	Bring-Your-Own-License (BYOL) オートメーションを使用すると、 に Windows 7 および Windows 10 デスクトップライセンスを使用するプロセスを簡素化できます WorkSpaces。	2018 年 11 月 16 日
PowerPro および GraphicsPro バンドル	PowerPro および GraphicsPro バンドルが利用可能になりました WorkSpaces。	2018 年 10 月 18 日
WorkSpace ログインの成功をモニタリングする	Amazon CloudWatch Events のイベントを使用して、正常な WorkSpace ログインをモニタリングして応答できます。	2018 年 9 月 17 日
Windows 10 のウェブアクセス WorkSpaces	ユーザーは、ウェブアクセスクライアントを使用して、Windows 10 デスクトップエクスペリエンス WorkSpace を実行している 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	ユニフォームリソース識別子 (URIs) を使用して、ユーザーに へのアクセスを提供できます WorkSpaces。	2018 年 7 月 31 日
Amazon Linux WorkSpaces	ユーザーに Amazon Linux WorkSpaces をプロビジョニングできます。	2018 年 6 月 26 日
IP アクセスコントロールグループ	ユーザーがアクセスできる IP アドレスを制御できます WorkSpaces。	2018 年 4 月 30 日

インプレースアップグレード	Windows 10 を Windows BYOL WorkSpaces 10 の新しいバージョン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 サービスと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	Value、Standard、Performance、Power バンドル WorkSpaces 間で を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 WorkSpaces 時に 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し、後でこれらのボリュームのサイズを増やすことができます。	2017 年 12 月 22 日
デバイスのアクセスコントロール	がアクセスできるデバイスのタイプを指定できます WorkSpaces。さらに、信頼されたデバイス (マネージドデバイスとも呼ばれます) WorkSpaces へのアクセスを制限できます。	2017 年 6 月 19 日
相互フォレストの信頼性	AWS Managed Microsoft AD とオンプレミスの Microsoft Active Directory ドメイン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プロビジョニング WorkSpacesできます。	2017 年 2 月 9 日
Windows Server 2016 バンドル	WorkSpaces は、Windows Server 2016 を搭載した Windows 10 デスクトップエクスペリエンスを含む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 WorkSpaces から Windows にアクセスできます。	2016 年 11 月 18 日
時間単位 WorkSpaces	ユーザーが時間単位で請求 WorkSpaces されるように を設定できます。	2016 年 8 月 18 日
Windows 10 BYOL	Windows 10 デスクトップライセンスを WorkSpaces () に持ち込むことができます BYOL。	2016 年 7 月 21 日
タグ指定のサポート	タグを使用して を管理および追跡できます WorkSpaces。	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 クライアントはそれを保存します。これにより、異なるディレクトリまたはリージョン WorkSpaces で を簡単に切り替えることができます。	2016 年 1 月 28 日
Windows 7BYOL、Chromebook クライアント、WorkSpace暗号化	Windows 7 デスクトップライセンスを WorkSpaces （ BYOL) に持ち込み、Chromebook クライアントを使用し、暗号化を使用できます WorkSpace。	2015 年 10 月 1 日
CloudWatch 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	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関する情報を追加しました WorkSpaces。	2015 年 3 月 31 日
パブリック IP アドレス	にパブリック IP アドレスを自動的に割り当てることができます WorkSpaces。	2015 年 1 月 23 日

変更	説明	日付
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) リージョンで利用できます。	2015 年 1 月 15 日
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 WorkSpace した からイメージを作成し、イメージからカスタム WorkSpace バンドルを作成できます。	2014 年 10 月 28 日
PCoIP ゼロクライアントサポート	ゼロクライアントデバイスにアクセスできます WorkSpaces PCoIP。	2014 年 10 月 15 日
WorkSpaces アジアパシフィック (東京) で が開始	WorkSpaces は、アジアパシフィック (東京) リージョンで利用できます。	2014 年 8 月 26 日
ローカルプリンターのサポート	のローカルプリンターサポートを有効にできます WorkSpaces。	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るデフォルトの組織単位 (OU) と、 WorkSpace マシンアカウントが作成される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	セキュリティグループを に追加できます WorkSpaces。	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) リージョンで利用できます。	2014 年 5 月 15 日

変更	説明	日付
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) リージョンで利用できます。	2014 年 5 月 5 日
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。